Cisco Tidal Enterprise Scheduler 6.2 Installation Guide

May 22, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-32249-01

Cisco Tidal Enterprise Scheduler 6.2 Installation Guide

Preface

This guide describes how to use Cisco Tidal Enterprise Scheduler (TES) 6.2.

Audience

This guide is for administrators who configure, monitor, and maintain TES, and who troubleshoot TES issues.

Related Documentation

See the *Cisco Tidal Enterprise Scheduler 6.2 Documentation Overview* for a list of all TES guides.

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Installation Prerequisites

This chapter discusses the system requirements, user requirements, installation prerequisites and the supported databases for the various components of Cisco Tidal Enterprise Scheduler (TES) version 6.2.0.

Minimum System Requirements

The following table contains the minimum system requirements for installing and running TES. The specified quantities of CPU, memory and disk space must be available for exclusive use by TES. Use additional RAM and disk space as necessary for your particular environment.

Table 1-1 System Requirements

Component	Platform					Minimum System Requirements (Dedicated Machine)			
Master (Primary or Backup)	**OS Name**	**Version**	**Chipset**	**32-bit**	**64-bit**	**JVM**	**Processor**	**RAM**	**Disk**
	HPUX	11.11	RISC	X		HP 7	Dual Processor	2GB for TES Master + 1GB per adapter	1GB
	Solaris	9,10	Sparc	X	X	Oracle 7	Dual Processor	2GB for TES Master + 1GB per adapter	1GB
		10	Opteron		X	Oracle 7	Xeon Dual	2GB for TES Master + 1GB per adapter	1GB
	AIX	5.3 TL,9,10,11,6.1, 7	RISC, PPC	X	X	IBM 7	Dual Processor	2GB for TES Master + 1GB per adapter	1GB
	Windows	Server 2008	Intel/AMD	X	X	Oracle 7	Xeon Dual Core 2GHz	2GB for TES Master + 1GB per adapter	1GB
		Server 2012	Intel/AMD	X	X	Oracle 7	Xeon Dual Core 2GHz	2GB for TES Master + 1GB per adapter	1GB

Component	Platform					Minimum System Requirements (Dedicated Machine)			
	Linux	Redhat Enterprise Server v4,v5, v6 (64-bit) Cent OS v4, v5, v6	Intel/AMD	X	X	Oracle 7	Xeon Dual Core 2GHz	2GB for TES Master + 1GB per adapter	1GB
		SUSE Enterprise Server v11	Intel/AMD	X	X	Oracle 7	Xeon Dual Core	2GB for TES Master + 1GB per adapter	1GB
		Oracle Enterprise Linux v5	Intel/AMD	X	X	Oracle 7	Xeon Dual Core	2GB for TES Master + 1GB per adapter	1GB
Fault Monitor (OS must match master)	HPUX	11.11	Itanium		X	HP 7	100 MHz	256MB	500MB
	Solaris	9,10	Sparc	X	X	Oracle 7	100 MHz	256MB	500MB
		10	Opteron		X	Oracle 7	100 MHz	256MB	500MB
	AIX	5.3 TL, 9,10, 11,6.1	RISC & PPC	X	X	IBM 7	100 MHz	256MB	500MB
	Windows	Server 2008	Intel/AMD	X	X	Oracle 7	400 MHz	256MB	500MB
		Server 2012	Intel/AMD	X	X	Oracle 7	400 MHz	256MB	500MB
	Linux	Redhat Enterprise Server v4,v5, v6 Cent OS v4, v5, v6	Intel/AMD	X	X	Oracle 7	400 MHz	256MB	500MB
		SUSE Enterprise Server v11	Intel/AMD	X	X	Oracle 7	400 MHz	256MB	500MB
		Oracle Enterprise Linux 5.2	Intel/AMD	X	X	Oracle 7	400 MHz	256MB	500MB
	VMWare	ESX 3.0, ESXi 3.5, ESXi 4.0, 5							

Component	Platform					Minimum System Requirements (Dedicated Machine)			
	VMWare ESX on UCS	ESXi 4.0 U1, 5	UCS: B250 M1, C250 M1, B200 M1, B200 M2, B250 M2, C200 M1, C210 M1						
		ESX 3.5 U5, 5	UCS: B250 M1, C250 M1, B200 M1, B250 M2, C200 M1, C210 M1						
Transporter	Windows 7 (64 bit); Windows 2008 (64 bit)	1.6	6 GB (recommended for moderate envs 25K jobs)						
Client Manager Web Service API runs against this platform	HPUX	11.11	RISC			HP 7	Dual Processor 1GHz	8GB for Client Manager	2GB/SCSI 10,000 RPM
	Solaris	9,10	Sparc		X	Oracle 7	Dual Processor 1GHz	8GB for Client Manager	2GB/SCSI 10,000 RPM
		10	Opteron		X	Oracle 7	Xeon Quad 2GHz	8GB for Client Manager	2GB/SCSI 10,000 RPM

Component	Platform					Minimum System Requirements (Dedicated Machine)			
	AIX	5.3,6.1,7	RISC & PPC		X	IBM 7	Dual Processor 1GHz	8GB for Client Manager	2GB/S CSI 10,000 RPM
	Windows	Server 2008	Intel x86/A MD		x	Oracle 7	Xeon Quad 2GHz	8GB for Client Manager	2GB/S CSI 10,000 RPM
		Server 2012	Intel/A MD		X	Oracle 7	Xeon Quad 2GHz	8GB for Client Manager	2GB/S CSI 10,000 RPM
	Linux	Redhat Enterprise Server v4,v5, v6 Cent OS v4, v5, v6	Intel x86/A MD		X	Oracle 7	Xeon Quad 2GHz	8GB for Client Manager	2GB/S CSI 10,000 RPM
		SUSE Enterprise Server v11	Intel x86/A MD		X	Oracle 7	Xeon Quad 2GHz	8GB for Client Manager	2GB/S CSI 10,000 RPM
		Oracle Enterprise Linux 5.2	Intel x86/A MD		X	Oracle 7	Xeon Quad 2GHz	8GB for Client Manager	2GB/S CSI 10,000 RPM
	VMWare	ESX 3.0, ESXi 3.5, ESXi 4.0, 5				Oracle 7	Xeon Quad 2GHz	8GB for Client Manager	2GB/S CSI 10,000 RPM

Component	Platform					Minimum System Requirements (Dedicated Machine)			
	VMWare ESX on UCS	ESXi 4.0 U1, 5	UCS: B250 M1, C250 M1, B200 M1, B200 M2, B250 M2, C200 M1, C210 M1						
		ESX 3.5 U5, 5	UCS: B250 M1, C250 M1, B200 M1, B250 M2, C200 M1, C210 M1						

Warning **It is recommended that no more than five agents be run on the minimum hardware platform. However, the number of agents that can be run on a given server depends upon the CPU and memory resources available on the machine. Add a single agent at a time and gauge the effect of each added agent on system performance before adding more. You have to experiment with the configuration to achieve optimal results.**

Note Although the minimum memory required is 4GB for PCs running the Web Client, additional memory helps with better performance. At least 2GB of free memory must be available for the browser.

Note When installing a 64-bit master for use with an Oracle database, the installer requires that 32-bit oracle client software in order to connect to the Oracle database. After installing, the master does not require the 32-bit client software to run.

Browser Compatibility

Table 1-2 Browser Compatibility

Browser Type	Version	Platform
Internet Explorer (64-bit) (32-bit not recommended)	9, 10	Windows Server 2003 Windows Server 2008 Windows Server 2012 RedHat Linux SUSE Linux Windows 7
Firefox	15, 16, 18, 20, 22, 24	Windows Server 2003 (32-bit and 64-bit) Windows Server 2008 (32-bit and 64-bit) Windows Server 2012 (32-bit and 64-bit) Redhat Linux (32-bit and 64-bit) SUSE Linux (32-bit and 64-bit) Windows 7 (32-bit and 64-bit)

Note For Client Manager installation instructions and compatibility matrix, refer to "Installing Client Manager" .

User Security Requirements

The security requirements for TES vary according to the task the user account needs to accomplish. The user account that installs the components of TES requires different security rights than an account that runs TES as a service. The user account that will operate TES has its own security needs. The following points and Table 1-3 illustrate security rights differences between the various TES components.

- If you are planning to use an Oracle or Microsoft SQL database, your database administrator will be required during installation of the Client Manger and the master. Passwords to the database and connections to the database are necessary for installing the product. Agent and master installations also require a Windows administrator to provide passwords during installation.
- The Client Manager and agent should be installed under the same user name with equivalent capabilities.
- When installing TES Agent for Unix, you must be able to log in as root.
- The Tidal Agent for Unix provides another layer of security by having its single java process run as the agent owner with the same security rights as its owner. By default, the agent does not have access to all of the dependent files, scripts and environment variables it may need. A Unix job cannot complete successfully unless you ensure that the agent has the proper access rights to all of the files needed during the processing of a job.

- The Windows components require access to COM objects. Verify that the user doing the installation can access COM objects or an access violation error will occur when you attempt installation. If necessary, the procedure to verify and provide access to COM objects is explained in "Java Path Mismatch" in the *Troubleshooting* chapter.
- LDAP users can be imported into TES for improving user audit trails. These imported users inherit security from multiple LDAP groups. Imported LDAP user information is stored into a user definition that includes email, telephone, etc. Imported LDAP users are allowed to be owners of scheduling constructs such as jobs if their security permits it. User definitions must be migrated to LDAP groups.
- The Administration group in 6.2 has three distinct entries for adding users, "Interactive Users", "Runtime Users" and "LDAP Groups". TES 6.0 allows for the setup of a user that authenticates against Active Directory/LDAP. TES also supports AD/LDAP only users.
- At login, user credentials are validated against Active Directory/LDAP. Once authenticated, TES obtains the users AD/LDAP groups and other information such and phone number and email.
- Once login has completed, a record is established in TES to represent the Active Directory/LDAP **only** user if not already present and only if the user belongs to an Active Directory/LDAP group defined in TES. All user activity logging is then done against this new user record allowing for correct auditing and reporting.
- Active Directory/LDAP only users will be allowed to create and own jobs and other objects if their security permissions permit.
- TES LDAP groups are supported by the creation of groups within the TES application.
- Security policies can be defined and specialized by application administrators.
- Each group within TES can be assigned one security policy.
- The security capabilities of a user are based upon the summation of the security policies defined for each of the groups that the user is a member of and any security policy directly assigned to the user. The latter is only available for users created within TES not imported from AD/LDAP.
- Workgroups are also available within the TES application. These workgroups can be used to own related objects. Users and groups can be made a member of one or more workgroups. Workgroup security allows for additional security policies to be applied to scheduling constructs (jobs, view, alerts, etc.) owned by the workgroup for a particular user associated with the workgroup.
- When a user or a group is made a member of a workgroup then additional security policies can be applied to this relationship. The users total security capabilities will then be a summation of their user applied security policy, the security policy associated with each of the groups they are a member of, and the security policies contained in the relationship between the user or group and the workgroups they are a member of (in the context of objects contained in that workgroup).

Table 1-3 Rights Required for Installation and Usage of Scheduler Components

	Installation Rights	Service Rights	User Rights
Windows Master	• Local Administrator • Able to access COM objects	• Local Administrator or Local System • Logon as a service • Able to access COM objects	Local Administrator or Local System
Unix Master	• Must be installed under a user created by root • Access rights to JVM	Access rights to JVM	• User account must be created by root • Access rights to JVM

Table 1-3 Rights Required for Installation and Usage of Scheduler Components

	Installation Rights	Service Rights	User Rights
Windows Agent	Local Administrator Able to access COM objects	Local System or if running under Domain\User must have local administrator rights including: • Logon as a batch job • Logon as a service • Act as part of the operating system • Replace a process level token • Able to access COM objects On machines running Windows 2003, you also need the following privileges: • Bypass traverse checking • Adjust memory quotas for the process • User must be root or created by root • Access rights to JVM	Local System or if running under Domain\User must have local administrator rights including: • Logon as a batch job • Logon as a service • Act as part of the operating system • Replace a process level token • User must be root or created by root • Access rights to JVM • Ability to change to the runtime user
Unix Agent	Logon as root	N/A	N/A
Client Manager	• Local Administrator • Able to access COM objects	N/A	General user rights

Installation Requirements

- Determine which components you are going to install and where you are going to install them before you install TES. Because the InstallShield Wizard/Scheduler Setup requires information about the location of masters, Client Managers and agents, decide beforehand where they will be installed. Obtain machine names, host names, port numbers and IP addresses before beginning the installation.
- Ensure that each computer used for TES can communicate with the other machines on the network. If you cannot ping to and from each component machine, TES cannot function properly. Network conditions affect the operation of TES.
- Ensure that you are logged on with an account that has Administrator privileges.
- Download the latest set of hotfixes for Tidal Enterprise Scheduler from cisco.com.
- Review any supplementary documentation provided with your software such as the release notes or *Read Before Installing*. Last-minute instructions may be contained in these documents.
- If you are upgrading TES, install the program in the same directory in which the previous version was installed to keep your data intact.
- Exit all Windows programs before running any installation.
- Contact Support if you have any questions.

Supported Databases

Before installing TES you should already have database software installed on your machine.

The Master supports the following databases:

- MSSQL Server 2008 or SQL Server 2012 single or multi-instance: 128 MB Data, 32 MB Log

- Oracle 10g, 11g, 11gR2 (Oracle provided software for Scheduler client): 400MB Data, 300MB index, 200MB temp

Note TES does not support case-sensitive sort-ordered databases.

You need the following number of database access licenses:

- Each master should have access to up to 20 database client licenses to use as needed during processing

Client Manager supports the following databases:

- Derby (default)
- SQL server (external)
- Oracle 11g R2 (external)

Supported Database Configurations

The following DB configurations are supported:

Master on Unix	Oracle DB on UNIX
Master on Windows	• Oracle DB on UNIX • MSSQL on Windows • Oracle On Windows

Microsoft SQL Database Requirements

Microsoft SQL Server users should verify the following items before installing TES:

- There exists a DATA folder in your SQL Server installation.
- There is enough space on the drive to create the TES database.
- The Microsoft SQL client or the actual database is already installed on the machine that will have a TES master on it.

If you are installing a TES master, SQL Server must already be installed, either on the same machine where you are installing the master, or on another machine in the same domain.

Oracle Database Requirements

The master uses only JDBC to connect to any Oracle-related database. TES requires that the OLE providers for the Oracle 10g, 11i database be installed on each TES machine. These OLE providers are normally installed only during a full Oracle client install. Have your Oracle administrator install these drivers on each machine that will run TES. The drivers are called “Oracle Provider for OLE DB” and are selected in the Oracle Windows Interfaces section of a custom install.

If you are performing a master installation, your database administrator will also need to know the Oracle tablespace datafiles to be used with TES. The following three Oracle tablespace datafiles are created by TES during installation and require at least the stated amount of tablespace:

- ADMIRAL_DATA 400 MB
- ADMIRAL_INDEX 300 MB

- ADMIRAL_TEMP 200 MB

The *tnsnames.ora* file must exist on or be available to the TES master machine. This file is typically found in the Oracle home directory. The *tnsnames.ora* file should be local since network access may not always be available to the master service, and it must be available to the TES master. Verify that the Oracle bin folder is in your system path before installing TES.

Because TES utilizes the Oracle Native drivers for connectivity, the Oracle SQL*Net client needs to be installed and configured on all Windows masters. To verify that the ORACLE client connection is correctly configured, from the DOS prompt, use the tnsping to the database tns entry.

Licensing

Before you can run TES, you need to run through the licensing procedure. This applies whether you are just trying out the software, or have already decided to implement TES. TES provides different types of licenses to fit your needs.

Note Ensure that your database is licensed in line with your database vendors licensing terms and conditions.

Table 1 Software License Types

License Type	Description
Demo License (unrestricted)	If you want to demo the product, you can ask for a demo license from a sales representative. You will be given a license code to enter when you run the product for the first time. Full use of the software will be available for a limited amount of time.
Demo License (restricted)	The restricted demo license allows full use of the product on a limited number of machines for a limited amount of time.
Production License	If you decide to purchase TES, your sales representative can give you a production license. This license will be customized to match your planned installation. Apply your license file as soon as possible so that the software does not expire. You will receive a Master/Agent License Summary which you should keep for your records.
Floating License	Usually a product license specifies that the software works on a particular machine, but a floating license is not tied to a specific machine. Instead the right to use the license “floats” among many users but only the approved number of users can use the license at once.
Annual Use Production License	This has provisions similar to a Production License and is renewed on a yearly basis.
Emergency License	If you already have a license, and you need to expand your scheduling capabilities for a short period of time for disaster recovery, you can request an Emergency License code. This code will give you unlimited use. You will be able to add as many agents as you need, or to transfer your master to another machine to help you through your situation.

Extensions and modules that add extra functionality to TES may require separate licenses. For example, SACmd (TES command line interface), the job monitoring tool and intermaster dependencies all require individual licenses. For more information and current availability, contact your sales representative.

You can license TES with a Demo license or a Full license. During installation, the installer will prompt you for a demo code, and if you give it a code, then it will create this file for you. When your Demo license expires, or if you did not enter it during installation, you can manually license TES.

Registered License Dialog

The Registered License dialog displays by selecting **Activities>Registered License** from the main menu of the Tidal Web client.

Master License Tab

This tab displays the following information about the master:

- **Company Name** – Your company name. No company name displays if you have a demo license. The company name displayed here is used in all Scheduler reports.
- **Master License for machine** – The licensed master machine name.
- **Serial Number** – The unique identification number of the master machine.
- **Operating System** – The operating system of the Scheduler master machine.
- **Database** – The type of database used. This field will show either Oracle or Microsoft SQL Server.
- **Expiration** – The license's expiration date. You may need to renew your license before the expiration date.
- **Options** – Displays added purchased software options that complement Scheduler (e.g. fault tolerance).
- **Connections** – Contains the available connections associated with the license.

Licensed Agents Tab

The Licensed Agents tab displays information about the agents licensed to work with the master.

Note If your license has a floating agent provision or if you are running an unrestricted demo, you can define your own agents. Consequently, the Licensed Agents tab will display no information.

This tab displays the following information about the agents:

- **Agent** – The machine name for the licensed agent.
- **Serial** – The serial number of the licensed agent.
- **Floating** – Specifies if the license is floating or not.
- **Operating System** – The operating system type of the licensed agent. Scheduler supports MPE/iX, MVS, z/OS, OS/400, Windows and Unix platforms.

- **Expiration** – The license's expiration date. You may need to renew your license before the expiration date.
- **Max Jobs** – The maximum number of jobs that you can run on the agent concurrently. You can configure a lower value for the agent from the Connections pane, but this value cannot exceed your licensed value.
- **Jobs** – Displays the current count of jobs, tracking the number of jobs to enforce the license restriction on an agent as shown in the Max Jobs column.
- **CPU** – The number of CPUs on an agent machine. If the number of CPUs on a machine exceeds the authorized number, the master disables the agent connection and logs a licensing error. The licensing discrepancy must be resolved by contacting the Licensing Administrator for Tidal Software before the agent connection can be re-established.

Warning **Restart the Client Manager after a new license has been loaded.**

Licensing Procedure

Registering the license for TES is done from the Tidal Web client.

Note Before you start the licensing procedure, set the system queue to 0. Select **Queues> System Queue**, and set the value to 0. This will stop all jobs from launching. Wait until all running jobs have completed.

To license with a Demo license:

Step 1 Stop the master. You must stop the master before you can load a license file. An error message will display if you attempt to load a license while the master is still running.

For Windows:

a. Click Start and select **Programs>TIDAL Software>Scheduler>Master>Service Control Manager**.

b. Verify that the master is displayed in the Service list and click the Stop button to stop the master.

For Unix:

Enter **tesm stop**.

Step 2 Create a file called demo.lic.

Step 3 Type the demo code into the demo.lic file.

Step 4 Save and place the file in the C:\Program File\TIDAL\Scheduler\Master\config directory.

Step 5 Restart the master:

- For Windows, restart the master by clicking Start in the Service Control Manager.
- For Unix, restart the master by entering tesm start.

The master will read and apply the demo code when it starts.

To license with a Full license:

Step 1 Stop the master:

For Windows:

a. Click Start and select Programs>TIDAL Software>Scheduler>Master>Service Control Manager.

b. Verify that the master is displayed in the Service list and click the Stop button to stop the master.

For Unix:

Enter tesm stop.

Step 2 Rename your Full license file to master.lic.

Step 3 Place the file in the C:\Program File\TIDAL\Scheduler\Master\config directory.

Step 4 Restart the master:

- For Windows, restart the master by clicking **Start** in the Service Control Manager.
- For Unix, restart the master by entering tesm start.

The master will read and apply the demo code when it starts.

Installing the Master for Windows

TES can be configured on a network in many different ways. The master is installed with default parameters that provide most users with optimum performance but individual circumstances may require reconfiguring the master parameters after installation. These parameters are managed in a *master.props* file residing on the master machine. Refer to "Configuring the Master" for information on modifying the main master properties.

Installation Prerequisites

The following requirements must be met for successful installation of the TES master:

- User with local Administrator privileges
- One of the Windows operating systems listed in "Minimum System Requirements".
- The master machine must be able to ping the database server's host name and to establish a normal database client connection to the database service (and the backup master and fault monitor server host names, if in a fault tolerant configuration)
- Database software already installed single or multiple instance (See "Supported Databases" for further information.)
- Apply all patches supplied in the latest hotfix for TES 6.2.
- Set the system properties to provide the complete path to the bin directory.

  For example:

  ```
  E:\Oracle\product\11.2.0\client_1\bin;%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\
  System32\Wbem;%systemroot%\System32\WindowsPowerShell\v1.0\;C:\Program
  Files\Java\jre7\bin
  ```

To set system properties to provide the complete Java path:

Step 1 Right click My Computer, and choose **Properties**.

Step 2 Click the **Advanced system settings** link in the left pane.

The System Properties dialog box displays.

Step 3 Click **Environment Variables**, and select the path to edit in the Environment Variables dialog box.

Step 4 Click **Edit** and provide the complete Java path, down to the bin directory.

Installing the Windows Master

Note This installation procedure for installting the Windows master differs depending upon whether the database being used is Microsoft SQL Server or Oracle.

Using a Microsoft SQL Database

To install the master component using a Microsoft SQL database:

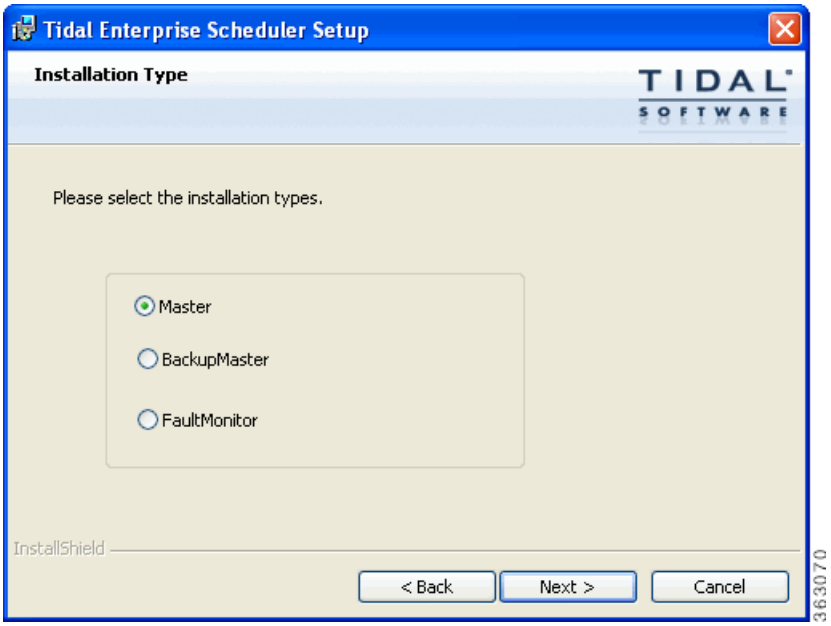
Step 1 Run *setup.exe*.

Step 2 On the Internet Explorer-Security Warning dialog box, click **Run**.

Step 3 On the Welcome panel, click **Next**.

Step 4 On the Installation Type panel, select **Master**, then click **Next**.

Figure 2-1 Installation Type Panel



Step 5 On the TES Super User panel, enter the following, then click **Next**.

- Enter the domain name for your master into the Domain field.
- Enter the name of the Super user for this master.
- If you have a demo code, enter the code into the If you have a demo code enter it here: field.

Step 6 On the Destination Folder panel, select the directory where the Scheduler files will reside, then click **Next**.

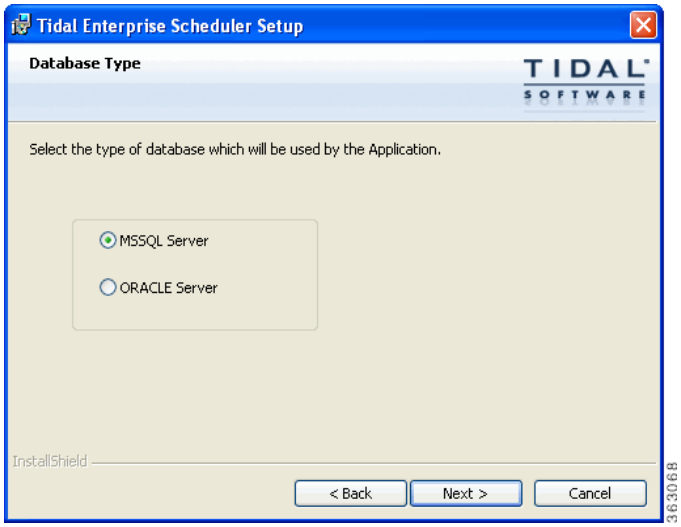
- Click **Browse**, locate a directory, select the appropriate file and click **Save**.

  -or-

- Accept the default location at *C:\Program Files\TIDAL*.

Step 7 On the Database Type panel, select **MSSQL Server**, then click **Next**.

Figure 2-2 Database Type Panel



Step 8 On the Database Server panel, identify the Microsoft SQL database and logon you are using, then click **Next**.

- **Database HostName**—Enter the hostname of the database server.

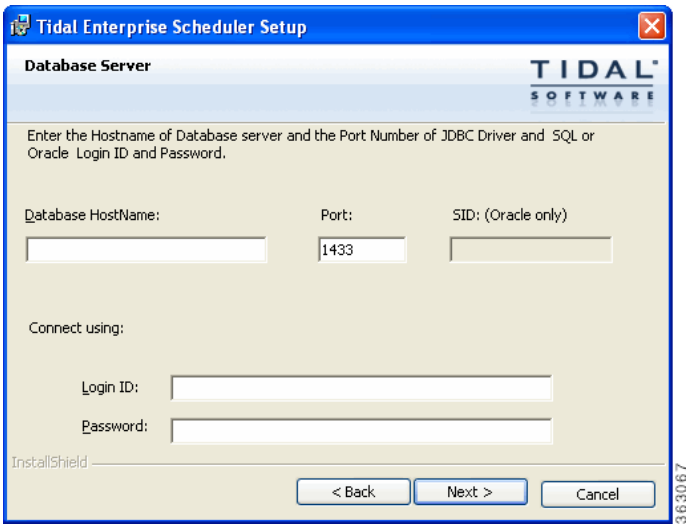
Note The master should not be installed on hosts with underscores in their names or the JMS connections will fail between components.

- **Port**—Enter the port number of the JDBC driver. The default port is 1433.
- **SID**—Enter the Oracle System ID (Oracle only).

Note The Oracle SID and Service Name should be the same on the database. However, if they are different, provide the Oracle Service Name as the SID in this field.

  - **Login ID**—Enter the login credentials for the database administrator.
  - **Password**—Enter the password for the database administrator.

Figure 2-3 Database Server Panel



Step 9 On the Admiral Database and Transaction Log File Path panel, click **Next** to accept the default paths.

Step 10 On the Database Size panel, enter database and log file sizes, then click **Next**.

- Enter new values (in megabytes).

  -or-

- Accept the default values.

The Active Directory/LDAP Authentication panel displays.

Step 11 Select an option, then click **Next**.

If configuring the Client Manager to use the Active Directory option, the Active Directory Authentication panel displays.

If configuring the Client Manager to use the LDAP option, the LDAP Authentication panel displays.

Step 12 For Active Directory, enter the following information:

- **Host—** Enter the hostname or IP address for the Active Directory server.
- **User Search Prefix—**Enter the location you want Active Directory to search for users.
- **Group Search Prefix—** Enter the location you want Active Directory to search for groups.
- **Port—**Enter the port number for the AD server.

-or-

For LDAP, enter the following information:

- **Hostname**— Enter the hostname or IP address for the LDAP server.
- **Port—** Enter the port number for the LDAP server.
- **BindDN—** Enter the user account to query the LDAP server.
- **UserObjectClass—** Specify a valid object class for the BindDB user. Only users who posses one or more of these objectClasses will be permitted to authenticate.
- **UserBindDN—** Enter the user account to query the LDAP server.
- **User-role based access for Oracle/Sun Directory Server—** Select this option if your TES 6.2 Web Client user authentication is defined to use Oracle/Sun Directory Server with role-based access.

- **GroupBindDN—** Enter the group account to query the LDAP server.

Step 13 On the Ready to Install the Program panel, click **Install** to start the installation process.The Installing Tidal TES - Master panel displays.

The progress of your master installation is displayed in the form of a progress bar.

Warning **Do not click Cancel once the installation process begins copying files in the Setup Status panel. Cancelling the installation at this point corrupts the installation program.**

You will not be able to install the component without the help of Support. If you decide you do not want to install the component, you must complete the installation and then uninstall.

Step 14 On the Setup Completed panel, click **Finish**.

Using an Oracle Database

Note The procedure for installing a master running an Oracle database is very similar to the procedure used when running a Microsoft SQL database. The differences are described in the following procedure.

To install the master component using an Oracle database:

Step 1 Run *setup.exe*.

Step 2 On the File Download-Security Warning panel, click **Run**.

Step 3 On the Internet Explorer-Security Warning panel, click **Run**.

Step 4 On the Welcome panel, click **Next**.

Step 5 On the Installation Type panel, select **Master**, then click **Next**.

Step 6 On the TES Super User panel, enter the following, then click **Next**.

- Enter the domain name for your master into the Domain field.
- Enter the name of the Super user for this master.
- If you have a demo code, enter the code into the If you have a demo code enter it here: field.

Step 7 On the Destination Folder panel, select the directory where the Scheduler files will reside, then click **Next**.

- Click **Browse**, locate a directory, select the appropriate file and click **Save**.

  -or-

- Accept the default location at *C:\Program Files\TIDAL*.

Step 8 On the Database Type panel, select **Oracle Server**, then click **Next**.

Step 9 On the Database Server panel, identify the Oracle database and logon you are using, then click **Next**.

- Database HostName – Enter the hostname of the database server.
- Port – Enter the port number of the JDBC driver. The default port is 1521.
- SID – Enter the Oracle System ID.

- Login ID – Enter the login credentials for the database administrator.
- Password – Enter the password for the database administrator.

Note This information is available from the Oracle Database Administrator.

Step 10 On the Oracle Tablespace Datafiles panel, specify the name and location of the Data, Index and Temp tablespaces so Scheduler can access the files, then click **Next**. By default, Scheduler calls the datafiles, ADMIRAL_DATA, ADMIRAL_INDEX and ADMIRAL_TEMP. You can retain the default name or replace the default values with different names but you must type the directory path to each datafile location.

Step 11 On the Ready to Install the Program panel, click **Install** to start the installation process.

The Installing Tidal TES - Master panel displays.

The progress of your master installation is displayed in the form of a progress bar.

Warning **Do not click Cancel once the installation process begins copying files in the Setup Status screen. Cancelling the installation at this point corrupts the installation program.**

You will not be able to install the component without the help of Support. If you decide you do not want to install the component, you must complete the installation and then uninstall.

Step 12 On the Setup Completed panel, click **Finish**.

Verifying Master Connection

Use the Service Control Manager to verify that the master is running.

To verify connection:

Step 1 From the Windows Start menu on the master machine, select **Programs > TIDAL Software > Scheduler > Master > Service Control Manager** to display the Tidal Service Manager.

Step 2 From the Service list, select **Scheduler Master**. The master status displays at the bottom of the dialog box.

Step 3 Click **Start** to start the master if it is not running.

Configuring the Master

Most of the master parameter configurations are completed from the *master.props* file in the *config* directory. Parameter values are added or modified from this file. If you used the default locations during installation the *master.props* file is located at:

C:/Program Files/TIDAL/Scheduler/Master/Config/master.props

Configuring the Master for SNMP

If you want to use Simple Network Management Protocol (SNMP) to send traps in TES, you must tell the master how to connect to the SNMP server. You can configure the master to use SNMP from the *master.props* file.

To configure the master for SNMP:

Step 1 Stop the master using the Tidal Service Manager.

a. From the Start menu on the master machine, choose **Programs > TIDAL Software > TIDAL Service Manager** to display the Tidal Service Manager.

b. From the Service list, select **Scheduler Master**. The master status displays at the bottom of the dialog box.

c. Click **Stop** to stop the master. (The bottom of the dialog box displays "Scheduler Master: Stopped".)

Step 2 Open the *master.props* file in a text editor such as Notepad.

The *master.props* file is located in the *config* directory. If you used the default locations during installation, the *master.props* file is located at:
C:/Program Files/TIDAL/Scheduler/master/config/master.props

Step 3 On separate lines, enter the following SNMP information:

snmphost=<hostname of the SNMP server>

snmpport=<port number used by the SNMP server>

Step 4 Replace the text enclosed in brackets with the hostname and port number for the SNMP server.

Step 5 Save and close the *master.props* file.

Step 6 Restart the master from the Tidal Service Manager.

Configuring the Nice Value for the Master Service

Usually the Scheduler master service would have the highest priority for CPU resources on the machine where it resides but there may be occasions where you want other services to have a greater priority to CPU resources. You can reconfigure the Scheduler master service to a lower priority by assigning it a Unix nice value as used in the `ps` command for the Solaris, HPUX and AIX operating systems.

Scheduler uses a different nice value scale than that used in Unix systems but the following formula can be used to convert the Scheduler nice value to a Unix nice value:

20 - (Scheduler nice value -1) = Unix nice value

For example, a Scheduler nice value of 40 for the master service would convert to a -19 Unix nice value, 20 - (40-1) = -19.

Changing the Master Database Password

To change the Master database password:

Step 1 Log on the master machine.

Step 2 Navigate to the master installation directory inside cmd.exe.

Step 3 Run the following command:

```
java -classpath lib\scheduler.jar -DTIDAL_HOME=.com.tidalsoft.scheduler.SetPwd tidal97
tidal98
```

Note In the command above, tidal97 is an example of the current password and tidal98 is an example the new password. When you execute the command, provide your own current and new passwords.

The master.props will have a line added to it similar to the following:

```
dbpwd=511 \\rx((YYYSS
```

Installing an Oracle Database

See "Using an Oracle Database" for Oracle database installation requirements.

Adding an Oracle Service as a Master Dependency

If you are installing the TES master on the same Windows machine that will be your Oracle database server, manually add the Oracle service as a dependency to the TES master service before it can start automatically when the system is rebooted.

To add the Oracle service as a TES master dependency:

Step 1 Log in as an **Administrator**.

Step 2 From the Windows Start menu, choose **Programs > TIDAL Software > Scheduler > Master>Service Manager > Scheduler Master**.

Step 3 Stop the master by clicking **Stop**.

Step 4 Click **Configure**, then click **Dependencies**.

Step 5 Select the service **OracleService <service name>** from the **Available Services** list and drag it to the Depends On tab.

Step 6 Click **OK**, then click **OK** again.

Step 7 Click **Start**.

The next time you reboot, the TES master service will start automatically after the Oracle server service has started.

Installing an Oracle Database Manually

Although it is recommended that the installation process create the Admiral database for Oracle, users can create the database manually. If the Create database manually after installation option is selected while installing the master, your DBA must perform the procedures below after the TES installation completes.

The Oracle SQL scripts needed to create the database can be found in the Oracle directory within the master directory where you installed the Scheduler program files. If you did not select the default location, the files are in the directory location you specified.

Inside the *oracle* directory is a *connectdb.sql* script. Certain parameters in this script must be edited before manual installation of the database.

Note If you wish to install the datafiles in a specific directory, the Oracle DBA can change the CREATE TABLESPACE statements to specify a different directory location for the datafiles. The datafile growth options may also be modified if desired. Do not lower the default SIZE values.

The CREATE USER, GRANT and ALTER USER statements contain critical security information values in the brackets < >. Contact Support for assistance with the appropriate values.

Once you have entered the information you received from Support in the appropriate places in the *connectdb.sql* script, save and close the script.

To install manually:

Step 1 Open the Oracle SQL*Plus program.

Step 2 Login as the SYSTEM user (or equivalent) and connect to the ADMIRAL TNS Name.

Step 3 Run the following installation script:

@C:\progra~1\TIDAL\Scheduler\master\oracle\instnew.sql

Note For debugging purposes, you may wish to run a spool file as you run the installation script.

Step 4 Edit *orapopulate.sql* so it will create a valid initial super user account.

Find the following statement and change **`DOMAINNAME`** and **`SUPERUSERNAME`** to be the domain and user name of the initial super user account:

insert into usrmst (usrmst_id, usrmst_domain, usrmst_name, usrmst_fullname, usrmst_desc, usrmst_phoneno, usrmst_pagerno, usrmst_email, usrmst_emailtype, secmst_id, lngmst_id, usrmst_password, usrmst_suser) values (1, DOMAINNAME, 'SUPERUSERNAME', 'SUPERUSERNAME', null, null, null, null, null, 6, 1, null, 'Y');

Note **DOMAINNAME** can be null. If it is not null, be sure to add single quotes around the domain name in the sql statement. Your Oracle TES database should now be installed.

Uninstalling the Windows Master

A *temp* directory must be present on the root of your hard drive in order for uninstallation to work properly.

Uninstallation Prerequisites

Before uninstalling the master:

Step 1 Stop all TES components.

Step 2 Exit all Tidal Web clients by choosing **File > Exit** from the menu for each Tidal Web client that is running.

Step 3 Stop the master:

a. From the Windows Start menu, choose **Programs > TIDAL Software > TIDAL Service Manager.**

b. From the Service list, choose **Scheduler Master**.

c. Click **Stop**; the light turns green when the master has stopped.

Once TES components have been stopped, you can begin the uninstallation process.

Uninstallation Procedure

The TES master is uninstalled from the Windows Control Panel.

To uninstall:

Step 1 From the Windows Start menu, choose **Control Panel**, then double-click **Add** or **Remove Programs**.

Step 2 Scroll down the list of programs installed on the machine to the Tidal Scheduler program.

Step 3 Click the Tidal Scheduler program to highlight it.

Step 4 Click **Remove** to start the uninstallation process. A confirmation message displays.

Note SNMP services are momentarily stopped when uninstalling the SNMP extension agent. They are restarted when uninstallation is complete.

Step 5 Click **OK** to uninstall. The Preparing Setup panel displays showing a progress bar. When the progress bar reaches 100%, a Scheduler confirmation dialog box displays.

Note On occasion, the master service may not be fully stopped even though the Service Manager says the master has stopped. Uninstalling the master before the master service completely stops displays an error message “Unable to stop service completely.” This message displays when the machine is unable to stop the master service quickly due to the volume of processes. Click **OK** to close the error message dialog box and wait while the machine catches up to complete the uninstallation process. When the uninstallation process finally completes, verify that all files were deleted from the location where the master files resided.

Warning **Do not cancel the uninstallation process once it begins or the uninstallation program will not be able to find its files the next time you attempt to uninstall. If you do cancel the uninstall, you will need to contact Technical Services.**

Note During uninstallation, a dialog box may display indicating that some files are locked because they are shared by other applications. Ignore the locked files and continue with the uninstallation.

Step 6 Click **OK** to finish.

Step 7 Repeat to remove other components.

Note If a Client Manager resides on the same machine as the master, the Client Manager must be uninstalled if the master is uninstalled.

Step 8 Once you complete uninstalling components, reboot the machine to clear the registry.

Note If you do not reboot after uninstallation(s), any subsequent installation may fail.

Some files or folders under the TES folder that were created after the installation might not be removed. You may want to manually delete these files and folders. The log file and the database created during installation remain and must be removed in separate procedures

Configuring the JVM Manually

To configure the JVM manually:

Step 1 Stop the master using the Tidal Service Manager.

a. From the Windows Start menu on the master machine, choose **Programs > TIDAL Software > TIDAL Service Manager** to display the **Tidal Service Manager**.

b. From the Service list, select **Scheduler Master**. The master status displays at the bottom of the dialog box.

c. Click **Stop** to stop the master. (The bottom of the dialog box displays “Scheduler Master: Stopped”.)

Step 2 Open the Windows Registry Editor.

Step 3 Locate the **HKEY_LOCAL_MACHINE Software > TIDAL Software > Scheduler** key in the Registry.

Step 4 Locate the JvmVersion value. The value should be 1.7. If there is no value, double-click the value to display its String Editor dialog box.

Note Run “path/to/java -version” to check the right version.

Step 5 Enter **1.7**, then click **OK** to close the dialog box and Registry.

Step 6 From the Tidal Service Manager, restart the master.

a. From the Windows Start menu on the master machine, choose **Programs > TIDAL Software > Scheduler > Master > Service Control Manager** to display the **Tidal Service Manager**.

b. From the Service scroll-down menu, choose **Scheduler Master**. The master status displays at the bottom of the dialog box.

c. Click **Start**.

Installing the Master for Unix

You can run TES on Unix by installing the Unix versions of the master and agent software. The current Unix version of the TES master only works with an Oracle database.

There are two methods to install the Unix version of the TES master:

- Installation Program (see "Installing the Unix Master".)
- Manually - From the command line as described in "Installing the Master for Unix from the Command Line". Before installing the Unix master from the command line, you must manually create the Oracle schema.

The master is installed with default parameters that provide most users with optimum performance, but individual circumstances may require reconfiguring the master parameters after installation. These parameters are managed in a *master.props* file residing on the master machine. Refer to "Configuring the Master" for information on modifying the main master properties.

Installation Prerequisites

The following requirements must be met prior to installation of the Unix master:

- One of the following Unix operating systems and JVM:
  - Solaris 2.9 or 2.10 (Sparc) with Sun JVM 1.7
  - Hewlett-Packard 11i(RISC) with Sun JVM 1.7 (must be using the most current patches) Hewlett-Packard 11i v1 or v2 (Itanium) with Sun JVM 1.7 (must be using the most current patches)
  - AIX 5.3 TL 5,6,9,10,6.1 with IBM JVM 1.7.
  - Linux Redhat Enterprise Server v4,v5 Intel (x86) kernel 2.2.14+– Sun JVM 1.7
  - Linux SUSE Enterprise Server v10,v11 Intel (x86) kernel 2.2.14+–Sun JVM 1.7
  - Java 1.7
- A user account created to own, control and install the Unix master files under. This user does not have to be root although whoever creates the user must be root.
- 300 MB of disk space for the product and its logs
- Installation from an X Windows terminal, either local or remote
- Master machine requires at least 2 Gig of RAM (The use of any TES adapters requires an additional 1 GB.) and dual 500 MHz processors dedicated to TES needs
- Oracle 10g or 11i database instance already installed and running

- Create a 'tidal' user on the unix box for use when installing the master.
- You should have your DBA available during installation to provide database configuration information.
- Apply all patches supplied in the latest hotfix for TES 6.2.

Note Only one master can be installed on a machine. TES cannot operate correctly if two masters are installed on the same machine.

Installing the Unix Master

To install the Unix master:

Step 1 Copy *install.bin* to the target machine.

Step 2 Change the permissions on the copied *install.bin* file to make the file executable by entering:

chmod 755 install.bin

Step 3 After copying the file to the directory, begin the installation program by entering:

sh ./install.bin

When the installation program starts, the installation splash screen displays, and the **Introduction** panel follows.

Step 4 After reading the introductory text that explains how to cancel the installation or modify a previous entry on a previous screen, click **Next**.

Step 5 On the Choose Installation Folder panel, enter the directory path to the location where you wish to install the master files or click **Choose** to browse through the directory tree to the desired directory.

Step 6 Click **Next**. The Select Appropriate Master panel displays.

Note The master machines, both primary and backup, must have mirror configurations, meaning that both machines must use the same version of operating system and JVM for fault tolerance to operate correctly.

Step 7 Select whether you are installing a primary or backup master.

The only instance you would select the **Backup** option is if you are installing fault tolerance, which requires a special license. If you are installing fault tolerance, install the primary master before you install the backup master.

Step 8 Click **Next**. The Select Admiral Database Creation Option panel displays.

Step 9 Select **Automatic** or **Manual**.

TES requires its own database to store job information. The installation program will create the database automatically unless you select the **Manual** option. The automatic database creation process creates a schema called 'tidal' and three tablespaces:

- ADMIRAL_DATA
- ADMIRAL_INDEX
- ADMIRAL_TEMP

If the schema name or any of the names of the tablespaces is used already, the installation will fail.

Step 10 Click **Next**. The Enter DBA UserName and Password dialog box displays.

TES must be able to access the Oracle database. You must provide the user name and password required to access the database. Your DBA can provide this information. The DBA user name is usually the 'system' user. The specified database user will create the 'tidal' schema and its three tablespaces.

Step 11 Click **Next**. The JDBC Driver Information panel displays.

Step 12 Provide the following information so the Unix master can connect to the database:

- **Database Hostname**—Name of the computer that hosts the database

Note The master should not be installed on hosts with underscores in their names or the JMS connections will fail between components.

- **Port Number**—Port number to connect to the database
- **SID**—Name of the Oracle database instance

Note The SID is case-sensitive.

Step 13 Click **Next**. The Test JDBC Connection panel displays.

Step 14 Click **Test JDBC Connection** to verify that the information configuring the database connection is correct. The installation program must be able to connect to the database before the installation can continue.

Note If the connection to the database cannot be established, an error message displays explaining what needs to be fixed. If the database cannot be accessed you must resolve the issue before proceeding with the installation SID is case-sensitive.

When the program accesses the database, a "Connection Successful" message displays.

Step 15 Click **Next**. The Admiral Tablespace Installation panel displays.

Step 16 Specify the location for the Oracle tablespace directories to be created.

- To use any location other than the default location, enter the directory paths to the ADMIRAL_DATA, ADMIRAL_INDEX and ADMIRAL_TEMP tablespaces. Do not change the actual datafile names. Change only the directory paths.
- If your database is on a Windows platform, be sure to use Windows pathname syntax (for example, *C:\Program Files\Microsoft SQL Server\MSSQL\Data*).
- If your database is on the Unix platform, use the proper Unix directory syntax (for example, */opt/oracle/oradata/Admiral/ADMIRAL_DATA*).

Step 17 Click **Next**. The Master Host Name panel displays.

Step 18 Enter the hostname (or machine name) of the machine that you are installing the Unix master on. Do not use the domain name.

Step 19 Click **Next**. The SNMP Information panel displays.

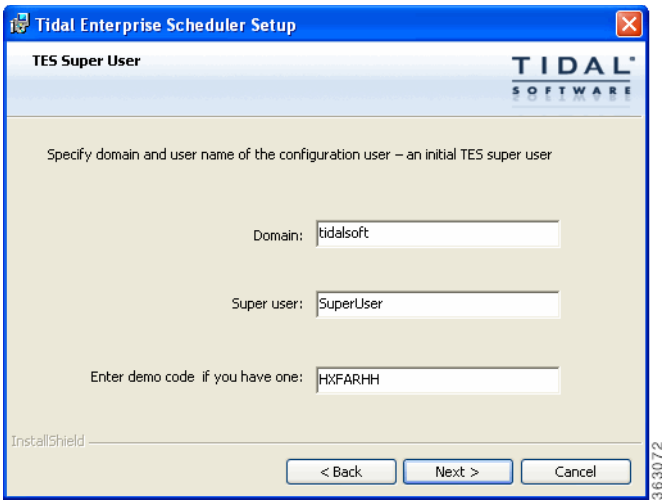
Step 20 Enter the name of the SNMP server machine.

If you want to use SNMP to send traps in TES, you must tell the Unix master how to connect to the SNMP server.

Step 21 Enter the port number of the SNMP server machine. The default port number is **162**. This information can be changed later if necessary.

Step 22 Click **Next** to continue the installation or to skip this step if you are not using SNMP traps. The TES SuperUser panel displays.

Figure 3-1 TES SUPERUSER panel



Step 23 Enter the domain name of the initial TES configuration Super User.

Step 24 Enter the name of the initial TES configuration Super User.

Step 25 If you have a Demo license, enter the license number, then click **Next**. The Pre-Installation Summary panel displays.

This screen summarizes the information entered during the installation procedure.

Step 26 Review the information to ensure it is correct.

Step 27 If any information is incorrect, retrace your steps and correct the information by clicking **Previous** until you reach the desired screen.

-or-

If the information is correct, click **Install** to start the installation of the Unix master files.

After the installation process completes, a screen provides a database status report. This report lists the various steps during the creation of the database and if the step was successful.

Step 28 Review the database report for any error notices.

Step 29 If the database was created without any errors, click **Next**.

-or-

If the report displays any errors during database creation, note the errors. You can correct the errors later by manually creating the database. Click **Next**.

Once installation is complete, the Installation Complete panel displays.

Step 30 Click **Done** to exit the installer.

Verifying Successful Installation

You should verify that the installation program installed all of the required files.

Verify that all of master files were installed by going to the directory location that you designated during installation and listing the directory contents with the following command:

ls -lF

The seven main file directories (not counting the *UninstallerData* directory) are listed at the top with the contents of the *bin*, *lib* and *config* directories also displayed.

Installing the Master for Unix from the Command Line

The Unix master can be installed using the installer program or by installing it from the command line.

To install from the command line:

Step 1 Copy *install.bin* to the target machine.

Step 2 Change the permissions on the *install.bin* file in the directory to make the file executable:

chmod 755 install.bin

Step 3 Open a command prompt window and enter:

 # sh ./install.bin -i console

Step 4 Press **Enter**. The following screen displays as the installation program begins.

Figure 3-2 Launching Installer Screen

```
Launching installer...

Preparing CONSOLE Mode Installation...

===============================================================================
ClientManager                     (created with InstallAnywhere by Macrovision)
-------------------------------------------------------------------------------
```

363080

The initial installation screen is followed with the Introduction screen that provides instruction for proceeding with the installation program.

Figure 3-3 Introduction Screen

```
===============================================================================
Introduction
------------

InstallAnywhere will guide you through the installation of ClientManager.

It is strongly recommended that you quit all programs before continuing with
this installation.

Respond to each prompt to proceed to the next step in the installation.  If you
want to change something on a previous step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE:

===============================================================================
```

363081

Step 5 Press **Enter**. The Choose Install Folder screen displays.

Step 6 Enter the directory path where the master files should be installed. It is recommended that you use the default directory path when installing.

Step 7 Press **Enter**. The Select Master Type screen displays.

Figure 3-4 Select Master Type Screen

```
==============================================================================
Select Master Type
------------------

Install the Primary master before installing the Backup master.


  ->1- Primary
    2- Backup

Type 1 or 2:
```

363084

Step 8 Select whether you are installing a primary or backup master.

Select the **Primary** option by entering **1** at the prompt.

-or-

Select the **Backup** option by entering 2 at the prompt if you are installing fault tolerance, which requires a special license. (If you are using fault tolerance, be sure to install the primary master before you install the backup master. Refer to the *Cisco Tidal Enterprise Scheduler Installation Guide* for more information on installing fault tolerance.)

Step 9 Press **Enter**. The JDBC Driver screen displays.

Step 10 Supply the following information so the Unix master can connect to the database:

- Database HostName – Enter the hostname of the database server.
- Port – Enter the port number of the JDBC driver. The default port is 1433.
- SID – Enter the Oracle System ID (Oracle only).

Step 11 Press **Enter**. The Master Hostname screen displays.

Figure 3-5 Master Hostname Screen

```
==============================================================================
Enter the hostname of the machine where you are installing the master.
------------------------------------------------------------------------------

Master Hostname:
```

363091

Step 12 Type the name of the machine where you are installing the master.

Note Do not include the domain name. If you are installing fault tolerance, this screen does not display when installing the backup master.

Step 13 Press **Enter**. The SNMP Information screen displays.

Figure 3-6 SNMP Information Screen

```
==============================================================================
Enter SNMP information to be used by the master. If you do not have the required
 information you can enter the information after the installation is finished.
------------------------------------------------------------------------------
------------------------------------------------------------------------------

SNMP Server Machine Name:
SNMP Trap Listener Port:
```

363087

If you want to use the email function in TES, you must tell the Unix master how to connect to the SNMP server. (The default SNMP port number is **162**.) This information can be changed later in the *master.props* file, if necessary.

Note To bypass this screen, press **Enter**.

Step 14 Enter the following information:

- **SNMP Server Machine Name**—name of the SNMP server machine
- **SNMP Trap Listener Port**—Enter the name of the SNMP trap listener port.

Step 15 Press **Enter**. The TES SuperUser screen displays.

Figure 3-7 TES SuperUser Screen

```
==========================================================================
TES SUPERUSER
-------------

Please the User Name of initial TES configuration User, TES SuperUser
Domain: (DEFAULT: ):
SuperUser: (DEFAULT: ):
```

363093

Step 16 Enter the domain name of the initial TES configuration Super User, then press **Enter**.

Step 17 Enter the name of the initial TES configuration Super User, then press **Enter**. The Pre-Installation Summary screen displays.

Step 18 Review the accuracy of the information.

Step 19 Press **Enter** to begin the installation.

-or-

If any of the information is incorrect, you can type **QUIT** to cancel the installation or you can continue with the installation and make corrections in the *master.props* configuration file.

The Installing screen displays.

Once installation is complete, the Installation Complete screen displays.

Step 20 Press **Enter** to exit the installer.

Step 21 Verify successful installation of the master files by following the procedure described in "Verifying Successful Installation".

Note If you are installing the Unix master from the command line, you must also manually install the database as a separate procedure. This procedure is described in the following section.

Updating Oracle Schema Manually

Although it is recommended that the installation process create the master database for Oracle, users can create the Oracle schema manually. If you are installing the Unix master from the command-line then you must first create the Oracle schema manually. Have your Oracle DBA perform the following procedures.

To update the Oracle schema manually:

Step 1 Locate the *connectdb.sql* script within the *sql* directory.

Step 2 Edit the following parameters in this script:.

Note For debugging purposes, you can run a spool file as you run the installation script.

- **create tablespace admiral_data datafile 'ADMIRAL_DATA' size 200m reuse autoextend on;**
- **create tablespace admiral_index datafile 'ADMIRAL_INDEX' size 100m reuse autoextend on;**
- **create temporary tablespace admiral_temp datafile 'ADMIRAL_TEMP' size 200M reuse;**
- **`create user tidal identified by <call Technical Services for password> default tablespace admiral_data quota unlimited on admiral_data quota unlimited on admiral_index temporary tablespace admiral_temp`**;

  (Contact Technical Services for the password to enter in the brackets < >.)
- **`grant create session, create table to tidal; connect tidal/<call Technical Services for password>@ <tnsname>`**;

  (Contact Technical Services for the password to enter in the brackets < >. Replace the string "tnsname" at the end of the **CONNECT** statement with the real TNSName that is used to connect to the Oracle database.)

Note If you wish to install the datafiles in a specific directory, the Oracle DBA can change the `CREATE TABLESPACE` statements to specify a different directory location for the datafiles. The datafile growth options may also be modified if desired. Do not lower the default SIZE values.

Step 3 Enter the information you received from Technical Services in the appropriate brackets in the *connectdb.sql* script.

Step 4 Save the script.

Step 5 Locate the *orapopulate.sql* script within the *sql* directory.

Step 6 Find the following statement and change **`DOMAINNAME`** and **`SUPERUSERNAME`** to be the domain and user name of the initial super user account:

insert into usrmst (usrmst_id, usrmst_domain, usrmst_name, usrmst_fullname, usrmst_desc, usrmst_phoneno, usrmst_pagerno, usrmst_email, usrmst_emailtype, secmst_id, lngmst_id, usrmst_password, usrmst_suser) values (1, DOMAINNAME, 'SUPERUSERNAME', 'SUPERUSERNAME', null, null, null, null, null, 6, 1, null, 'Y');

Note **DOMAINNAME** can be null. If it is not null, be sure to add single quotes around the domain name in the sql statement. Your Oracle TES database should now be installed.

Step 7 Save the script.

Step 8 Login as the SYSTEM user (or equivalent).

Step 9 Run the *connectdb.sql* script to create a user called *tidal* and to create the database tablespaces. Run the following scripts as the tidal user you just created.

a. Run the *adoracle.sql* script and if there are no errors issue a commit; statement.

b. Run the *orapopulate.sql* script and if there are no errors issue a commit; statement.

c. Run the *nodmst.sql* script and if there are no errors issue a commit; statement.

Your Oracle TES database should now be installed. If any errors occurred when running those scripts, do not continue. Collect as much information on the errors as possible and contact either the consultant assisting your installation or Technical Services at Cisco.

Controlling the Unix Master

Control the Unix master from the command line using tesm command as described in the following table:

Command	Description
tesm start	Starts the Unix master.
tesm stop	Stops the Unix master.
tesm status	Checks the status of the Unix master. If the master is not running, a message displays that the server is stopped or paused. If the server is running, the command line will not only indicate the status and details the specifications and versions of the system software used with the Unix master. For example: **Server is running** **TIDAL Product Name: TIDAL TES for Unix** **TIDAL Product Version: 6.2.0** **TIDAL Home Directory: /u01/buildersa/TIDAL/master/bin/..** **Operating system name: AIX** **Operating system architecture: ppc64** **Operating system version: 6.2** **User's account name: builder** **User's home directory: /home/builder** **Java Runtime Environment Version: 1.7** **Java Runtime Environment vendor: IBM Corporation** **Java installation directory: /usr/java13_64/jre** **Java Virtual Machine specification version: 1.0** **Java Virtual Machine specification vendor: Sun Microsystems Inc.** **Java Virtual Machine implementation version: 1.7**
	Java Virtual Machine implementation vendor: IBM Corporation **Java Virtual Machine implementation name: Classic VM** **Java Runtime Environment specification version: 1.7** **Java class path: /u01/buildersa/TIDAL/master/bin/../lib/Scheduler.jar**
tesm version	Checks the version of the Unix master.

Note **./** may not be required on some systems. Consult your system administrator to determine how the commands should be used.

Using the Command Line

You can use the command line to directly access the Unix master but you can only access it from the machine that the Unix master is installed on. (You do not need to provide the name of the machine in the command.) You can use single or multiple-command mode when entering commands.

Uninstalling the Unix Master

There are two ways to uninstall the master. The first is done using the contents of the *Uninstaller* folder. The second is done through the command line. Use the method you are most comfortable with.

Uninstalling From the Uninstaller Folder

The uninstallation procedure will not be successful if attempted while the master is running. You must stop the Unix master before you can remove it.

To uninstall from the *Uninstaller* folder:

Step 1 Check the status of the master to see if it is running, by entering:

./tesm status

Step 2 If the status check shows the master is not running, proceed to the next step. If the status check shows the master is running, stop the master by entering:

./tesm stop

Step 3 Once the master is stopped, use the Unix file manager to locate the uninstaller folder called *UninstallerData*.

Step 4 From the *UninstallerData* folder, run *Uninstall_UnixMaster*. The Uninstall Master panel displays.

Step 5 Click **Uninstall**. A status panel is displayed to illustrate the progress of the uninstallation program.Once the uninstall is complete, the Uninstall Complete panel displays.

The Unix master is now uninstalled. Any files that were created after the master is installed are not removed. Files that were not removed must be manually removed.

Step 6 Click **Done** to exit.

Note The uninstallation program only removes the Client Manager files installed at the time of installation. If you created other files in the master directory after installation, these files are not removed. You must manually delete these additional files.

Uninstalling Using the Command Line

The uninstallation procedure will not be successful if the master is running. Stop the master before beginning uninstallation.

To uninstall using the command line:

Step 1 Check the status of the master to verify that it is not running by entering:

./tesm status

Step 2 If the status check shows the master is not running, proceed to the next step. If the status check shows the master is running, stop the master by entering:

./tesm stop

Step 3 Once the master is stopped, return to the master directory.

Have your Unix administrator remove the master directory and its contents.

Installing Client Manager

This chapter outlines the installation procedure for installing Client Manager.

Two main components of the TES architecture are the Master and Client Manager. The Client Manager allows TES to achieve higher performance and scalability needs. Its purpose is to service requests from user-initiated activities, such as through the Tidal Web Client, Tidal Transporter and from other external sources that utilize the Command Line Interface (CLI) or published TES Web services. Client Manager allows the TES master to focus more capacity on core scheduling needs related to job execution and job compilations, while the Client Manager addresses demands from activities such as users viewing/configuring scheduling data and output. A single Client Manager is mandatory and additional Client Managers can be deployed to address additional performance needs.

Note With TES version 6.2.0, you can deploy a stand-alone TES cache database (MSSQL 2005, 2008, 2012 or Oracle 11gR2), as opposed to using the default embedded cache database (Derby). Having a stand-alone cache database allows for faster synchronization time upon Client Manager startup. Additionally, a stand-alone cache database improves the overall UI experience by offering faster filtering and scrolling response times.

Installation Prerequisites

For Unix

- *install.bin* files
- TES Unix master installed and configured as described in this guide
- Apply all patches supplied in the latest hotfix for TES 6.2.

For Windows

- *setup.exe*
- Apply all patches supplied in the latest hotfix for TES 6.2.

Compatibility Matrix

	Platform				Minimum System Requirements (Dedicated Server)			
	OS Name	**Version**	**Chipset**	**64-bit**	**JVM**	**Processor**	**RAM**	**Disk**
Client Manager **Web Service API runs against this platform**	HPUX	11.23,11.31	Itanium	X	HP 1.7	Dual Processor 1GHz	8GB for Client Manager	2GB/SCSI 10,000RPM
	Solaris	9,10	Sparc	X	Sun 1.7	Dual Processor 1GHz	8GB for Client Manager	2GB/SCSI 10,000RPM
	Solaris	10	Opteron	X	Sun 1.7	Xeon Quad 2GHz	8GB for Client Manager	2GB/SCSI 10,000RPM
	AIX	5.3,6.1	RISC & PPC	X	IBM 1.7	Dual Processor 500MHz	8GB for Client Manager	2GB/SCSI 10,000RPM
	Windows	2003 (Standard SP1+, Enterprise SP1+)	Intel x86 /AMD	X	Intel x86/AMD: Sun 1.7	Xeon Quad 2GHz	8GB for Client Manager	2GB/SCSI 10,000RPM
	Windows	Server 2008	Intel/AMD	X	Sun 1.7	Xeon Quad 2GHz	8GB for Client Manager	2GB/SCSI 10,000RPM
	Linux	Redhat Enterprise Server v4,v5 Cent OS v4, v5	Intel/AMD	X	Sun 1.7	Xeon Quad 2GHz	8GB for Client Manager	2GB/SCSI 10,000RPM
	Linux	SUSE Enterprise Server v10,v11	Intel/AMD	X	Sun 1.7	Xeon Quad 2GHz	8GB for Client Manager	2GB/SCSI 10,000RPM
	Linux	Oracle Enterprise Linux 5.2	Intel/AMD	X	Sun 1.7	Xeon Quad 2GHz	8GB for Client Manager	2GB/SCSI 10,000RPM
	VMWare ESX on UCS	ESXi 4.0 U1	UCS: B250 M1, C250 M1, B200 M1, B200 M2, B250 M2, C200 M1, C210 M1					

	Platform				Minimum System Requirements (Dedicated Server)		
	VMWare ESX on UCS	ESX 3.5 U5	UCS: B250 M1, C250 M1, B200 M1, B250 M2, C200 M1, C210 M1				

Warning **It is recommended that no more than five agents be run on the minimum hardware platform. However, the number of agents that can be run on a given server depends upon the CPU and memory resources available on the machine. Add a single agent at a time and gauge the effect of each added agent on system performance before adding more. You have to experiment with the configuration to achieve optimal results.**

Before You Begin

- Obtain machine names, host names, port numbers and IP addresses before beginning the installation.
- Ensure that each computer used for TES can communicate with the other machines on the network. If you cannot ping to and from each component machine, TES cannot function properly. Network conditions affect the operation of TES.
- Ensure that you are logged on with an account that has Administrator privileges.
- Review any supplementary documentation provided with your software.
- Exit all Windows programs before running any installation.
- Contact Support if you have any questions.

Installation Procedures

If the minimum system requirements have been met, Client Manager can be installed on the same machine as the master. Before installing Client Manager:

- install and configure a TES Windows/Unix master
- install JDK version 1.7 on the Client Manager machine

Installing Client Manager for Windows

To install Client Manager:

Step 1 Transfer the appropriate installation files to the target machine (binary mode).

Step 2 Double-click *setup.exe*. The Security Warning dialog box displays.

Step 3 Click **Run**. The Internet Explorer-Security Warning dialog box displays.

Step 4 Click **Run**. The InstallShield Wizard Welcome dialog box displays.

Step 5 Click **Next**. The Destination Folder panel displays.

Step 6 Select the directory where the TES files will reside.

- Click **Change** to search for a directory.

  -or-

- Accept the default location *C:\Program Files*.

Step 7 Click **Next**. The TES DSP Name and Master IP panel displays.

Step 8 In the **TES DSP NAME** field, enter the name of your Data Source (TES 6.2) Plug-in.

This value can be anything you want it to be. The default is `tes-6.2`.

Note Architecturally, the Client Manager is written to be a generic container of plug-ins and is not TES-specific. The TES-specific parts of the UI are in TES plugin.

Step 9 In the Primary Server IP field, enter the host name or IP address for your primary master. The default port is **6215**.

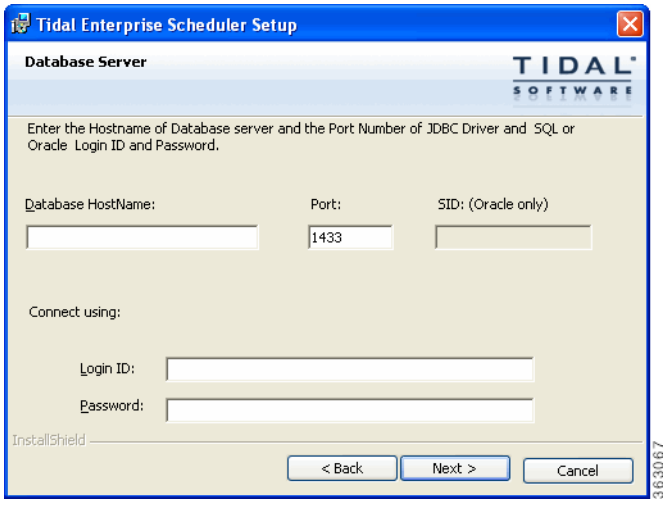
Step 10 If using Fault Tolerance, in the Backup Server IP field, enter the IP address for your backup master.

Step 11 Click **Next**. The Cache Database Server panel displays.

By default, Internal Cache DB server is selected. Alternatively, external DB servers may be provisioned to run Cache Database.

Step 12 Click **Next**. The Database Server Credentials panel displays if you selected an external database server.

Figure 4-1 Database Server Credentials Panel

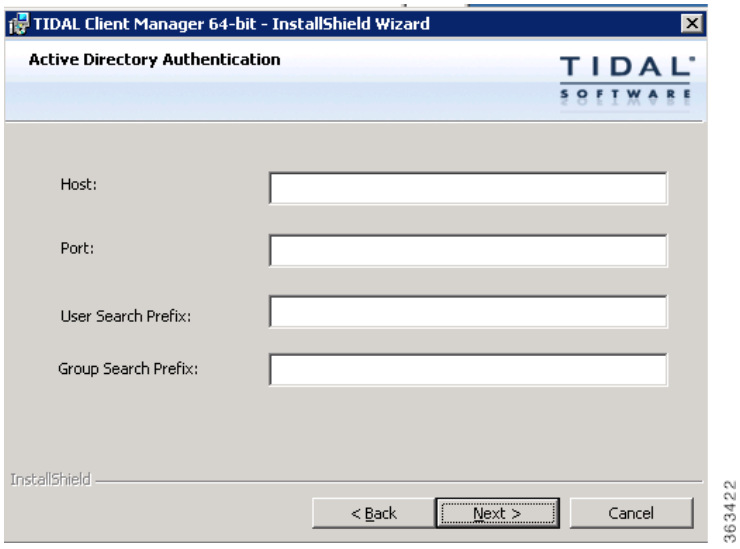


Step 13 Enter the credentials for the selected external database, then click **Next**. The Active Directory/LDAP Authentication panel displays.

Step 14 Select an option, then click **Next**.

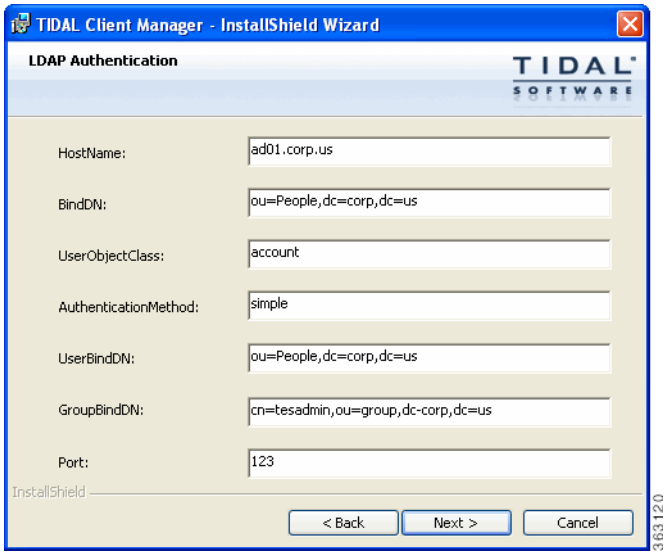
If configuring the Client Manager to use the Active Directory option, the Active Directory Authentication panel displays.

Figure 4-2 Active Directory Authentication Panel



If configuring the Client Manager to use the LDAP option, the LDAP Authentication panel displays.

Figure 4-3 LDAP Authentication Panel



Step 15 For Active Directory, enter the following information:

- Host – Enter the hostname or IP address for the Active Directory server.
- User Search Prefix – Enter the location you want Active Directory to search for users.
- Group Search Prefix – Enter the location you want Active Directory to search for groups.
- Port – Enter the port number for the AD server.

-or-

For LDAP, enter the following information:

- Hostname – Enter the hostname or IP address for the LDAP server.
- Port – Enter the port number for the LDAP server.
- BindDN – Enter the user account to query the LDAP server.
- UserObjectClass – Specify a valid object class for the BindDB user. Only users who posses one or more of these objectClasses will be permitted to authenticate.
- UserBindDN – Enter the user account to query the LDAP server.
- User-role based access for Oracle/Sun Directory Server – Select this option if your TES 6.2 Web Client user authentication is defined to use Oracle/Sun Directory Server with role-based access.
- GroupBindDN – Enter the group account to query the LDAP server.

Example of an AD Setting

```
Security.Authentication=ActiveDirectory
ActiveDirectory.Host=sjc-ad-1
ActiveDirectory.Port=389
ActiveDirectory.UserSearchPrefix=DC=tidalsoft,DC=local
ActiveDirectory.GroupSearchPrefix=DC=tidalsoft,DC-local
```

Example of an LDAP Setting

```
Security.Authentication=LDAP
LDAP.HostName=172.25.6.xxx
LDAP.Port=389
LDAP.BindDN=ou=people,dc=tidalsoft,dc=local
LDAP.UserObjectClass=inetOrgPerson
LDAP.ContextFactory=com.sun.jndi.ldap.LdapCtxFactory
LDAP.AuthenticationMethod=simple
LDAP.UserBindDN=dc=tidalsoft,dc=local
LDAP.GroupBindDN=dc=tidalsoft,dc=local
```

Note TES 6.2 allows for multiple-domain user authentication for CM. The purpose of this function is to allow users defined in different domains to be authenticated within one CM configuration to avoid installing one CM per domain limitation.

To enable this function:

1. Add the following new property value in *clientmgr.props*, located under *<CM_INSTALL>\config*.

Security.Authentication.Ext.File=user-auth.xml

Where **user-auth.xml** is the file name.

2.Build the user-auth.xml file to include all AD/LDAP servers for TES user authentication.

```
<ext-user-auth>
<user-auth>
<name>TIDALSOFT</name>
<desc>Configure AD for user user authentication</desc>
<type>ActiveDirectory</type>
<host>hou-ad-1.tidalsoft.local</host>
<port>389</port>
<ad.usersearchprefix>DC=tidalsoft,DC=local</ad.usersearchprefix>
<ad.groupsearchprefix>DC=tidalsoft,DC=local</ad.groupsearchprefix>
</user-auth>
<user-auth>
<name>ITTIDAL</name>
<desc>Configure Open LDAP Server for user authentication</desc>
<type>LDAP</type>
<host>10.88.103.148</host>
<port>5389</port>
<ldap.binddn>ou=People,dc=ittidal,dc=com</ldap.binddn>
<ldap.userobjectclass>account</ldap.userobjectclass>
<ldap.userbinddn>dc=ittidal,dc=com</ldap.userbinddn>
```

<ldap.groupbinddn>cn=testest,ou=Group,dc=ittidal,dc=com</ldap.groupbinddn>
<ldap.useridentifiertype>uid</ldap.useridentifiertype>
</user-auth>
</ext-user-auth>

In the above example, the authentication process will validate **tidalsoft** first and then **ittidal**.

Step 16 Click **Next**. The Ready to Install the Program panel displays.

Step 17 Click **Install**. The Installing Tidal Client Manager panel displays.

Step 18 If any information is incorrect, retrace your steps and correct the information by clicking **Back** until you reach the desired screen.

-or-

If the information is correct, click **Install** to start the installation of the Client Manager files.

The Installing Tidal Client Manager panel displays. The status of your client installation displays with a progress bar.

Caution Do not click **Cancel** once the installation process begins copying files in the Setup Status dialog box. Cancelling the installation at this point corrupts the installation program.You will not be able to install the component without the help of support. If you decide you do not want to install the component, complete the installation and then uninstall.

Step 19 The Setup Completed panel displays.

Step 20 Click **Finish**.

Note Before starting the Client Manager, be sure to apply the latest hotfix obtained from cisco.com. To ensure compatibility, apply the latest 6.2 hotfix patches to the Master and other components, each time the hotfix patches are applied to the CM. The first time the Client Manager is started, it initializes its data from the master. Depending upon the amount of data, this could take up to 20 minutes.

Verifying Successful Installation

You should verify that the installation program installed all of the required files.

Verify that Client Manager files were installed by going to the directory location that you designated during installation.

The seven main file directories (not counting the *UninstallerData* directory) are listed at the top with the contents of the *lib* and *config* directories also displayed.

Note Watch for the primary and secondary sync in cliengmanager\log\clientmgr.out. Completion of the primary sync indicates that the client can be logged into, but all data has not been loaded yet. Please wait until the secondary sync is complete to properly view all jobs and information.

Installing Client Manager for Unix

To install Client Manager for Unix:

Step 1 Copy *install.bin* to the target machine.

Step 2 Change the permissions on the copied *install.bin* file to make the file executable by entering:

chmod 755 install.bin

Step 3 After copying the file to the directory, begin the installation program by entering:

sh ./install.bin

When the installation program starts, the installation splash screen displays.

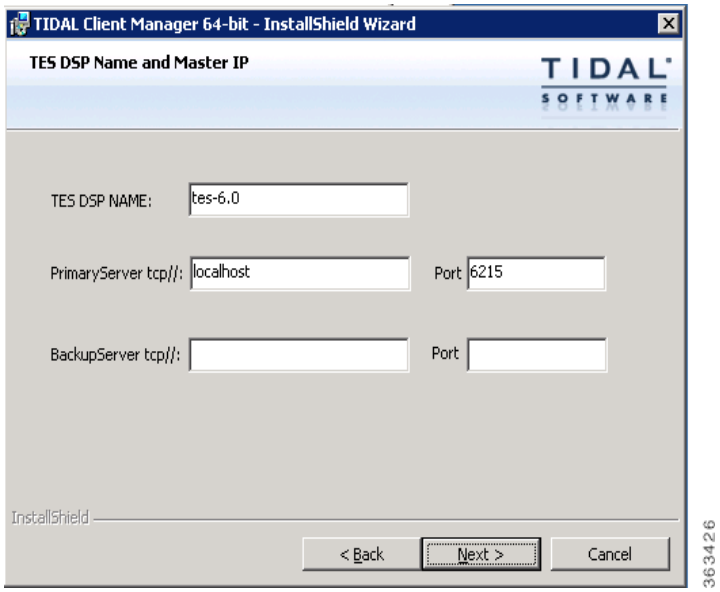
The Introduction panel follows.

Step 4 After reading the introductory text that explains how to cancel the installation or modify a previous entry on a previous screen, click **Next**. The Choose Installation Folder panel displays.

Step 5 Enter the directory path to the location where you wish to install the master files or click **Choose** to browse through the directory tree to the desired directory.

Step 6 Click **Next**. The TES DSP Name and master IP panel displays.

Figure 4-4 TES DSP Name and master IP Panel



Step 7 In **TES DSP NAME** field, enter the name of your Data Source (TES 6.2) Plug-in.

This value can be anything you want it to be. The default is `tes-6.2`.

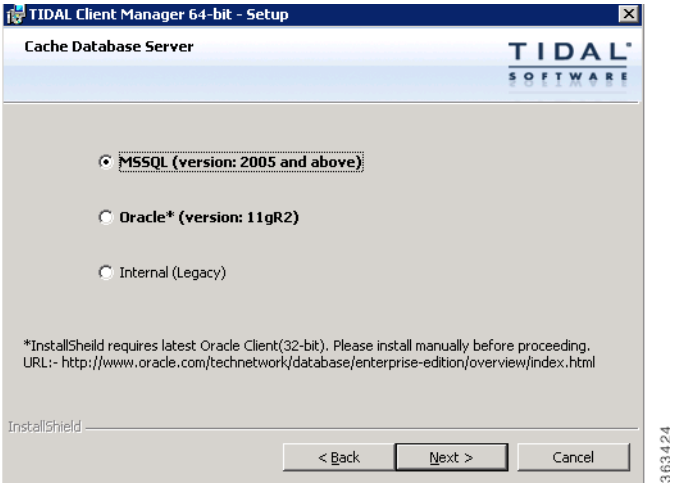
Note Architecturally, the Client Manager is written to be a generic container of plug-ins and is not TES-specific. The TES-specific parts of the UI are in TES plugin.

Step 8 Enter the following details:

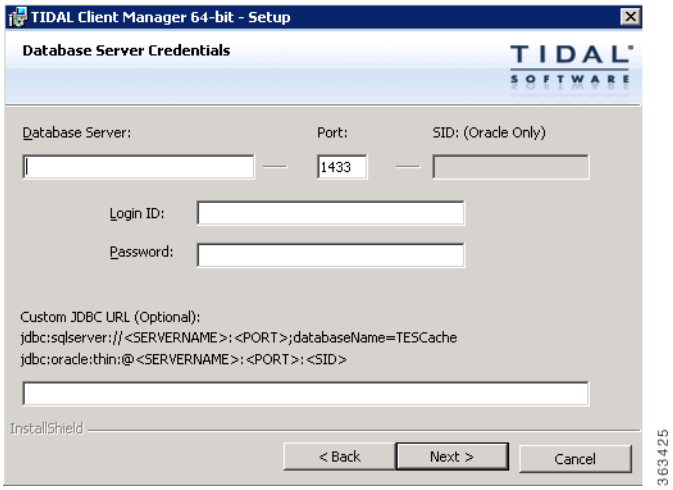
- **Primary Server IP**—Enter the host name or IP address for your primary master. The default port is **6215**.

- **Backup Server IP**— If using Fault Tolerance, enter the IP address for your backup master.

Step 9 Click **Next**. The Cache Database Server panel displays.



Step 10 Click **Next**. The Database Server Credentials panel displays.



Step 11 Enter the required authentication information, then click **Next**. The Active Directory/LDAP Authentication panel displays. See also, "Note" on page 4-7.

Step 12 Select an option, then click **Next**.

If configuring the Client Manager to use the Active Directory option, the Active Directory Authentication panel displays. If configuring the Client Manager to use the LDAP option, the LDAP Authentication panel displays.

Step 13 For Active Directory, enter the following information:

- **Host** – Enter the hostname or IP address for the Active Directory server.
- **User Search Prefix** – Enter the location you want Active Directory to search for users.
- **Group Search Prefix** – Enter the location you want Active Directory to search for groups.
- **Port** – Enter the port number for the AD server.

-or-

For LDAP, enter the following information:

- **Hostname** – Enter the hostname or IP address for the LDAP server.
- **Port** – Enter the port number for the LDAP server.
- **BindDN** – Enter the user account to query the LDAP server.
- **UserObjectClass** – Specify a valid object class for the BindDB user. Only users who posses one or more of these objectClasses will be permitted to authenticate.
- **UserBindDN** – Enter the user account to query the LDAP server.
- **User-role based access for Oracle/Sun Directory Server** – Select this option if your TES Web Client user authentication is defined to use Oracle/Sun Directory Server with role-based access.
- **GroupBindDN** – Enter the group account to query the LDAP server.

Step 14 Click **Next**. The Pre-Installation Summary panel displays.

This screen summarizes the information entered during the installation procedure.

Step 15 Review the information to ensure it is correct.

Step 16 If any information is incorrect, retrace your steps and correct the information by clicking **Previous** until you reach the desired screen.

-or-

If the information is correct, click **Install** to start the installation of the Client Manager files.

The Installing Tidal Client Manager panel displays.

The status of your installation is displayed with a progress bar. The Install Complete panel displays.

Step 17 Click **Done** to exit the installer.

Note The first time the Client Manager is started, it initializes its data from the master. Depending upon the amount of data, this could take up to 20 minutes.

Installing Client Manager from a Command Line

To install Client Master from a command line:

Step 1 Copy *install.bin* to the target machine.

Step 2 Change the permissions on the copied *install.bin* file to make the file executable by entering:

chmod 755 install.bin

Step 3 After copying the file to the directory, begin the installation program by entering:

sh ./install.bin -i console

The following screen displays as the installation program begins.

When the installation program starts, the Introduction screen displays.

Step 4 After reading the introductory text that explains how to cancel the installation or modify an previous entry on a previous screen, press **Enter**. The Choose Installation Folder screen displays.

Step 5 Enter the directory path to the location where you wish to install the Client Manager files, then press **Enter**.

Step 6 Verify the path you entered, then press **Enter**. The Get TES DSP Name and master IP screen displays.

Note The master machines, both primary and backup, must have mirror configurations, meaning that both machines must use the same version of operating system and JVM for fault tolerance to operate correctly.

Step 7 Enter the name of your Data Source (TES 6.2) Plug-in, then press **Enter**.

Step 8 Enter the host name or IP address for your primary master, then press **Enter**.

Step 9 Enter the port number for the primary master, then press **Enter**.

Step 10 Enter the host name or IP address for your backup master, then press **Enter**.

Step 11 Enter the port number for the backup master, then press **Enter**.

Step 12 If using Fault Tolerance, enter the IP address for your backup master, then press **Enter**. The Get Authentication Method screen displays.

Step 13 Enter **1** for the Active Directory option or **2** for the LDAP option, then press **Enter**.

Step 14 For Active Directory, enter the following information:

- Host – Enter the hostname or IP address for the Active Directory server.
- User Search Prefix – Enter the location you want Active Directory to search for users.
- Group Search Prefix – Enter the location you want Active Directory to search for groups.
- Port – Enter the port number for the AD server.

Note Contact your IT Administrator for Active Directory/LDAP authentication values.

-or-

For LDAP, enter the following information:

- Hostname – Enter the hostname or IP address for the LDAP server.
- Port – Enter the port number for the LDAP server.
- BindDN – Enter the user account to query the LDAP server.
- UserObjectClass – Specify a valid object class for the BindDB user. Only users who posses one or more of these objectClasses will be permitted to authenticate.
- UserBindDN – Enter the user account to query the LDAP server.
- User-role based access for Oracle/Sun Directory Server – Enter **1** for **Yes** if your TES Web Client user authentication is defined to use Oracle/Sun Directory Server with role-based access.

Step 15 Press **Enter**. The Pre-Installation Summary screen displays.

Step 16 Press **Enter**. The Installing screen displays.

Once installation is complete, the Installation Complete screen displays.

Step 17 Press **Enter** to exit the installer.

Verifying Successful Installation

You should verify that the installation program installed all of the required files.

Verify that Client Manager files were installed by going to the directory location that you designated during installation and listing the directory contents with the following command:

ls -lF

The seven main file directories (not counting the *UninstallerData* directory) are listed at the top with the contents of the *bin*, *lib* and *config* directories also displayed.

Starting and Stopping Client Manager

Starting and Stopping the Windows Client Manager

To start Client Manager:

Step 1 From the Windows Start menu on the master machine, choose **Programs > TIDAL Software > Scheduler > Master > Service Control Manager** to display the **Tidal Service Manager**.

Step 2 From the Service list, choose **Client Manager**. The Client Manager status displays at the bottom of the dialog box.

Step 3 Click **Start** to start the Client Manager.

To stop Client Manager:

Step 1 From the Windows Start menu on the master machine, choose **Programs > TIDAL Software > Scheduler > Master > Service Control Manager** to display the **Tidal Service Manager**.

Step 2 From the Service list, select **Client Manager**. The Client Manager status displays at the bottom of the dialog box.

Step 3 Click **Stop** to stop the Client Manager.

Starting and Stopping the Unix Client Manager

To start Client Manager:

Step 1 Open a command prompt window.

Step 2 Enter:

./cm start

Note ./ may not be required on some systems. Consult your system administrator to determine how the commands should be used.

Step 3 Press **Enter**.

To stop Client Manager:

Step 1 Open a command prompt window.

Step 2 Enter:

./cm stop

Step 3 Press **Enter**.

Uninstalling Client Manager

Uninstalling the Windows Client Manager

The TES master is uninstalled from the Windows Control Panel.

To uninstall Client Manager:

Step 1 From the Windows Start menu, choose **Control Panel**, then double-click **Add or Remove Programs**.

Step 2 Scroll down the list of programs installed on the machine to the Client Manager program.

Step 3 Click the Client Manager program to highlight it.

Step 4 Click **Remove** to start the uninstallation process. A confirmation message displays.

Step 5 Click **OK** to uninstall. The Preparing Setup panel displays showing a progress bar. When the progress bar reaches 100%, a confirmation dialog box displays.

Warning **Do not cancel the uninstallation process once it begins or the uninstallation program will not be able to find its files the next time you attempt to uninstall. If you do cancel the uninstall, you will need to contact Technical Services.**

Note During uninstallation, a dialog box may display indicating that some files are locked because they are shared by other applications. Ignore the locked files and continue with the uninstallation.

Step 6 Click **OK** to finish.

Step 7 Repeat to remove other components.

Step 8 Once you complete uninstalling components, reboot the machine to clear the registry..

Warning **If you do not reboot after uninstallation(s), any subsequent installation may fail.**

Some files or folders under the *Scheduler* folder that were created after the installation might not be removed. You may want to manually delete these files and folders. The log file and the database created during installation remain and must be removed in separate procedures.

Uninstalling the Unix Client Manager

To uninstall the Client Manager:

Step 1 Open a command prompt window.

Step 2 Enter:

 # sh ./Uninstall_UnixClientManager

Step 3 Press **Enter**. The Preparing CONSOLE Uninstall panel displays followed by the About to uninstall panel.

Step 4 Click **Complete Uninstall** to completely remove all features and components of Client Manager that were installed.

-or-

Click **Uninstall Specific Features** to choose specific features of Client Manager that were installed to be uninstalled.

Step 5 Click **Next**. A status bar is displayed to illustrate the progress of the uninstallation program.

Once the uninstall is complete, the Uninstall Complete panel displays.

The Client Manager for Unix is now uninstalled. Any files that were created after the Client Manager is installed are not removed. Files that were not removed must be manually removed.

Step 6 Click **Done** to exit.

Note The uninstallation program only removes the Client Manager files installed at the time of installation. If you created other files in the master directory after installation, these files are not removed. You must manually delete these additional files.

.Uninstalling the Client Manager From the Unix Console

You can also uninstall the Client Manager from the console. The program that uninstalls the Client Manager is one of the files installed during installation of the Client Manager. The program, called *Uninstall_ClientManager*, is in the Client Manager directory created during installation.

To uninstall the Client Manager using the command line:

Step 1 Open a command prompt window.

Step 2 Enter:

 # sh ./Uninstall_ClientManager -i console

Step 3 Press **Enter**. The Preparing CONSOLE Uninstall screen displays followed by the About to uninstall screen.

Step 4 Press **Enter**. A status bar is displayed to illustrate the progress of the uninstallation program.

The Client Manager is now uninstalled. Any files that were created after the Client Manager is installed are not removed. Files that were not removed must be manually removed.

Step 5 Press **Enter** to exit the installation.

Note The uninstallation program only removes the master files installed at the time of installation. If you created other files in the master directory after installation, these files are not removed. You must manually delete these additional files.

Configuring SSL

Configuring SSL for Web Client Connections

This section describes the procedure to enable SSL on for Web Client connections. Client Manager uses an embedded Jetty Web Server to implement web access, configuring SSL on Client Manager is essentially the same as that on Jetty. A simple demo is discussed in the next section to provide a jumpstart.

Note that this guide assumes you already have the following Cisco Tidal products installed and connected to one another:

- Tidal (TES) Master
- Client Manager
- TES Data Source Provider (DSP) Plugin

Demo

The Client Manager comes with a demo certificate to allow you to quickly test its SSL functionality.

To enable the demo:

Step 1 Shut down the Client Manager.

Step 2 Using a text editor, open Web server configuration file *config/webserver.xml* located in Client Manager installation directory.

Note Back up this file before you start editing it to ensure there is a good copy to fall back to.

Step 3 Find the segment of SSL connector that looks like the following. Uncomment the segment by removing "<!--" at the beginning and "-->" at the end.

```
<!--
<Call name="addConnector">
```

```
  <Arg>
    <New class="org.mortbay.jetty.security.SslSelectChannelConnector">
      <Set name="Port">8443</Set>
      <Set name="truststore">config/demo-keystore</Set>
      <Set name="keystore">config/demo-keystore</Set>
      <Set name="trustPassword">OBF:1vny1ym91x1b1z...</Set>
      <Set name="password">OBF:1vny1ym91x1b1z7e1vu...</Set>
      <Set name="keyPassword">OBF:1u2u1vn61z0p1yt4...</Set>
      <Set name="maxIdleTime">30000</Set>
      <Set name="acceptors">2</Set>
      <Set name="statsOn">true</Set>
      <Set name="lowResourceMaxIdleTime">5000</Set>
      <Set name="lowResourcesConnections">5000</Set>
    </New>
  </Arg>
</Call>
-->
```

Step 4 Save the file and start the Client Manager.

Step 5 Open a web browser on the Client Manager host system and enter the URL of TES Web UI with HTTPS protocol, as seen below:

https://localhost:8443/client

Note You may be prompted with a message about the site does not have a trusted certificate. This is because the demo certificate is not signed by a certificate authority. It is only for demo purpose and not meant to be used in production server. You may instruct the browser to proceed.

Your browser is now communicating with the Client Manager via HTTPS protocol.

Configuring SSL Using Your Own Certificate

To configure:

Step 1 Obtaining server key and certificate

You may generate key and certificate by yourself or obtain them from a trusted certificate authority (CA):

a. Generating key and certificate

There are various tools that allow you to generate keys and certificates, among them the Java Keytool that comes with JRE installation.

Java Keytool Example: generating key and certificate in a keystore

keytool -keystore my_keystore -alias tescm -genkey -keyalg RSA

Once you have the keystore, you can follow the instructions in Step 2 to configure SSL connector for the Client Manager. However, your certificate will not be trusted by web browser and user will be prompted to this effect. To set up a production grade server, you must request a well known certificate authority (CA) to sign your key/certificate.

b. Obtaining key and certificate from a trusted CA

There are many trusted CA's, such as AddTrust, Entrust, GeoTrust, RSA Data Security, Thawte, VISA, ValiCert, Verisign, beTRUSTed. Each CA has its own instructions which should be followed (look for JSSE section), but all will involve a step to generate a certificate signing request (CSR).

Java Keytool Example: generating CSR

keytool -certreq -alias tescm -keystore my_keystore -file mycsr.csr

Step 2 Configuring SSL connector with the server key and certificate.

In this section, you will edit the web server configuration file with the key and certificate you obtained from previous section.

a. Shut down the Client Manager.

b. Copy your server key store to the *config* directory in Client Manager's installation directory.

c. Using a text editor to open the Jetty Web Server configuration file *config/webserver.xml* located in Client Manager installation directory.

Note Back up this file before editing it to ensure there is a good copy to fall back to.

d. Uncomment the segment of SSL connector as described in Step 2 of Demo.

e. Replace the values of the following elements by the values applicable to your certificate.

"keystore": Path to the key store mentioned in step b

"password": Password needed to open the key store

"keyPassword": Password needed to read the key, if it's different from the password of the key store

Note Back up this file before editing it to ensure there is a good copy to fall back to.

Note that you can obfuscate the passwords before storing them in the file so their secrecy is secured:

- First, open a command shell window and change directory to the **lib** directory under Client Manager's installation directory.
- Issue one of the following commands:

If on Windows:

java -cp ./jetty-6.2.10.jar;./jetty-util-6.2.10.jar org.mortbay.jetty.security.Password blah <your_password>

If on Unix/Linux:

java -cp ./jetty-6.2.10.jar:./jetty-util-6.2.10.jar org.mortbay.jetty.security.Password blah <your_password>

where **`<your_password>`** is the password to be obfuscated.

- From the output of the command, copy the entire line that starts with "OBF:" (including OBF:) and paste it into the value field of that password in the file.

- Repeat step 1 to 3 for each of the other passwords.

f. Optionally, you can change the port number to be used with HTTPS protocol by modifying the value of the "Port" element. Default is **8443** as seen in the file.

g. Save the file and start the Client Manager.

Step 3 Testing HTTPS connection to Client Manager from Web browser.

Open a Web browser and enter the URL of TES Web UI with HTTPS protocol, for example:

https://<hostname>:<portnumber>/client

Replace **<hostname>** by the actual DNS name or IP address of the Client Manager system.

Replace **<portnumber>**by the actual port number of the SSL connector.

Your browser is now communicating with the Client Manager via HTTPS protocol.

Configuring SSL access for use with Active Directory server

Follow these steps to connect to a Active Directory, SSL-enabled environment.

To configure:

Step 1 Shut down the Client Manager.

Step 2 Download the CA certificate for the Active Directory server from CA Certificate server, or export the installed Certificate from browser. Then save the certificate into a file.

For example:

a. Navigate to http://<CA_SERVER>/certsrv, and then click **Download a CA certificate**, certificate chain, or CRL.

b. From the **CA Certificate** list, choose the certificate.

c. From the Encoding method section, click the **DER** radio button.

d. Click **Download CA Certificate**.

e. Save the certificate, such as *certnew.cer*.

Step 3 Build a trusted keystore for the CA certificate.

For example,

C:\>keytool -import -trustcacerts -keystore store.jks -alias <unique-name> -file certnew.cer -storepass password

Step 4 Using a text editor, modify *<CM_INSTALL>/config/clientmgr.props* to include the following three lines, then save *clientmgr.props*:

For example:

Security.SSL.enabled=Y

Security.SSL.trustStore=c:\\<path>\\store.jks

Security.SSL.trustStorePassword=password

Step 5 Restart the Client Manager.

Connecting to an Active Directory or Open LDAP, SSL-enabled environment

To connect to a Active Directory or Open LDAP, SSL-enabled environment:

Step 1 Stop the Client Manager.

Step 2 Request a copy of the CA Certificate for Client access.

For Active Directory server, download the CA certificate from CA Certificate server, or export the installed Certificate from your browser.

For example:

a. Navigate to http://<CA_SERVER>/certsrv, and then click **Download a CA certificate**, certificate chain, or CRL.

b. From the **CA Certificate** list, select the certificate.

c. From the **Encoding method** section, click the **DER** radio button.

d. Click **Download CA Certificate**.

e. Save the certificate, such as *certnew.cer*.

-or-

For Open LDAP server, copy a DER encoded CA Certificate from the Open LDAP Client to the Client Manager machine. For example, *certnew.cer*.

Step 3 Build a trusted keystore for the CA certificate.

For example,

C:\>keytool -import -trustcacerts -keystore store.jks -alias <unique-name> -file certnew.cer -storepass password

Step 4 Using a text editor, modify *<CM_INSTALL>/config/clientmgr.props* to include the following three lines, then save *clientmgr.props*.

For example:

Security.SSL.enabled=Y

Security.SSL.trustStore=c:\\<path>\\store.jks

Security.SSL.trustStorePassword=password

Step 5 Restart the Client Manager.

References

- How to configure SSL http://docs.codehaus.org/display/JETTY/How+to+configure+SSL
- Securing Passwords http://docs.codehaus.org/display/JETTY/Securing+Passwords
- SslSelectChannelConnector http://jetty.codehaus.org/jetty/jetty-6/apidocs/org/mortbay/jetty/security/SslSelectChannelConnector.html

Installing the Java Client

Cisco TES 6.2 offers a desktop-like client experience with the introduction of a light-weight Java client which can be installed as a standalone application or can be launched through a URL from the TES Master.

Installers are provided for various operating systems.

Installation Prerequisites

The following requirements must be met prior to installation of the Java Client:

- Java 7 (64-bit)
- Hardware specifications:
  - Memory: 8GB to 16GB
  - CPU (64-bit): 2.2+ GHz Quad Core
- Software specifications:
  - Only JavaFx2 certified systems are supported. See:

    http://www.oracle.com/technetwork/java/javafx/downloads/supportedconfigurations-1506746.html
  - Install Desktop Experience (Windows Server Only). See: http://technet.microsoft.com/en-us/library/cc754314.aspx
  - The software installs and runs only in X-Windows desktop mode (for example, GNOME, KDE) of all UNIX based operating systems.

Installing the Java Client for Windows

To install the Java client for Windows:

Step 1 Run the *install.exe* file. The installation wizard displays.

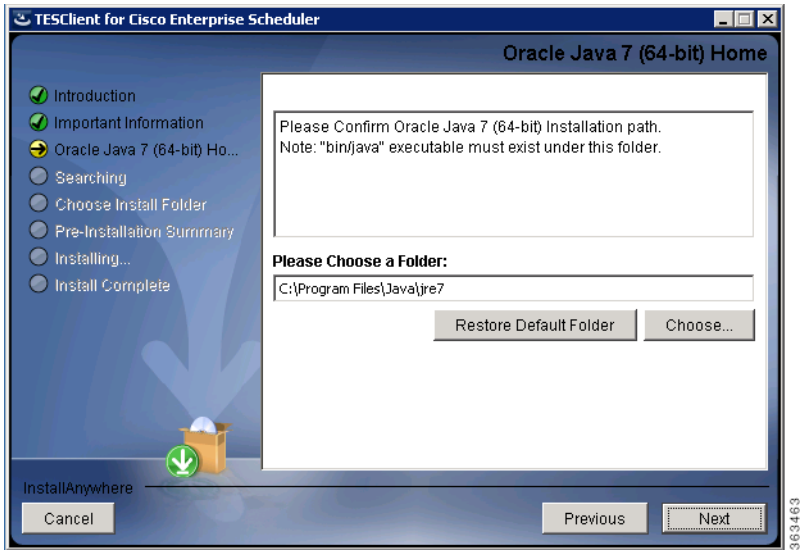
Step 2 At the Introduction screen, click **Next.**

Step 3 At the Important Information screen, read the information and click **Next**.

Step 4 At the Oracle Java 7 (64-bit) Home screen, choose the path to the Java 7 folder.

Note You may have installed multiple Java virtual machines. Ensure that you choose version 7 specifically.

Figure 5-1 Oracle Java 7 (64-bit) Home Screen



Step 5 At the Choose Install Folder screen, select the location where you want the Java client to be installed.

Step 6 The Pre-Installation Summary screen shows the items that will be installed. Click **Install**. The installation progress is shown in the next screen.

Step 7 The Install Complete screen summarizes the results of the installation. Click **Done**.

Confirm that a new TES client shortcut is created.

Installing the Java Client for Unix

To install the Java client for Unix:

Step 1 Run the *install.bin* file. The installation wizard displays.

Step 2 At the Introduction screen, click **Next.**

Step 3 At the Important Information screen, read the information and click **Next**.

Step 4 At the Oracle Java 7 (64-bit) Home screen, choose the path to the Java 7 folder.

Note You may have installed multiple Java virtual machines. Ensure that you choose version 7 specifically.

Step 5 At the Choose Install Folder screen, select the location where you want the Java client to be installed.

Step 6 The Pre-Installation Summary screen shows the items that will be installed. Click **Install**. The installation progress is shown in the next screen.

Step 7 The Install Complete screen summarizes the results of the installation. Click **Done**.

Step 8 You can now launch the software by executing the `tesclient.sh` command.

Running the TES Java Client

You can run the Cisco TES 6.2 Java client as an application on your system, as well as via a web browser.

Running the Java Client as a System Application

Prerequisites

The following prerequisites must be met to run the Java client as a system application:

- Java client Host machine must be in DNS/NIS+ domain.
- Java client Host machine must be allowed to connect to port 6215 of Scheduler's host.
- Scheduler's master.props must have valid LDAP/AD configuration.

To run the Java client as an application on your system:

Step 1 Launch the Java client that you have installed. The Login screen displays.

Step 2 Enter the following details:

- **Server**— The scheduler’s hostname
- **User**— AD/LDAP user name
- **Password**—AD/LDAP password

Step 3 Click **Connect**.

The Java client application window displays.

Note The logs and help folders are created in your *temp* folder. You can view them by clicking **View > Client Logs**.

Note Startup scripts of the Java client can be optionally modified to add jvm arguments for optimal performance.

Running the Java Client Via a Web Browser

Prerequisites

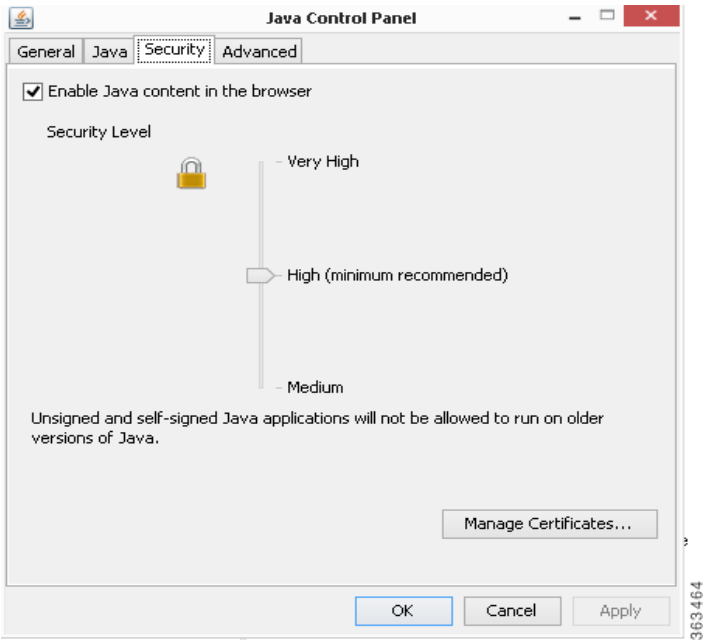
The following prerequisites must be met to run the Java client via a web browser:

- By default, scheduler will run a webserver at port 8080. The Java client host must be allowed to access a configured port on scheduler's host machine.
- On Windows, only Internet Explorer 64-bit (c:\Program Files\Internet Explorer\iexplorer.exe) is capable of running 64-bit Java7. Only 64-bit Java7 will support 8GB memory requirements.
- For all operating systems and browsers, you must enable Java content in the Java Control Panel.

Note Confirm that browser's security settings allow running Java applets.

Figure 5-2

Java Control Panel



To run the Java client via a web browser:

Step 1 Open a TES-supported web browser and enter the following URL:

http://*master's hostname:8080/tesclient*

where *master's hostname* is the hostname of TES.

Step 2 Click **Launch Enterprise Scheduler**.

Step 3 Click **Run** to allow execution of the Java client.

The Java client is launched.

If the version of Java client does not match what has been installed on the master, remove all temporary Java files using options available in the **General** tab of the Java Control Panel.

Uninstalling the TES Java Client

The Java client applications that are installed on Windows systems can be uninstalled from the Control Panel.

For UNIX systems, use **`install.bin -r`** to uninstall the Java client.

Note If you face issues removing the software, inspect and cleanup the *.com.zerog.registry.xml* file, located under the user's home directory (for Unix), or at c:\Program Files\Zero G Registry (for Windows).

Installing Fault Tolerance

Introduction

The basic principle of fault tolerance is to keep your production schedule running continuously despite machine failures.

Auto Mode

Auto mode is the default way of configuring fault tolerance. This mode allows the primary master to run in standby mode. If the primary master fails and the backup master assumes control, then the backup master assumes the active role. When the primary master that failed comes back online, it remains in standby mode. This type of fault tolerance does not care if the original primary master is actively controlling the production or if the configured backup master is in control. Regardless of the original configuration, each master is interchangeable and can operate in either an active or standby mode. See also, "Operational Modes for Fault Tolerance".

Fixed Mode

When configured in Fixed mode, if the machine managing your production schedule fails, fault tolerance ensures that another machine is available to assume control over the production schedule. Scheduler's fault tolerance ensures that a backup master can keep production going if the primary master should fail.

Note Fault tolerance does not protect against database failures. This is best left to your database administrator who can set up data mirroring based on the type of database being used.

Whenever the primary master is running while the backup master remains available to assume control, the system is in standby mode. If the primary master is unable to run, control of the production schedule passes to the backup master ensuring uninterrupted production. Whenever the backup master assumes control from the primary master, the system is the backup mode.

When the backup master assumes control, it continues the production schedule until control is manually switched back to the primary master. During the time the backup master controls the production schedule, fault tolerance is disabled. Fault tolerance is enabled again when the primary master resumes control. In the backup mode, fault tolerance is disabled because the backup master does not have a backup.

Note Plan to spend approximately two hours for the installation and configuration of fault tolerance.

During a failover, the green light beside the fault monitor name (located in the first column of the Connections pane) turns red. This light indicates that fault tolerance is not operating.

The status lights warn users that without master redundancy, the network is vulnerable to failure. Returning the primary master to service and restoring your system to a normal fault tolerant status should be the highest priority. Use the switch back procedure to return the primary master to service. See "Primary Master Switchback".

In the Unix installation procedure after providing a directory location for the installation files, a screen asks if you wish to install a primary master or backup master. You should install the primary master first. Complete the primary master installation and then repeat the master installation on a different machine, selecting the backup master option for the second installation. For more information on installing the primary and backup masters for Unix, refer to "Installing the Master for Unix".

Components of Fault Tolerance

Fault tolerance consists of the following main components:

- Client Manager – The Client Manager services requests from user initiated activites, such as through the Tidal Web Client.
- Primary Master – The primary master controls production scheduling during normal system operations.
- Backup Master – The backup master operates in standby mode until it takes over for the primary master. In case of a failover, the backup master becomes active and clients reconnect to the backup master.
- Fault Monitor – The fault monitor continuously monitors the status of the primary and backup masters. It initiates the transfer of scheduling control from the primary master to the backup master. The Tidal Web client provides an interface to the fault monitor service.

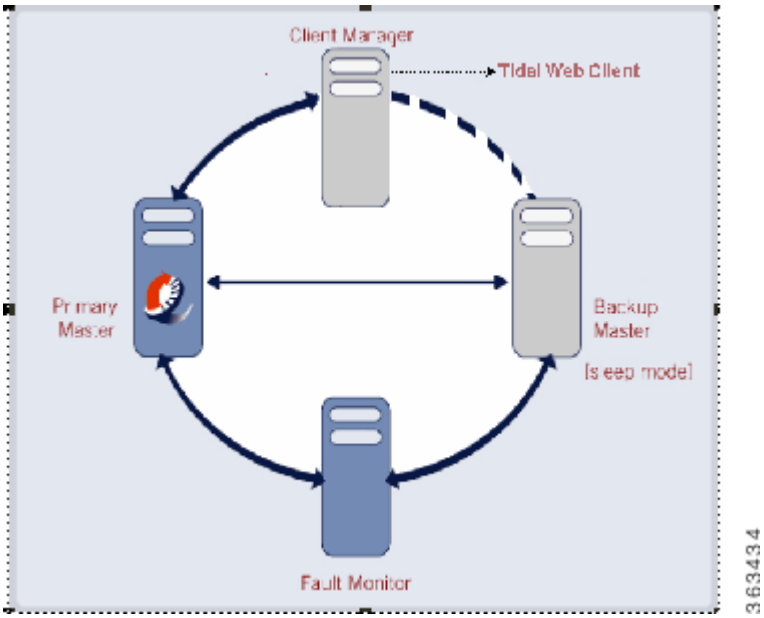
Both the primary master and the backup master are designed to communicate with a database. Responsibility for setting up and maintaining this database is left to your database administrator. *TES* does *not* provide fault tolerance for the database.

Operational Modes for Fault Tolerance

Normal (Sleep) Mode

Figure 5-1 shows normal operation, or the sleep mode. The backup master remains in the background until required though maintaining constant communication with both the primary master and the fault monitor.

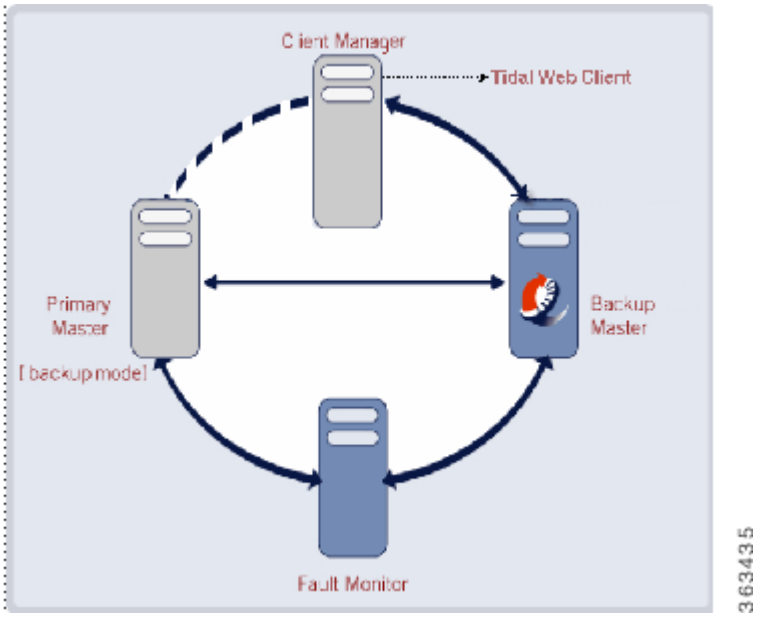
Figure 5-1 Normal Operation, Sleep Mode



Backup Mode

Figure 5-2 shows fault tolerance operation when the primary master goes down (backup mode). The backup master becomes active, assuming control of the production schedule while the primary master is out of service. Both figures show only the main components of fault tolerance.

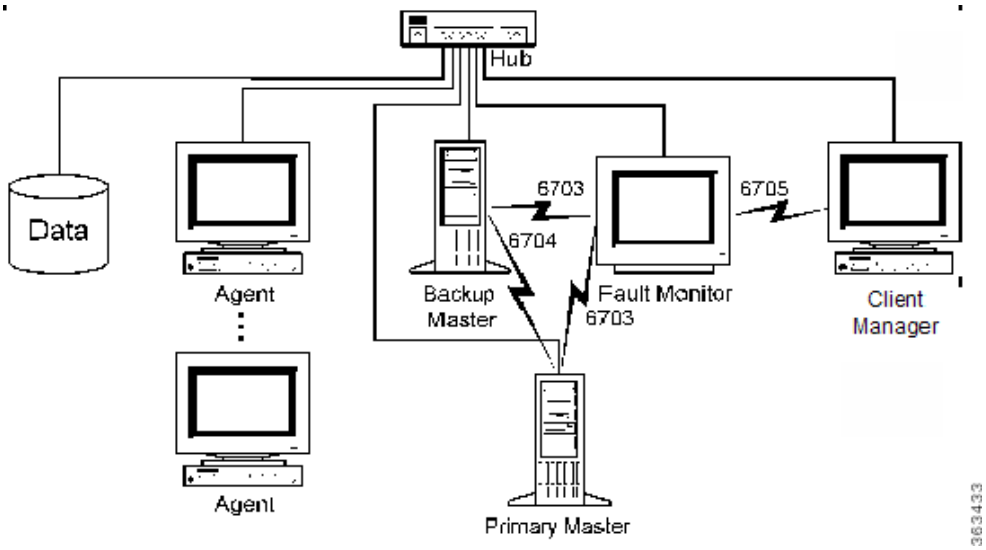
Figure 5-2 Primary Master Down, Backup Mode



Network Configuration

For fault tolerance to operate properly, the physical network connections between the various components must be configured properly for reliable communication. Dedicated TCP/IP communication ports, configured during installation, are used to exchange messages between components and to verify whether the connections are up or down. Figure 5-3 shows the network connections and the communication ports.

Figure 5-3 Network Configuration



System Requirements

The primary master, the backup master and the fault monitor must be installed on separate machines. There are different system requirements for the Windows and Unix platforms. See your Cisco Tidal Enterprise Scheduler User Guide for the system requirements.

User Account Requirements

The account used to install fault tolerance must meet the following requirements:

- The account must be a domain user account, not a local machine account.
- The account must be part of the local Administrators group.
- The account must have the advanced local user rights Logon as a service and Act as part of the operating system set by the system administrator on each server
- If you are installing on Unix, the masters and fault monitor must be installed under either root or a user created by root.

Warning **If these user requirements are not met, fault tolerance will not install properly and your system will be unprotected in the case of a failure.**

Prerequisites for Installation

The following points list the conditions that must be met before fault tolerance is installed. Failure to meet these preliminary conditions will result in unnecessary delay and may cause the installation process to fail.

- There must be at least three machines for a fault tolerance setup.
- All three machines must be in the same domain.
- The primary master must be installed, licensed and operational.
- Both the primary and backup masters must meet the minimum system requirements for TES.
- The primary master and the backup master must have the same operating system (including patches), database connectivity and hardware configuration. Their software and configuration should mirror the each other.
- The same version of JVM must be installed on the primary master, backup master and fault monitor machines.
- The backup master's clock should be as closely synchronized as possible with the primary master's clock.

Installing Fault Tolerance for Windows

Installing fault tolerance on a network means adding another master to shadow an existing master. The first master becomes the primary master in TES while the second master is referred to as the backup master. This backup master, like the primary master, is controlled from the Service Manager. The procedure to install this backup master is similar yet different from the procedure detailed in the *Installing the Master* chapter.

A network component that monitors the operation of the two masters called the fault monitor is installed on a third machine. A Fault Monitor window is added to the **Navigator** pane in the Tidal Web client.

This chapter describes how to:

- install (or upgrade) the backup master on a Windows machine
- install the fault monitor on a Windows machine

Prerequisites for Installation

The following items should be completed and ready prior to starting fault tolerance installation.

- Create a backup of your database. As a matter of general operating policy, it is recommended that a database be backed up at least once daily.
- Ensure that the primary and backup master clocks run no more than 15 seconds apart.
- The primary and backup master machines should mirror each other in hardware and software configurations.
- The primary and backup master machines must be able to ping each other, the fault monitor and the database.

  The fault monitor machine must be able to ping the Client Manager, primary and backup masters.

  Client Manager can reside on either the master machine or on a separate machine. In this case, there will be a fourth machine.
- Use three separate PCs, one as a primary master, one as a backup master and one as a fault monitor.

Installation Check List

To ensure a successful and smooth installation of fault tolerance, prior to the start of installation collect the information about the machine components needed during installation. Use the following check list to collect the necessary information:

Primary Master:

Computer Name_____

Host Name_____

Backup Master:

Computer Name_____

Host Name_____

Fault Monitor:

Computer Name_____

Host Name_____

Record the domain user account.

Domain Account_____

Record the port numbers to be used by the primary master, backup master and fault monitor.

Fault monitor to master_____

Master to master_____

Fault monitor to client_____

Scheduler provides default port numbers of **6703** for fault monitor to master, **6704** for master to master, and **6705** for fault monitor to client.

Installing Components for Fault Tolerance

Before installing, get license files for your TES fault tolerance components from the Licensing Administrator for Scheduler. The fault tolerance setup consists of steps which must be performed in order. The procedures for each step are covered in this chapter.

A Scheduler primary master, Client Manager and agent(s) must be already installed, licensed and operational for a successful fault tolerance installation. The individual components can be installed on different machines, but they must all be in the same domain as your fault tolerance setup. You will need to refer to the information collected on the Installation checklist. The first master installed becomes your primary master.

Installing the Backup Master

To install the backup master:

Step 1 Load the Tidal Enterprise Scheduler installation DVD-ROM into the DVD-ROM drive of the machine where the backup master is being installed. The Tidal Scheduler panel displays.

Step 2 On the Scheduler screen, click the **Backup Master** link and select the Run this program from its current location option in the File Download dialog box. The Welcome panel displays.

Step 3 Click **Next**. The Installation Type panel displays.

Step 4 Select **BackupMaster**, then click **Next**.

Step 5 On the Destination Folder panel, select the directory where the TES files will reside.

- Click the **Change** button to search for a directory.

  -or-

- Accept the default location *C:\Program Files\TIDAL*.

Step 6 Click **Next**. The Database Type panel displays.

Step 7 Select the type of database being used and click **Next**. The Database Server panel displays.

Step 8 Enter the name of the database server used by the primary master.

Step 9 Click **Next**. The Ready to Install the Program panel displays.

Step 10 Click **Install**. The Installshield Wizard Complete panel displays.

Step 11 Click **Finish** to close the wizard.

Installing the Fault Monitor

Warning **The fault monitor must be installed on a separate machine from the primary and backup masters.**

To install the fault monitor:

Step 1 Click the **Fault Monitor** link on the TIDAL Scheduler installation screen for Internet Explorer.

-or-

If using the Netscape browser, copy the fault monitor files to a *temp* directory as directed in the TES Installation Steps section.

The Welcome panel displays.

Step 2 Click **Next**. The Installation Type panel displays.

Step 3 Select **FaultMonitor**, then click **Next**. The **Destination Folder** panel displays.

Step 4 Select the directory where the TES files will reside:

- Click the **Change** button to search for a directory.

  -or-

- Accept the default location *C:\Program Files*.

Step 5 Click **Next**. The Enter requested data panel displays.

Step 6 Enter the following:

- FM Port –The port number of the fault monitor.
- Client Port – The port number of the Client Manager.

Step 7 Click **Next**. The Ready to Install the Program panel displays.

Step 8 Click **Install**. The Installing panel displays the progress of your fault monitor installation in the form of a progress bar.

The Setup Completed panel displays.

Step 9 Click **Finish** to complete fault monitor installation and return to the Scheduler installation dialog box.

Controlling the Fault Monitor

You can monitor the fault monitor from the Tidal Web client. If you have installed fault tolerance, then a Fault Monitor tab displays inside the *Master Status* folder under the *Operations* folder in the Navigator pane of the Tidal Web client.

Note To see the Fault Monitor option, you must be properly licensed for fault tolerance and your security policy must include access to the fault monitor option.

The fault monitor can also be accessed from the command line of the machine it is installed on.

Starting the Fault Monitor

To start the fault monitor, use the following command:

Step 1 From the Windows Start menu, and choose **Programs > Tidal Software > Tidal Service Manager** to display the Tidal Services Manager.

Step 2 From the Service list, choose **SchedulerFaultMon**.

Step 3 Click **Start**.

Stopping the Fault Monitor

To stop the fault monitor, use the following command:

Step 1 CFrom the Windows Start menu, and choose **Programs > Tidal Software > Tidal Service Manager** to display the Tidal Services Manager.

Step 2 From the Service list, choose **SchedulerFaultMon**.

Step 3 Click **Stop**.

Checking the Fault Monitor Status

To check the operation status of the fault monitor, use the following command:

Step 1 On the Fault Monitor machine, click the Windows Start button and choose **Programs > Tidal Software > Tidal Service Manager** to display the Tidal Service Manager.

Step 2 From the Service list, select **Fault Monitor**. At the bottom of the Tidal Service Manager, the status of the selected service displays.

Installing Fault Tolerance for Unix

This section describes how to:

- install the fault monitor on a Unix machine
- verify that files were successfully installed
- start, stop and check the status of the fault monitor from the command line

While there is a fault monitor console for the Windows platform that displays activity messages about fault monitor components, there is no such fault monitor console for the Unix platform. The activity messages from the fault monitor can be displayed and controlled from the Fault Monitor pane in the Tidal Web client. For more information, refer to the "Fault Monitor Interface".

Prerequisites for Installation

The following items should be completed and ready prior to starting fault tolerance installation.

- Create a backup of your database. As a matter of general operating policy, it is recommended that a database be backed up at least once daily.
- Ensure that the primary and backup master clocks run no more than 15 seconds apart.
- The primary and backup master machines must be able to ping each other, the fault monitor and the database.

  The fault monitor machine must be able to ping the Client Manager, primary and backup masters.

  Client Manager can reside on either the master machine or on a separate machine. In this case, there will be a fourth machine.
- Use three separate Unix machines, one as a primary master, one as a backup master and one as a fault monitor.

Installation Check List

To ensure a successful and smooth installation of fault tolerance, prior to the start of installation collect the information about the machine components needed during installation. Use the following check list to collect the necessary information:

Primary Master:

Computer Name_____

Host Name_____

Backup Master:

Computer Name_____

Host Name_____

Fault Monitor:

Computer Name_____

Host Name_____

- Record the user account.

  User Account_____
- Record the port numbers to be used by the primary master, backup master and fault monitor.

  Fault monitor to master_____

  Master to master_____

  Fault monitor to CM_____

TES provides default port numbers of **6703** for fault monitor to master, **6704** for master to master, and **6705** for fault monitor to Client Manager.

Installing Components for Fault Tolerance

Before installing, get license files for your TES fault tolerance components from the Licensing Administrator for TES. The fault tolerance setup consists of steps which must be performed in order. The procedures for each step are covered in detail in this chapter.

A TES primary master, Client Manager and agent(s) must be installed, licensed and operational for a successful fault tolerance installation. The individual components can be installed on different machines, but they must all be in the same domain as your fault tolerance setup. The first master installed will be your primary master.

Installing the Backup Master

Instructions for installing the backup master are the same instructions provided in this guide for installing the master (primary) for Unix. The hardware and software requirements for a backup master are the same as the requirements for a primary master. During the installation procedure a screen is displayed to designate whether the installation is for a primary or backup master. Selecting the ***Backup*** option, ensures that a backup master is installed. Complete the described procedure to install and verify successful installation of the backup master.

Installation Prerequisites for the Fault Monitor

See your *Cisco Tidal Enterprise Scheduler User Guide* for the requirements that must be met for successful installation of the Unix fault monitor.

Installing the Fault Monitor

Warning **The fault monitor must be installed on a separate machine from the primary and backup master machines. Only one fault monitor can be installed on a machine.**

To install the fault monitor:

Step 1 If you are copying the installation files from the network, FTP the *install.bin* file to the directory you created.

If you are using the DVD-ROM, locate the *install.bin* file for your operating system on the DVD-ROM and copy it to a directory you created. The file can be found on the DVD-ROM at *<DVDROMDRIVE>\UnixFaultMon\<operating system>\install.bin*

Step 2 Change the permissions on the *install.bin* file in the directory to make the file executable:

chmod 755 install.bin

Step 3 After copying the file to the directory, begin the installation program by entering:

sh ./install.bin

The Introduction panel displays.

Step 4 After reading the introductory text that explains how to cancel the installation or modify an previous entry on a previous screen, click **Next**. The Choose Install Folder panel displays.

Step 5 Select the directory where the TES files will reside:

- Click **Choose** to search for a directory. If you change your mind after selecting a different destination, select **Restore Default Folder** to revert back to the default installation location.

  -or-

- Accept the default location: */opt/unixsa*

Step 6 Click **Next**. The Port Numbers panel displays.

Step 7 Enter the port number of the Fault Monitor and the Client Manager, then click **Next**. The Pre-Installation Summary panel displays the destination location selected for the fault monitor files.

If the location is not where you intended, click **Previous** until you return to the Choose Install Folder panel and correct the installation location.

Step 8 Click **Install** to begin the installation of files. The Installing UnixFM panel displays.

The Install Complete panel displays when the installation process is completed.

Step 9 Click **Done** to exit the installation program.

Verifying Successful Installation of the Fault Monitor

You should verify that the installation program installed all of the necessary files.

Go to the *bin* directory location where you installed the fault monitor files and list the contents of the directory with the following command:

ls -l

You must have two files called *tesfm* and *tmkdea* before the fault monitor can operate correctly.

Controlling the Fault Monitor

You can monitor the fault monitor from the Tidal Web client. If you have installed fault tolerance, then a Fault Monitor tab displays inside the *Master Status* folder under the *Operations* folder in the Navigator pane of the Tidal Web client.

Note To see the Fault Monitor option, you must be properly licensed for fault tolerance and your security policy must include access to the fault monitor option.

The fault monitor can also be accessed from the command line of the machine it is installed on.

Starting the Fault Monitor

To start the fault monitor, use the following command:

tesfm start

Stopping the Fault Monitor

To stop the fault monitor, use the following command:

tesfm stop

Checking the Fault Monitor Status

To check the operation status of the fault monitor, use the following command:

tesfm status

Modifying the Fault Monitor Configuration

You can change the properties of the fault monitor that were set during the installation. Circumstances may force you to change the configuration of the fault monitor as it was originally installed or you may need to change the logging levels of various components for diagnostic purposes.

The properties of the fault monitor are managed in a file called *master.props* that resides in the *config* directory on the fault monitor machine.

The *master.props* file on the fault monitor looks like the following example:

FMMasterPort=6703

FMClientPort=6705

Be careful when changing the properties of the fault monitor, incorrect entries to the *master.props* file may prevent the proper operation of the Unix fault monitor.

Note If you change the Fault Monitor Client Port number in the Connection Definition dialog box in the Tidal Web client, you must manually change the FMClientPort number in the fault monitor *master.props* file also.

The properties options that are managed in the *master.props* file are listed below:

Property	Default Value	What it Controls
FMMasterPort	6703	Number of the port used by the master to connect to the fault monitor. The default number is 6703.
FMClientPort	6705	Number of the port used by the Client Manager to connect to the fault monitor. The default number is 6705. This port number must match the port number in the fault monitor's Connection Definition dialog box in the Tidal Web client. If you change the port number in one place, you must manually change the port number in the other place.
CMDMasterPort (Optional)	6600	Number of the port that the command line program uses to connect to the Unix master machine. (This property is only used to modify the port if it is being used by another application.)

Fixing a Port Number Conflict

A port number conflict may occasionally occur in the fault monitor. Certain port numbers are used by default in the fault monitor. If another application is using the same port numbers then the fault monitor will not work and you must change the port numbers. Some port numbers can be changed from the Connection Definition dialog box for that component but others must be manually changed on the fault monitor machine. This port conflict may occur with either the port being used by the Client Manager to connect to the fault monitor (**6705**) or with the port used by the command line program to connect to the Unix master machine (**6600**).

To fix a port number conflict:

Step 1 On the fault monitor machine, locate the *config* directory.

Step 2 Open the *master.props* file to see the various properties that control the port numbers used by the fault monitor.

- FMClientPort is for the port used by the Client Manager to connect to the fault monitor.
- CMDMasterPort is for the port used by the command line program.

Step 3 Change the port number to a port number not in use by any other application.

Note Be sure that the port numbers in the master.props file match the port numbers in the component's Connection Definition dialog box.

Using Fault Tolerance

Fault tolerance in TES is configured on the Fault Tolerance tab in the System Configuration dialog box of the Tidal Web client. Messages about fault tolerance are displayed in both the Fault Monitor console and the Tidal Web client Fault Monitor pane. The following sections explain how to configure and verify fault tolerance.

Licensing Fault Tolerance

The Fault Tolerance function cannot be used unless it is properly licensed. You must shut down fault tolerance to load the license file.

Note Fault tolerance cannot be turned off if the backup master is active. The primary master must be in control to turn off fault tolerance.

Obtain the license code from the licensing manager at Cisco. Registering the license for Fault Tolerance is performed from the Tidal Web client.

To load a production license for Fault Tolerance, you need the proper license file.

To license Fault Tolerance with a Full license:

Step 1 Stop the master:

For Windows:

a. From the Windows Start menu, choose **Programs > TIDAL Software > Scheduler > Master > Service Control Manager** to display the Tidal Services Manager.

b. Verify that the master is displayed in the Service list and click on the **Stop** button to stop the master.

For Unix:

Enter **tesm stop**.

Step 2 Rename your Full license file to *master.lic*.

Step 3 Place the file in the *C:\Program File\TIDAL\Scheduler\Master\config* directory.

Step 4 For Windows, restart the master by clicking **Start** in the Service Control Manager. For Unix, restart the master by entering **tesm start**.

The master will read and apply the license when it starts.

Failover Configuration

From the Activities menu, choose **Configure Scheduler** to display the System Configuration dialog box.

Enabling Fault Tolerance

To enable fault tolerance:

Step 1 Before enabling fault tolerance, stop the backup master.

a. From the Windows Start menu, choose **Programs > TIDAL Software > Scheduler > Master > Service Control Manager** to display the Tidal Services Manager.

b. In the Service list, select **Backup Master** if it is not selected.

c. Click the **Stop** button to stop the backup master.

Step 2 In the Tidal Web client, choose **Configure Scheduler** from the Activities main menu to display the System Configuration dialog box.

Step 3 Select the Fault Tolerance tab.

Step 4 Click the Enable Failover option to add the check mark and enable fault tolerance operation.

Step 5 To complete the Enable Failover process, verify that the Fault Monitor and the Backup Master are started.

Fault Tolerance Tab Options

The Fault Tolerance tab of the System Configuration dialog box contains the following options:

- Failover Enable – Enables fault tolerance. If this option is not selected, then no action (failover) is taken if the master fails. If this option is selected, control of production switches over to the designated backup master if a failure occurs on the primary master. The default configuration is disabled. Selecting this check box, displays the following options to enter the information required to configure fault tolerance.
- Machine Name (backup master only) – The name of the machine where the backup master resides.
- Backup-To-Master Port (backup master only) – The port number used for communication between backup master and primary master.
- Machine Name (fault monitor only) – The name of the machine where the fault monitor resides.
- Fault Monitor Master Port (6703 is the default) – The port number used by the fault monitor to communicate with masters.

- Fault Monitor Client Port (6705 is the default) – The port number used by the fault monitor to communicate with the Client Manager.

Starting Fault Tolerance

To start fault tolerance:

Step 1 Verify that Failover is enabled. See "Enabling Fault Tolerance".

Step 2 Close all Clients.

Step 3 Stop the Client Manager, Masters, Primary and Backup, if running, via the Service Control Manager (Windows) or the command line (Unix).

Step 4 Verify that the Fault Monitor is running.

Step 5 Start the Primary Master and verify that it is running via the Service Control Manager (Windows) or the command line (Unix).

Step 6 Start the Backup Master and verify it is running via the Service Control Manager (Windows) or the command line (Unix).

Step 7 Start the Client Manager via the Service Control Manager (Windows) or the command line (Unix).

Step 8 Log into the application via the Tidal Web Client and choose **Operations > Master Status**.

Step 9 Select the Fault Monitor tab and validate Poll Activity. You should see *Primary OK and Backup OK. [Standby Mode].*

More options are displayed to add the information required to configure fault tolerance. Refer to "Fault Tolerance Tab Options" for more information on the options used to configure fault tolerance.

Verifying Fault Tolerance Operation

To verify fault tolerance operation:

Step 1 Launch the Tidal Web client and from the Navigator pane, select **Operations > Fault Monitor** to display the Fault Monitor pane.

Step 2 Check the activity messages displayed in the Fault Monitor pane to verify that all components of fault tolerance are operating correctly.

Setting Failover Time

By default, failover takes three minutes. You can adjust this time period for more or less primary master recovery time.

To set failover time:

Step 1 Locate the *master.props* file in the **config** directory where you installed the fault monitor files on the fault monitor machine.

Step 2 Open the *master.props* file in a text editor.

Step 3 On a separate line in the file, enter:

ToleranceTime=<number of minutes>

where the brackets are replaced with the number of minutes to pass without contact with the primary master before failover to the backup master.

Step 4 Stop the fault monitor.

Step 5 Start the fault monitor to enable the new parameter.

Modifying Fault Tolerance Parameters

You can change the properties of the fault monitor that were set during the installation. Circumstances may force you to change the configuration of the fault monitor as it was originally installed or you may need to change the logging levels of various components for diagnostic purposes.

The properties of the fault monitor are managed in a file called *master.props* that resides in the *config* directory on the fault monitor machine.

The *master.props* file on the fault monitor looks like the following example:

FMMasterPort=6703

FMClientPort=6705

Be careful when changing the properties of the fault monitor, incorrect entries to the *master.props* file may prevent the proper operation of the fault monitor.

Note If you change the Fault Monitor Client Port number in the Connection Definition dialog box in the Tidal Web client, you must manually change the FMClientPort number in the fault monitor *master.props* file also.

The rest of the fault tolerance parameter options that are managed in the *master.props* file are listed below:

Property	Default Value	What it Controls
FaultMonitorLog	INFO	Sets the level of detail for recording messages about the fault monitor to the Fault Monitor log.
FaultToleranceLog	INFO	Sets the level of detail for recording messages about fault tolerance components to the Fault Monitor log.
FMMasterPort	6703	Number of the port used by the master to connect to the fault monitor. The default number is **6703**.
FMClientPort	6705	Number of the port used by the Client Manager to connect to the fault monitor. The default number is **6705**. This port number must match the port number in the fault monitor's Connection Definition dialog box in the Tidal Web client. If you change the port number in one place, you must manually change the port number in the other place.

Property	Default Value	What it Controls
ToleranceTime	3	Number of minutes the fault monitor will go without communication with the primary master before having the backup master assume control.
CMDMasterPort (Optional)	6600	Number of the port that the command line program uses to connect to the Unix master machine. (This property is only used to modify the port if it is being used by another application.)
Tuning for DSP to FM message traffic (all DSP connections).		
MinSessionPoolSize	2	—
MaxSessionPoolSize	5	—
MaxConcurrentMessages	5	—

Fixing a Port Number Conflict

A port number conflict may occasionally occur in the fault monitor. Certain port numbers are used by default in the fault monitor. If another application is using the same port numbers then the fault monitor will not work and you must change the port numbers. Some port numbers can be changed from the Connection Definition dialog box for that component but others must be manually changed on the fault monitor machine. This port conflict may occur with either the port being used by the Client Manager to connect to the fault monitor (**6705**) or with the port used by the command line program to connect to the Unix master machine (**6600**).

To fix a port number conflict:

Step 1 On the fault monitor machine, locate *config* > *master.props*.

Step 2 Use a text editor to open the file to see the various properties that control the port numbers used by the fault monitor.

- FMClientPort is for the port used by the Client Manager to connect to the fault monitor.
- CMDMasterPort is for the port used by the command line program.

Step 3 Start the Client Manager.

Step 4 Change the port number to a port number not in use by any other application.

Step 5 Stop the fault monitor.

Step 6 Start the fault monitor to enable the new parameter.

Note Be sure that the port numbers in the *master.props* file match the port numbers in the component's Connection Definition dialog box.

Fault Monitor Interface

The fault monitor can also be displayed from the Tidal Web client console pane. To display messages from the fault monitor in the client, click the Fault Monitor tab within the *Master Status* folder. The Fault Monitor pane displays any messages from the fault monitor.

Note To see the Fault Monitor option, you must be properly licensed for fault tolerance, and your security policies must include access to the fault monitor option.

Fault Monitor Pane Context Menu

Various functions for the fault monitor can be accessed from the context menu of the Fault Monitor pane. To display the menu, right-click anywhere in the Navigator pane or the Fault Monitor pane.

The Fault Monitor pane context menu.

- Refresh – Updates the information displayed in the Fault Monitor tab.
- Print – Prints the messages displayed in the Fault Monitor tab.
- Print Selected – Prints the selected messages displayed in the Fault Monitor tab.
- Stop All – Stops the operation of the primary master, the backup master, and the fault monitor. When you select this option, a Confirm dialog box displays. Click **Yes** to continue and **No** to abort.
- Stop Fault Monitor – Stops the fault monitor. When you select this option, a Confirm dialog box is displayed. Click **Yes** to continue and **No** to abort. If the fault monitor is not running, failover is not possible.
- Stop Backup and FaultMon – Stops the operation of the backup master and the fault monitor. When you select this option, a Confirm dialog box displays. Click **Yes** to continue and **No** to abort. When the backup master and fault monitor are stopped, the primary master continues without being fault tolerant.

Notice that there are no menu options to start the fault monitor or the primary master. These components are started from the Service Manager or if you are using the Unix version, the components are started from the command line of each machine hosting that component.

Fault Tolerance Operation

Fault tolerance is only available if a backup machine is available to assume control. This means that if a primary master fails and the backup master assumes control during a failover, your system is no longer fault tolerant. If you are using the backup master because the primary master failed then there is no backup protection in case the backup master also fails. You must restore the failed master to operation to return to a fault tolerant mode. Only when both masters are operational, with one master running and the other master on standby, is your system fault tolerant.

Note Fault tolerance cannot be turned off if the backup master is active. The primary master must be in control to turn off fault tolerance.

The default way of configuring fault tolerance though, allows the primary master to run in standby mode. If the primary master fails and the backup master assumes control, then the backup master assumes the active role. When the primary master that failed comes back online, it remains in standby mode. This type of fault tolerance does not care if the original primary master is actively controlling the production or if the configured backup master is in control. Regardless of the original configuration, each master is interchangeable and can operate in either an active or standby mode. Fault tolerance is configured to run in this manner by using the AUTO value for the FT_OPERATION property in the *master.props* file.

Note The default value for the FT_OPERATION property in the master.props file is AUTO.

This duality of roles can be confusing to keep track of, but the messages displayed in the Fault Monitor pane note in which mode a master is operating. If a master is in control, it is considered active and if it is in standby mode, this is also noted. For example, a message in the Fault Monitor pane may read *"Backup OK [Active]"* to denote that the designated backup master is in control. A similar message concerning the backup master in standby mode would read *"Backup OK [Standby]."*

Fault tolerance can operate in a different manner if needed. One of the masters can be designated to always be the primary master. Its primary master role is fixed. The machine that is configured as the primary master must be in control with the backup master on standby before the system is considered fault tolerant. The primary master cannot run in standby mode. In this configuration, the system can never be fault tolerant if the backup master is in control. Once a failover occurs, the primary master cannot be restarted until the backup master is stopped. Fault tolerance can be configured to run in this manner by using the FIXED value for the FT_OPERATION property in the *master.props* file.

Stopping Scheduler in Fault Tolerant Mode

If TES is running in fault tolerant mode, all of the Scheduler components can be conveniently stopped from the Fault Monitor pane in the Tidal Web client. Scheduler will automatically stop the components in the proper sequence.

To stop Scheduler in Fault Tolerant mode:

Step 1 Stop all fault tolerance components from the Navigator pane of the Tidal Web client by selecting **Operations > Fault Monitor** to display the Fault Monitor pane.

Step 2 Right-click the Fault Monitor pane and from the displayed context menu, choose **Stop All**.

Starting Scheduler in Fault Tolerant Mode

Note It is a recommended practice to prevent any new jobs from being submitted during this procedure by setting the system queue to 0. Let the active jobs complete.

To start Scheduler in Fault Tolerant mode:

Step 1 On the fault monitor machine, verify that the fault monitor is running.

Step 2 Start the primary master.

Step 3 Start the backup master.

Step 4 Launch the Tidal Web client and from the Fault Monitor pane, verify that both masters are running.

Primary Master Switchback

Primary master switchback is the process of switching scheduling duties from the backup master back to the primary master and restoring normal fault tolerance operation.

To switch back to the primary master on the Windows platform:

Note It is a recommended practice to prevent any new jobs from being submitted during this procedure by setting the system queue to 0. Let the active jobs complete before beginning the switchback.

Step 1 From the fault monitor machine, verify that the fault monitor is running.

Step 2 If the primary master is not running, start it.

Step 3 Stop the backup master.

Step 4 The primary master will leave standby mode and assume control.

Step 5 Start the backup master.

Step 6 Launch the Tidal Web client and verify in the Fault Monitor pane that both masters are running.

Switchback is complete once the primary master is actively controlling the production schedule and the backup master is in Standby mode. Be sure to reset the system queue to its original setting.

Installing the Agent

An agent is a separate installation component of TES that runs jobs on behalf of the master. Offloading jobs to agents frees the master for intensive scheduling tasks such as production compiles. Agents exist for various platforms. Check with your sales representative for the current list of the types of agents available.

Prerequisites

OS	Version	Chipset	32-bit	64-bit	JVM	Processor	RAM	Disk
Windows	Server 2012	Intel/AMD	X	X	.NET 2.0	Pentium 800MHz	512 MB	100MB Disk (program & data)
Windows	Server 2008 Standard Edition	Intel/AMD	X	X	.NET 2.0	Pentium 800MHz	512 MB	100MB Disk (program & data)
Windows	Server 2008 Enterprise Edition	Intel/AMD	X	X	.NET 2.0	Pentium 800MHz	512 MB	100MB Disk (program & data)
Windows	Server 2003 (Cluster) PS Services Requires	Intel/AMD	X	X	.NET 2.0	Pentium 800MHz	512 MB	100MB Disk (program & data)
HPUX	11.11	PA-RISC	X		HP 1.7.0	100 MHz	512 MB	100MB Disk (program & data)
HPUX	11.23, 11.31	Itanium		X	HP 1.7.0	100 MHz	512 MB	100MB Disk (program & data)
AIX	6.1	PowerPC/RISC	X	X (32-bit emulation mode only)	IBM 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
								(Continued)

OS	Version	Chipset	32-bit	64-bit	JVM	Processor	RAM	Disk
AIX	5.3 TL 5, ~~6~~, 9, 10, 11	PowerPC/RISC	X	X (32-bit emulation mode only)	IBM 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Solaris	9	Sparc	X	X	Sun 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Solaris	10	Sparc	X	X	Sun 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Solaris	10	Opteron		X	Sun 1.5.0			
Linux	Redhat Enterprise Linux AS Release 4 & 5	Intel/AMD	X	X	Sun 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Linux	SUSE Enterprise Server v11	Intel/AMD	X	X	Sun 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Linux	Oracle Enterprise Linux 5.2 (Same as Redhat)	Intel/AMD	X	X	Sun 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Linux	openSUSE 10.2 (i586) - Kernel 2.6.18.8-0.9-default	Intel/AMD	X	X	Sun 1.5.0_14	100 MHz	512 MB	100MB Disk (program & data)
Linux	Cent OS 5.4	Intel/AMD	X	X	Sun 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Linux	Linux Kernel 269 or above	PowerPC	X	X	IBM Java 1.5	100 MHz	512 MB	100MB Disk (program & data)
zLinux	Suse SLES_ (Suse Linux Enterprise Server) R9 in a 32 bit image. Kernel level is 2.6.5-7.244+	zSeries	X	X	1.4+	100 MHz	512 MB	100MB Disk (program & data)
Tru64	5.1B	Alpha		X	HP 1.4.2_7+	100 MHz	512 MB	100MB Disk (program & data)
VMWare	ESX 3.0, ESXi 3.5, ESXi 4.0							
Microsft Virtual Server	2005							
OVMS	7.3+	Alpha		X	JVM 1.4+			
	8.2+	IA64						
								(Continued)
SCO,NSK, Parallel Virtuoso	Call					Call		
z/OS					JVM 1.4.2+			

Installing the Agent for Windows

Companies often need to provide centralized scheduling and administration of workloads that span multiple machines and multiple locations. TES master/agent architecture provides that capability.

In the basic TES network, the master uses a centralized database, containing all calendar and job scheduling information. One or more agent machines execute the production schedule. One or more client machines provides the TES user interface or console. The only prerequisite for the master/agent relationship is that the machine acting as the master must be on the same TCP/IP network as the machines serving as agents.

Scheduler provides agents for Windows environments and agents for Unix environments. This section discusses the Agent for Windows installation.

Installation Rights	Agent User Rights	Runtime User Rights
Local Administrator Able to access COM objects	Local System or if running under Domain\User must have local administrator rights including: • Logon as a service • Logon as part of the operating system • Replace a process token • Able to access COM objects On machines running Windows 2003 or later: • Bypass traverse checking • Adjust memory quotas for the process	• Logon as a batch job

Installing Agents

To install an agent:

Step 1 Load the installation DVD into your machine's DVD-ROM drive.

Note If you are not running the install from the installation DVD, skip to Step 4.

The Scheduler Installation screen displays.

Step 2 Click the **Tidal Agent for Windows** link.

Step 3 When the dialog box displays asking to save the file, click **Save File**.

Step 4 Double-click the *Agent_windows_TIDAL Agent.msi* file. The Security Warning dialog box displays.

Step 5 Click **Run**. The Status panel displays.

The Welcome panel displays.

Note If any other agents are running on the machine, a dialog box notifies you that the agent(s) must be stopped before the installation can continue.

Step 6 Click **Next**. The Choose Destination Location panel displays.

Step 7 Select the directory where the Scheduler files will reside:

- Click **Change** and select the appropriate file.

  -or-

- Accept the default location at *C:\Program Files*.

Step 8 Click **Next**. The Agent Port Number panel displays.

Step 9 Enter the port number that the agent will listen on. The default port is **5912**.

Step 10 Click **Next**. The Ready to Install the Program panel displays.

Step 11 Click **Install.**

Note Do not click **Cancel** once the installation process begins copying files in the Setup Status screen. Cancelling the installation at this point corrupts the installation program.

You will not be able to install the component without the help of Support. If you decide you do not want to install the component, you must complete the installation and then uninstall.

The Setup Completed panel displays.

Step 12 Click **Finish**.

Verifying the Installation

To verify installation:

Step 1 From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

Step 2 From the Services list, choose **AGENT_1**.

If the Tidal Service Manager displays the message *AGENT_1: Running* at the bottom, then the agent is running and the installation was successful.

Note If you want to edit the service parameters, click the ellipsis button to access the Service Configuration dialog box.

Configuring Agents

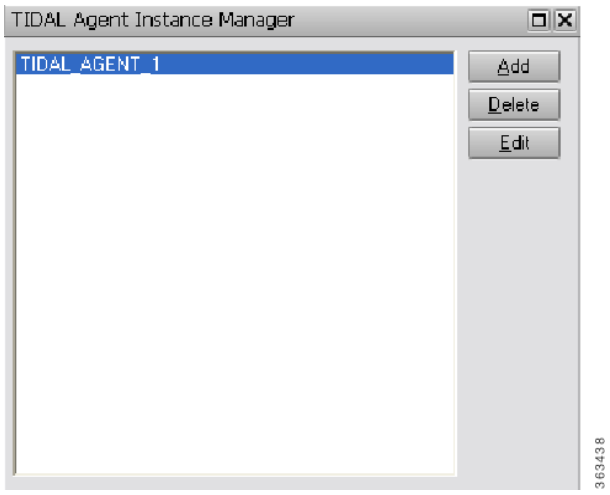
You can add and edit agent instances with the Agent Instance Manager.

Adding Agent Instances

To add an instance:

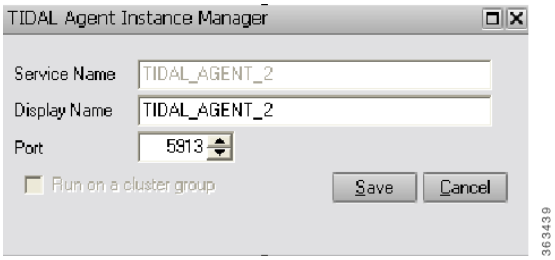
Step 1 From the Windows Start menu, choose **Programs > TIDAL Software > Agent > Instance Manager** to display the Instance Manager.

Figure 6-1 Tidal Agent Instance Manager



Step 2 Click **Add**. The following dialog box displays.

Figure 6-2 Tidal Agent Instance Manager 2



Step 3 Enter the following:

- Display Name – The name of the agent to add. The name in this text field is automatically generated as a possible candidate for the name of your agent. You can keep the name or change the name.
- Port – Select the port number the agent uses to listen for master connections.

Note Service Name is the name of the agent service. The name in this field is automatically generated and cannot be edited.

Step 4 Click **Save**.

Note To connect to the agent you just added, see "Defining an Agent Connection".

Editing Agent Instances

You can modify the port number and the name of the instance that is displayed but the service name remains the same.

Note The **Edit** button is unavailable as long as the agent is running.

To edit an instance:

Step 1 Stop the agent.

a. From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

b. From the Services list, choose **AGENT_1**.

c. Click **Stop**.

Step 2 Fromthe Windows Start menu, choose **Programs > TIDAL Software > Agent > Instance Manager** to display the Instance Manager.

Step 3 Select the instance.

Step 4 Click **Edit**. The Edit dialog box displays.

Step 5 Make the necessary edits, then click **Save**. The Information dialog box displays.

Step 6 Click **OK**.

Step 7 Re-start the agent.

a. From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

b. From the Services list, choose **AGENT_1**.

c. Click **Start**.

Deleting Agent Instances

Deleting agent instances does not delete the agent. Even if you delete all of the instances you must still uninstall the agent program to remove the agent.

Note The **Delete** button is unavailable as long as the agent is running.

To delete an instance:

Step 1 Stop the agent.

a. From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

b. From the Services list, choose **AGENT_1**.

c. Click **Stop**.

Step 2 Fromthe Windows Start menu, choose **Programs > TIDAL Software > Agent > Instance Manager** to display the Instance Manager.

Step 3 Select the instance.

Step 4 Click **Delete**. A confirmation message displays.

Step 5 Click **Yes**.

Note It is recommended that you do not delete the last agent instance called agent_instance_1. It is better to uninstall the agent program to remove the last agent instance. For instructions on how to uninstall the agent, refer to "Uninstalling Agents".

Note To delete an agent through the client, see "Defining an Agent Connection".

Configuring Agents for Windows

This section is optional.

After installing or adding agents, you can configure some Windows settings through the Services window, as documented below, or through the Tidal Services Manager as discussed in "Verifying the Installation".

To configure an agent for Windows:

Step 1 From the Windows Start menu, choose **Settings > Control Panel**.

Step 2 Double-click **Administrative Tools**.

Step 3 Double-click **Services**.

Step 4 Double-click the agent you just installed.

Step 5 On the **General** tab of the AGENT Properties dialog box, click **Stop** to stop the service.

Step 6 On the **Log On** tab, select **This Account**.

Step 7 Enter the requested information in the User Name/Domain Name and Password fields, then click **OK**.

Step 8 Right-click the agent and choose **Start**.

-or-

On the **General** tab, click **Start** to restart the agent.

Step 9 Close the Services and Administrative Tools dialog boxes.

Step 10 Go to the client and follow the procedure detailed in "Configuring Agents for Windows" to re-connect the agent.

Configuring Agent Parameters

Certain parameters of the Windows agent can be configured for the convenience of users. You modify the parameters of a Windows agent by adding the parameter statements to the command line or optionally (for most parameters) in the *tagent.ini* file. If the default location was used during the agent installation, the agent files are located in *C:\Program Files\TIDAL\Agent\Bin*.

Any parameters specified on the command line will take precedence over anything specified in *tagent.ini*. Some parameters that are needed during start still must be specified on command line (cpuload, msgthreads, rjaport).

The *tagent.ini* file in the *bin* directory works the same as in Unix agents, except the agent(s) definition and ports are not specified there. There is a [config] section and an [<Agent Name>] section. The parameters specified in the [config] section are global and the parameters specified in the [<Agent Name>] section only apply to that agent and will override specifications in the [config] section for the specific agent.

Following is an example of a *tagent.ini* file:

[config]

debug=y

logdays=3

logsize=1024000

encryptonly=y

sslvldcrt=y

vldhstcrt=y this is a synonym for **sslvldcrt**, as host validation also applies to SSH (only works in *tagent.ini*)

[TIDAL_AGENT_1]

debug=high

logdays=5

logsize=2048000

encryptonly=n

vldhstcrt=n

If specified in *tagent.ini,* these parameters do not need to be specified on command line.

Restart the agent after modifying any of the agent's parameters.

Sample and supported parameters list below:

The following agent parameters can be modified:

Debug

y|high

Where:

y (yes) turns on low-level debugging and **high** turns on maximum debug level.

Logdays

n

Where:

n is the number of days to preserve logs. Older logs will be deleted.

Sftpumask

<xxxx>

Where:

xxxx is permissions mask (4 digit octal) for files being created on Unix-type system by SFTP PUT actions. Default is '**0022**'.

Logfilesize

<xxxxxxxxx>

Where:

xxxxxxxxx is the maximum log file size in bytes (1048576 is 1MB). Default is 2048000.

Number of Message Threads

A new startup parameter, **MSGTHREADS=x,** has been added. It can optionally be specified on the startup line. The default number of threads that will handle messages is 5 and this seems optimal for 1-2 CPU machines. If you have more CPUs you may want to increase your thread count.

EncryptOnly Option

The **EncryptOnly** startup parameter option has been added. **EncryptOnly=Y** will cause an Agent to not remain connected to any Master that has turned off message encryption.

The default is **EncryptOnly=N**. It must be set to **Y** (Yes) in order for the more restrictive rules to take effect.

Secure FTP Host Validation

Tidal Enterprise Scheduler Agents v3.0 validates the host defined in FTPS SSL certificate. This is a change in behavior from the current Windows agent. The Host Validation feature can be disabled by specifying a **SSLVLDCRT** parameter on the agent command line. The default is **SSLVLDCRT=Y** (yes). You can turn this off by specifying **SSLVLDCRT=N**. Use Service Manager to edit the Agent startup parameters (add them to the **PATH** field). Use **vldhstcrt** as an optional synonym that is available only in *tagent.ini*.

AGTRESOURCE

AGTRESOURCE=CPU;VMEM enables monitoring CPU and VMEM monitoring with default time (15 seconds)

AGTRESOURCE=CPU,10000 enables monitoring only CPU with default time

AGTRESOURCE=CPU,10000;VMEM,15000 enables

The **AGTRESOURCE** specifications above indicate that (1) CPU utilization and Virtual Memory utilization should be monitored, (2) only CPU utilization should be monitored and change the time interval to 10 seconds (10000 milliseconds) and (3) CPU utilization should be monitored at a time interval of 10 seconds (10000 milliseconds) and that Virtual Memory utilization should be monitored every 15 seconds (15000 milliseconds).

The default time to send the resource value(s) to the Master will be 15 seconds and the minimum allowed will be 5 seconds.

MultiFTPStd

Y|N

Where:

Y is default, Standard FTP, no error if no files are operated on by MGET, MPUT or MDELETE.

N is non-standard FTP completion where the job will complete abnormal if no files are operated on.

FTPTimeout

nnnnnn

Where:
nnnnnn is timeout time in milliseconds. **0** will cause no timeout (infinity).

The Windows default timeout is 2 minutes (120000 milliseconds). This is a signed integer value.

Starting and Stopping Agents

To start or stop an agent:

Step 1 From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

Step 2 From the Services list, choose the name of the agent.

Step 3 Click **Start** to start the agent.

-or-

Click **Stop** to stop the agent.

Checking Agent Status

To check the status of an agent:

Step 1 From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

Step 2 From the Services list, choose the name of the agent.

The status of the agent is displayed at the bottom of the manager.

Configuring Jobs to Run in the Foreground

Since job processes do not normally require user interaction, they usually run in the background on the agent machine. If needed, you can configure your agent's system to run job processes in the foreground. Running processes in the foreground both allows user interaction with the process as it runs and enables more processes to run by providing another desktop. This can be configured to run in two different ways..

Note Changing settings in the Windows registry can have serious consequences on your computer system. Consult with your Windows system administrator before making any changes in the registry.

If you want to be able to interact with the process, you can configure the job to run in a command prompt window.

To configure jobs to run in the foreground:

Step 1 Open the Windows Registry Editor on the agent machine.

a. From the Window Start menu, choose **Run**. The Run dialog box displays.

b. Enter **regedit**.

c. Click **OK**.

Step 2 In the registry tree on the left, select the key at HKEY_LOCAL_MACHINE\SOFTWARE\TIDAL Software\Agent and create the key TIDAL_AGENT_1 (or the name of whichever defined Agent you wish to effect) below Agent.

Note On 64-bit systems, these keys and Strings need to be defined under "Wow6432Node" e.g. HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TIDAL Software\Agent\...

Step 3 Right-click the TIDAL_AGENT_1 key and choose **New > String Value** from the resulting menu.

Step 4 Name the new key that is created on the right pane, JobLaunchMode.

Step 5 Right-click the new JobLaunchMode key and select the Modify option from the context menu to display the Edit String dialog box.

Step 6 In the Value Data field, type one of the following numeric values to configure the appearance of the command prompt window:

0 = Hides the command prompt window and activates another window.

1 = Activates the command prompt window and displays it minimized.

2 = Activates the command prompt window and displays it in its current size and position.

3 = Activates the command prompt window and displays it at maximum size.

4 = Activates the command prompt window and displays it at minimized size.

5 = Displays the command prompt window in its current size and position but the window is not activated.

6 = Displays the command prompt window at its most recent size and position but the window is not activated.

7 = Activates and displays a window at its original size and position. Recommended when displaying the command prompt window for the first time.

If needed, you can repeat this procedure for the other agent instances that are listed in this key.

To revert back to the original configuration, delete the registry key that was added.

If you want the job process to run in the foreground without interacting with the job, you can run it from the default desktop.

Configuring Jobs to Run from the Default Desktop

To run a job from the default desktop:

Step 1 Open the Windows Registry Editor on the agent machine.

a. From the Windows Start menu, choose **Run**. The Run dialog box displays.

b. Enter **regedit**.

c. Click **OK**.

Step 2 In the registry tree on the left, select the key at HKEY_LOCAL_MACHINE\SOFTWARE\TIDAL Software\Agent and create the key TIDAL_AGENT_1 (or the name of whichever defined Agent you wish to effect) below Agent.

Note On 64-bit systems, these keys and Strings need to be defined under "Wow6432Node" e.g. HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TIDAL Software\Agent\...

Step 3 Right-click the TIDAL_AGENT_1 key, then choose **New > String Value** from the resulting menu.

Step 4 Name the new key that is created on the right pane, JobUseDefDesktop.

Step 5 Right-click the new **JobUseDefDesktop** key and choose **Modify** from the context menu to display the Edit String dialog box.

Step 6 In the **Value Data** field, type **1**.

If needed, you can repeat this procedure for the other agent instances that are listed in this key.

To revert back to the original configuration, delete the registry key that was added.

Configuring a Windows Agent to be a Remote Job Adapter Proxy

Designating the Port for HTTPS

To designate the HTTPS port:

Step 1 From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

Step 2 Click the ellipsis button to display the Service Configuration dialog box.

Step 3 In the Path field, edit the command line of the Agent by entering the following parameter:

RJAPort=PPPPP

Where **PPPPP** (e.g. **50001**) is the port number you want to use for the HTTPS connection from the Adapter.

For example:

"C:\Program Files\TIDAL\Agent\Bin\TidalAgent.exe" AGENT=TIDAL_AGENT_1 PORT=5912 PATH="C:\Program Files\TIDAL\Agent" RJAPort=PPPPP

Step 4 Click **OK**.

Step 5 Allow Service Manager to restart the agent when you save the change.

Note The proxy support will not be available in this Agent if the RJAPort is not specified in the command line. The Agent will not be usable by the Adapter until the RJAPort parameter is specified.

Note After adding the RJAPort parameter, you will need to add another dependency to the Agent service definition called HTTP SSL. You can do this by going into Service Manager and clicking the ellipses (...) for the specific agent, selecting the 'Dependencies' tab, and then selecting 'HTTP SSL' as a new dependency. The Agent will not start automatically at system start-up with-out adding this dependency.(May not be available in Windows 2008 and beyond).

Assigning Certificate to the Port for HTTPS

If your machine already has a valid server certificate, you should only have to perform <Jumps>Step below.

To create a self-signed host certificate and configure it to a port:

Step 1 Open a DOS prompt (Command Shell).

a. From the Windows Start menu, choose **Run**. The Run dialog box displays.

b. Enter **cmd**.

c. Click **OK**.

Step 2 Enter the following to create and install a self-signed certificate in the certificate store:

```
makecert -r -pe -n "CN=localhost" -eku 1.3.6.1.5.5.7.3.1 -ss my -sr
localMachine -sky exchange
```

Note makecert is available in the SDK if you have Visual Studio 2005 installed (*Microsoft Visual Studio 8\SDK\v2.0\Bin*). There are other ways to get a certificate, Google will give you several options.

Step 3 Start Microsoft Management Console (mmc) and copy the certifcate "local" located in *Personal* > *Certificates* into *Trusted Root Certification Authorities* > *Certificates*.

Step 4 At the DOS prompt (Command shell) run:

Note The port used to connect from the master to the proxy agent via HTTPS (the RJAPORT) requires that it be configured to use SSL.

For pre-2008 systems:

httpcfg.exe set ssl -i 0.0.0.0:PPPPP -c "Root" -h XXXXX

where **0.0.0.0:PPPPP** is the IP and port. This is for **https://localhost:PPPPP**, where **XXXX** is the Thumbprint value of the local certificate. To obtain the thrumbprint of a certificate, open the certificate and click the **Details** tab. Copy the thumbprint and delete all blanks (spaces) between numbers in 'Thumbprint'

Note It is critical that the name after '-c' in the httpcfg set matches the store that the certificate is in, Root is recommended (see below).

Store Names:

- AddressBook -The X.509 certificate store for other users.
- AuthRoot - The X.509 certificate store for third-party certificate authorities (CAs).
- CertificateAuthority - The X.509 certificate store for intermediate certificate authorities (CAs).
- Disallowed - The X.509 certificate store for revoked certificates.
- My - The X.509 certificate store for personal certificates.
- Root - The X.509 certificate store for trusted root certificate authorities (CAs).
- TrustedPeople - The X.509 certificate store for directly trusted people and resources.
- TrustedPublisher - The X.509 certificate store for directly trusted publishers.

For post-2008 systems:

netsh http add sslcert ipport=0.0.0.0:PPPPP certhash=XXXX appid={YYYYYY}

where **ipport=0.0.0.0:PPPPP** (e.g. **0.0.0.0:50001**) is IP and port, this is for **https://localhost:PPPPP**.

`certhash= XXXX` is the Thumbprint value of the local certificate. To obtain the thrumbprint of a certificate, open the certificate and select the Details tab. Copy the thumbprint and delete all blanks (spaces) between numbers in 'Thumbprint'.

`appid={YYYYYY}` is a GUID identifying the owning application.

Step 5 Click **OK**.

Uninstalling Agents

To uninstall the agent, you must use the **Add/Remove Programs** utility in the Windows Control Panel.

To uninstall an agent:

Step 1 Close the TES client to begin the uninstallation process.

Step 2 From the Windows Start menu, choose **Settings>Control Panel**, then double-click **Add or Remove Programs**.

Step 3 Scroll down the list of programs installed on the machine to the Scheduler program.

Step 4 Click the Scheduler program to highlight it.

Step 5 Click **Remove** to start the uninstallation process.

Step 6 When prompted to confirm that you want to uninstall the program, click **OK**.

Step 7 Click **Finish** to end the uninstallation process.

Step 8 Reboot the machine to save the changes to the registry.

Note Occasionally, an empty folder may be left in the Start menu after uninstalling Scheduler components. If this occurs, go to the Programs directory and manually delete the empty folder. The installation log file must also be manually deleted.

Installing the Agent for Unix

Companies often need to provide centralized scheduling and administration of workloads that span multiple machines and multiple locations. TES master/agent architecture provides that capability.

In the basic TES network, the master uses a centralized database, containing all calendar and job scheduling information. One or more agent machines execute the production schedule. One or more client machines provides the TES user interface or console. The only prerequisite for the master/agent relationship is that the machine acting as the master must be on the same TCP/IP network as the machines serving as agents.

TES provides agents for Windows environments and agents for Unix environments. This chapter discusses the Agent for Unix installation.

Installing the Agent for Unix from the Command Line

Before installing the Tidal Agent for Unix, backup your files and gather the following information:

- Name of the user who will own the agent
- Port number for the agent
- Directory path for the Java Virtual Machine (JVM)

To install the agent from the command line:

Step 1 Insert the installation DVD-ROM into the machine you want to install the agent on.

Step 2 Login as root.

Step 3 Copy the *install.sh* and *install.tar* files from the directory on the DVD-ROM (**<DVD-ROM>\agent\unix\cmdline**) to your temp directory..

Note Do not unpack the install.tar file. The file will automatically unpack during the installation process

Step 4 Change the permissions on the *install.sh* file in the directory to make the file executable:

chmod 554 install.sh install.tar

Step 5 Begin the installation by entering:

./install.sh

An introduction screen displays as the installation program begins.

Step 6 Type **Y** to continue the installation and press **Enter**. The Select the Owner screen displays.

The top of the screen shows the users defined on the machine you are installing on. In some cases, you may want to select a user who is not defined on the local machine but is defined as a NIS user allowing the user to install over the network.

Step 7 Enter the name of the user to own the agent.

Note Carefully consider which user to run the agent as. It may be desireable to create a user specifically for this purpose.

Step 8 Press **Enter**. The Select the Location screen displays.

Step 9 Type **Y**, then press **Enter.**

Note Carefully consider which user to run the agent as. It may be desireable to create a user specifically for this purpose.

The Agent Configuration Menu screen displays.

Step 10 Type **1** to select the Add Instance option, then press **Enter.** The Select the Location for the Agent Files screen displays.

Step 11 Enter the information you gathered before beginning installation:

- Name to call the agent
- Number of the port the agent should use
- Directory path for the Java binary files (JVM)

Step 12 Press **Enter**. A confirmation summary screen displays the information that you entered.

Step 13 If the information is correct, press **Enter**.

-or-

If the information is not correct, type **n**. You are prompted again for the name, port number, and directory path for the agent.

Configuring Agents

You can configure Unix agents (add and delete agent instances) using the **Agent Configuration Menu**.

To display this menu:

Step 1 Log on as agent owner on the agent machine.

Step 2 Go to the *bin* directory by entering:

cd /opt/TIDAL/Agent/bin

Step 3 Type in the following:

./tagent config

The **Agent Configuration Menu** displays.

Adding Agent Instances

To add an instance:

Step 1 In the Agent Configuration Menu enter **1 a**nd press **Enter**.

Step 2 Enter the name of the agent, its port number and the directory path to the Java binaries and then press **Enter**.

Step 3 Enter **Y** and press **Enter**. An agent instance is added.

Step 4 Start the agent by entering:

./tagent <agent name> start

Viewing the Status of Agent Instances

View the status of an agent by entering in the *bin* directory:

./tagent <agent name> status

Once you have entered that command a status screen displays.

Deleting Agent Instances

To delete an instance:

Step 1 Stop the agent.

Step 2 In the Agent Configuration Menu enter **3** and press **Enter**. The Select Agent Instance to Delete panel displays.

Step 3 Type the number of the instance to delete.

Step 4 Press **Enter** to delete the instance.

Configuring Agent Parameters

Certain parameters of the Unix agent can be configured for the convenience of users. You modify the parameters of an agent by changing the parameter values in the *tagent.ini* file. The *tagent.ini* file is located in the Unix agent directory. If the default location was used during the agent installation, the agent files are located at */opt/TIDAL/Agent/bin*. Following is an example of a *tagent.ini* file:

```
# ==============================================
# Agent Configuration Information
# ==========================================
[config]
agents=sun02,sun11,aix02,test
degbug=yes
ovb=tidaldebug
java=/usr/bin/
#sslvldcrt=n
sshvldhst=/home/secure/prd2_id_rsa.pub
sslvldhst=/home/secure/vvm1.pem


[test]
port=5915
java=/usr/j2rel.4.2_06/bin
minmem=32
maxmem=64
logdays=5
```

```
[sun02]
port=5915
java=/usr/j2rel.4.2_06/bin
sslvldcrt=n

[sun11]
port=5915
encryptonly=y

[aix02]
port=5915
java=/usr/java5_64/bin
sslvldcrt=/home/secure/host.crt
ulimitold=y
~
~
~
~
~
"tagent.samp" 34 lines, 592 characters
```

Restart the agent after modifying any of the agent's parameters.

The following agent parameters can be modified:

Debug

y

Where:

y (yes) turns on low-level debugging of startup activity of agent.

Ovb

tidaldebug

Where this statement turns on the maximum level of debug logging of agent activity.

Logdays

n

Where:

n is the number of days to preserve logs. Older logs will be deleted.

Sftpumask

<xxxx>

Where:

xxxx is permissions mask (4 digit octal) for files being created on Unix-type system by SFTP PUT actions. Default is **0022**.

profile=y

The profile parameter is used to have the agent permanently override the For Unix, source user's profile option on the Options tab of the Job Definition dialog box.

Specifying the **y** value means that all jobs that run on this agent will source the specified runtime user profile. In effect, a y forces For Unix, source user's profile to be set for all jobs.

Leaving the parameter value blank (the default value) or specifying a n value means that only jobs with the For Unix, source user's profile option selected will source the user's profile.

homedir=y

The `homedir` parameter specifies the agent's home directory.

A `y` value means that the starting path will be the runtime user's home directory instead of the agent's home directory.

Leaving the parameter value blank (the default value) or specifying a **n** value means that the home directory remains the directory where the agent is installed..

Note This parameter will override the working directory setting in the master for all jobs to the user's home directory.

minmem and maxmem

The `minmem` and `maxmem` parameters control how many MB of memory should be allocated to the agent processes. These memory parameters can be adjusted as individual needs warrant. Your system may need more or less than the default memory allotments.

The `minmem` parameter specifies that at least the amount of RAM specified should be available. The default value is 16 MB of RAM.

The `maxmem` parameter specifies that no more than the amount of RAM specified should be available for the agent processes. The default value is 48 MB of RAM.

For example, to set the minimum memory to 32 MB and the maximum memory to 64 MB, specify:

minmem=32

maxmem=64

fp=path of environment file

The `fp` parameter specifies a particular environment file to be used by an agent instance. To associate an environment file to an agent, enter the pathname of the environment file using the following format, **`fp=/folder/file`**.

Each agent instance can be assigned its own environment file and its associated environment variables with their various values. Each variable specified in the environment file should follow a **`variable=value`** format as in the following examples:

TZ=CST
SchedulerT=1
PATH=/usr/sbin

Jobstopwait=n seconds

The Jobkillwait parameter specifies the time interval between sending a SIGTSTP warning that a Unix job is about to be put on hold and actually sending the SIGSTOP signal to pause the job.

The default value is 1 second before pausing the job but the number of seconds between the warning and the actual pausing of the job can be modified from this parameter.

Jobkillwait=n seconds

The Jobkillwait parameter specifies the time interval between sending a SIGTERM warning that a Unix job is about to be aborted/cancelled and actually sending the SIGKILL signal to abort/cancel the job.

The default value is 5 seconds before cancelling the job but the number of seconds between the warning and the actual cancelling of the job can be modified from this parameter.

EncryptOnly Option

The EncryptOnly startup parameter option has been added. EncryptOnly=Y will cause an Agent to not remain connected to any Master that has turned off message encryption.

The default is EncryptOnly=N. It must be set to **Y** (Yes) in order for the more restrictive rules to take effect.

Secure FTP Host Validation

Tidal Enterprise Scheduler Agents v3.0 validates the host defined in FTPS SSL certificate. This is a change in behavior from the current Windows agent. The Host Validation feature can be disabled by specifying a SSLVLDCRT parameter on the agent command line. The default is **SSLVLDCRT=Y** (yes). You can turn this off by specifying SSLVLDCRT=N. Use Service Manager to edit the Agent startup parameters (add them to the PATH field).

SSLVLDHST

<location of file containing host certification key file>

For FTPS Host validation, the location of the file containing the public host certificates (generally self-signed), if not authenticated through a Certificate Authority.

The certificates in the file must be of the OpenSSL PEM format and be bracketed as follows:

```
-----BEGIN CERTIFICATE-----
... first certificate ...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... second certificate ...
-----END CERTIFICATE-----
```

SSHVLDHST

<location of SSH host key file>

For SFTP Host validation, the location of the file containing the public Keys for the servers that SFTP connections will be established with.

Provides a list of hosts and their associated public keys in the given file. The format of the file is similar to that used in OpenSSH. Each line contains the name of a host followed by its IP address (separated by a comma), the type of key it has, and its key (in base-64 printable form). For example:

```
jackspc,192.168.1.1 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIE...
```

cpuload

The cpuload parameter controls whether the Agent sends system load information back to the master. The default is 'no'. The information is only needed if you are using the Balanced option on an Agent list. When 'yes' is specified, the load information will be collected and sent back to the master at one minute intervals.

AGTRESOURCE

AGTRESOURCE=CPU;VMEM enables monitoring CPU and VMEM monitoring with default time (15 seconds)

AGTRESOURCE=CPU,10000 enables monitoring only CPU with default time

AGTRESOURCE=CPU,10000;VMEM,15000 enables

The AGTRESOURCE specifications above indicate that (1) CPU utilization and Virtual Memory utilization should be monitored, (2) only CPU utilization should be monitored and change the time interval to 10 seconds (10000 milliseconds) and (3) CPU utilization should be monitored at a time interval of 10 seconds (10000 milliseconds) and that Virtual Memory utilization should be monitored every 15 seconds (15000 milliseconds).

The default time to send the resource value(s) to the Master will be 15 seconds and the minimum allowed will be 5 seconds.

Starting and Stopping Agents

You can start or stop an agent by entering on the command line:

./tagent <agent name> start

-or-

./tagent <agent name> stop

Note You should stop all Unix agents before rebooting the Unix system. It is recommended to add the agent stop command to a Unix system shutdown script to be used when restarting a Unix system.

Note When issuing the tagent start command, verify that you are logged on as the user intended to run the agent.

Preventing Unauthorized Users from Using an Agent

The Unix agent can be configured to allow only specific users to run jobs on that agent. A list of users can be created to exclude or allow users access to the agent. If an unauthorized user tries to run a job on an agent that he is excluded from, the job will end with an "Error Occurred" status.

To exclude users from an agent

Step 1 Login as the owner of the agent.

Step 2 Create a file called *Users.cfg* in the agent's root directory, e.g., **/opt/TIDAL/Agent/<name of agent>**.

Note The file name, *Users.cfg*, is case sensitive, so only the first letter should be capitalized and the rest of the name should be lower-case.

Step 3 Change the *Users.cfg* file permissions to limit access to just the agent owner, by entering:

chmod 700 Users.cfg

Step 4 In the *Users.cfg* file, enter:

EXCLUDE

Step 5 List those users that will be prohibited from accessing the agent.

Each user must be on a separate line.

Following is an example of a *Users.cfg* file:

EXCLUDE
JDegnan
MCarpent
TESUser

If the list of users to exclude is long, enter **INCLUDE** instead of **EXCLUDE**. Then you can list the users to give access to the agent if this is easier.

Step 6 To ensure that the changes take effect, stop and restart the agent.

-or-

Disconnect and reconnect the client connection to the agent.

Note While this procedure prevents unauthorized users from running system commands on an agent they are excluded from, FTP jobs can still be run from the agent because an user does not login to an agent to FTP.

Uninstalling Agents

The Agent for Unix is uninstalled from the command line.

Uninstalling Using the Command Line

The uninstallation procedure will not be successful if the agent is running. Stop the agent before removing the TES Agent for Unix.

To uninstall:

Step 1 Check the status of the agent to verify that it is not running by entering:

./tagent <agent name> status

Step 2 If the status check shows the agent is not running, proceed to the next step.

-or-

If the status check shows the agent is running, stop the agent by entering:

./tagent <agent name> stop

Step 3 Once the agent is stopped, return to the location where you installed the Unix agent. By default, this location is the */opt* directory.

Step 4 At the command prompt, enter:

cd /opt

Step 5 Have your Unix administrator remove the agent directory and its contents

Connections and Agent Procedures

Defining an Agent Connection

To define a connection between the agent and the master :

Step 1 From the Navigator pane of the TES client, choose **Administration > Connections**.

-or-

Click the **Connections** button on the TES toolbar.

The Connections pane displays.

Step 2 Double-click the agent name.

-or-

Right-click in the Connections pane and choose **Add Connection > Agent for Windows** or **Add Connection > Agent for Unix** from the resulting menu.

The Connection Definition dialog box displays.

Step 3 Enter a name for the agent you installed.

Note This name does not have to match the machine name or instance name.

Step 4 On the General tab, configure:

- Job Limit – The maximum number of jobs you want to run concurrently on this agent. It is recommended that you do not run more than 80 jobs at once.
- Default Runtime User – The default runtime user that will appear when creating a new job on this agent.

Step 5 Select the Enabled option.

Step 6 Select the Connection tab.

Step 7 In the Machine Name field, enter the name or IP address of the machine that the agent is installed on. This name must be a valid DNS name.

Step 8 In the Master-to-Agent Communication Port field, enter the agent's listener port number specified when installing the agent.

Step 9 If you want to enter a description of this agent, select the Description tab and enter a description; otherwise, click **OK** to save the connection.

Deleting an Agent Connection

To delete an agent connection:

Step 1 From the Connections pane, select the agent to delete.

Step 2 Click the **Delete** button on the TES toolbar or press the **Delete** key on your keyboard.

Note You cannot delete an agent connection unless you are connected to the master. You can delete an agent connection that is currently in use, however, jobs that were to run on that agent will be disabled. Those jobs will not run again until you assign them to a valid new agent.

Enabling or Disabling Agents

You can disable an agent if you do not want it to run jobs. If a job is about to be submitted to run on a disabled agent, its status changes to *Agent Disabled*.

To enable/disable an agent:

Step 1 From the Navigator pane, choose **Administration > Connections** to display the Connections pane.

Step 2 Double-click the agent.

-or-

Select the agent and click the **Edit** button on the TES toolbar.

Step 3 In the agent's Connection Definition dialog box:

- To enable the agent, select the Enabled option.
- To disable the agent, clear the Enabled option.

Note You can also enable or disable agents using the context menu in the Connections pane.

Step 4 Click **OK**.

Changing an Agent's Job Limit

You can change an agent's job limit to specify the number of jobs that can run on it concurrently. You can also control the number of jobs running concurrently using queues.

To change an agents job limit:

Step 1 From the Navigator pane, choose **Administration > Connections** to display the Connections pane with the licensed computers.

Step 2 Double-click the agent to edit or select the agent and click the **Edit** button on the TES toolbar to display the agent's connection definition.

Step 3 Select the General tab if it is not showing.

Step 4 In the Job Limit field on the General tab, change the job limit to the desired value.

Step 5 Click **OK**

Changing the Name of the Computer Displayed in TES

To change the name of the computer:

Step 1 From the Connections pane, double-click the licensed computer to edit or select the computer and click the **Edit** button. The licensed computer's Connection Definition displays.

Step 2 In the Name field, change the computer's name. This name is used when referring to the computer on TES panes and dialog boxes.

Step 3 Click **OK**.

Changing the Machine Hostname of the Computer

To change the hostname of the computer:

Step 1 From the Connections pane, double-click the licensed computer to edit, or select the computer and click the **Edit** button to display the licensed computer's Connection Definition dialog box.

Step 2 Select the Connection tab.

Step 3 In the Machine Name field, update the computer's name.

This name can be found in the DNS section of the TCP/IP protocol of your network configuration. See your System Administrator for more information.

Cluster Configuration

Configuring a Cluster to Run the Windows Agent

The Agent for Windows can run in a Windows cluster environment. A cluster environment is defined as multiple machines working together as one system. The cluster environment provides a level of redundancy so that if one of the machines in the cluster fails, another machine is available to replace the failed component.

The following instructions describe how to configure a two node cluster environment to run the Windows agent offered by Scheduler.

Prerequisites

Before installing the Tidal Agent for Windows on the nodes of a cluster, you must first complete and/or verify the following on each node:

- Verify that the systems on each node are identical
- Verify that the agent machines in each node meet the hardware and software requirements specified in the Installing the Agent for Windows chapter of the Installation and Configuration Guide for Scheduler.
- Verify that the user installing the Windows agent has the specified user rights including access to the registry on each machine.
- Verify that the cluster group has the following resouce types:
  - Network name
  - IP address
  - Physical disk

Configuring the Agents for a Cluster

During configuration, you should complete a step on a machine and then go around to the other machines in the cluster and do the same step. When that step has been performed on each machine in the cluster, return to the first machine and do the next step and then again do that step on the other machines in the cluster, and return to the first machine and do the next step, etc.

An agent instance must exist on every node in the cluster before it can be configured to run as a cluster. This means that if you add a third agent instance to a machine, before you configure that instance, go to all of the other machines in the cluster and add a third instance.

To configure the agents:

Step 1 Verify that the cluster works correctly.

Check that the cluster software is installed and configured correctly by forcing a failure on a server. Be sure that a failover to another server occurs as intended and that control can be returned to the server that failed. Your Windows Cluster Administrator should help you with this.

Step 2 Install the Agent for Windows on the first cluster node.

Be sure to install the agent to a non-clustered physical disk on the local machine using the default directory path during installation.

Caution You must install the agent on the same disk drive letter on each cluster node. For example, if you install the agent on the C drive of one node, the agent must be installed on the C drive of the other nodes also.

Step 3 Stop the agent if it is running.

Note If an agent instance is configured as part of a cluster, you will not be able to stop the agent. You must stop the agent service.

Step 4 An agent instance must exist on every node in the cluster before it can be configured to run as a cluster. If you are adding an agent instance, add the agent instance to a machine. See "Installing the Agent for Windows". Go to each of the other nodes in the cluster and add that same instance.

Once each of the nodes on the cluster have the same agent instance on it, you can edit the agent instance to configure it for the cluster.

Step 5 From the Windows Start menu, choose **Programs > TIDAL Software > Agent > Instance Manager** to display the Agent Instance Manager.

Step 6 Select the first agent instance and click the **Edit** button to display the Agent Instance Manager's configuration screen.

If this agent instance is on a node that is configured for a cluster with an existing agent service, the Run on a cluster group option is available. If the node is not part of a cluster than this option is unavailable. You cannot proceed any further without verifying with your Windows Cluster Administrator that the node is correctly configured as a member of the cluster.

Step 7 Select the Run on a cluster group option to expand the screen to display the cluster configuration fields.

Step 8 In the Cluster Group field, select which cluster group that this agent instance belongs to.

Step 9 In the Physical Disk field, select the disk that the agent instance resides on. All the disks that were created on all of the cluster groups are listed. Be sure to select a disk that exists on the cluster group you selected.

Step 10 In the Work Directory field, enter the pathname to the work directory that was created for the cluster group.

Note This Work Directory must be on a shared disk that moves with the active node on a fail-over.

Step 11 In the Cluster Nodes field, select which node this agent instance is on. When the fields are completed, click the **Save** button.

Step 12 Go to each node and repeat this procedure for each agent instance.

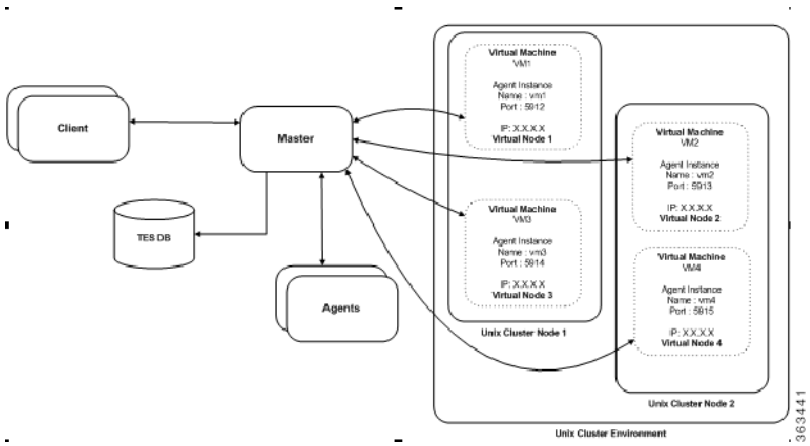
Step 13 When each agent instance on each node is configured properly, start each clustered agent instance from its active node using Scheduler's Service Control Manager. Starting the agent instance in the Service Control Manager automatically starts the agent resource in the Windows Cluster Administrator.

Configuring a Cluster to Run the Unix Agent

The Agent for Unix can run in a Unix cluster environment.

The following diagram illustrates how Enterprise Scheduler is configured in an environment with Unix cluster

Figure 6-3 Unix Cluster Environment



The Master component connects to agent instances associated to a virtual machine using the virtual machine name and IP address and the port number. This allows the Scheduler master to maintain the agent connection when the cluster management software moves the virtual machine to another participating node.

Prerequisites

To configure the Tidal Agent for Unix on a cluster to follow the virtual machine, the following prerequisites must be met:

- The SAN/NFS Agent installation location must be mounted at the same mount point on all of the cluster nodes.
- Java Virtual Machine (JVM) prerequisites must be installed on all of the nodes. These prerequisites for the JVM include installing all OS patches, maintaining kernel parameters, etc.
- The same JVM must be installed on each of the physical nodes (and, whenever possible, the JVM should be installed in the same directory location on each of the nodes.)
- The Agent owner account must be accessible from all of the nodes.
- The minimum requirements for the Scheduler agent must be met on each of the individual nodes.
- The installation and configuration of Tidal Agents for Unix in a cluster can be broken down into the following four steps:
  - Installing Agent files on the SAN/NFS mount location.
  - Configuring agent instances (only one instance per virtual machine).
  - Configuring the cluster Virtual Machine.
  - Configuring Scheduler to connect to the agent instances on a virtual machine.

Installing Agent on the SAN/NFS Location

To install the agent on the SAN/NFS location:

Step 1 FTP the agent installation files to one of the participating nodes in the cluster.

Step 2 Login as root to the same physical node where the agent installation files were copied.

Step 3 Change to the directory where the agent installation files were copied.

Step 4 Follow the normal Agent installation procedure that is described in the "Installing the Agent for Windows" with the following exceptions:

- When entering a location for the agent files, select the SAN/NFS location (visible to all the nodes).
- Ensure that the Agent owner is a NIS user or if the agent owner is a local user on all of the participating nodes than the Agent owner must have the same UID and GID.
- At the end of the installation procedure, do not configure any agent instances.

Configuring Agent Instances

To configure agent instances:

Step 1 Identify each of the Virtual Machines that require an agent instance associated with it.

Step 2 Login to a cluster node as the agent owner.

Step 3 Change to the agent *bin* directory and run the t**agent –config** command to begin the agent configuration.

Step 4 Select the Add Instance option and add one instance for each of the virtual machines.

- It is a best practice to give each agent instance the same name as the virtual machine hostname to help identify which instance is associated to which virtual machine.
- The port number for each agent instance must be unique.

The Agent Instance configuration file will look similar to the following example that shows a configuration file for a cluster with four virtual machines:

Agent Instance configuration file

[/opt/TiDAL/Agent/bin/tagent.ini]

```
# ================================================================
# Agent Configuration Information
# ================================================================

[config]
agents=vm1,vm2,vm3,vm4

[vm1]
port=5912

[vm2]
port=5913
```

[vm3]

port=5914

[vm4]

port=5915

Configuring Cluster Virtual Machine

This step varies from one cluster solution to another but basically all cluster solutions require the following three operations to enable the agent instance to be associated to the virtual machine.

- Start the Agent instance
- Monitor the Health of the Agent instance
- Stop the Agent instance

Start a Agent instance

To start an agent instance, issue the following command:

su <agent owner> -c "<agent install location>/bin/tagent <agent instance name> start"

Replace the text in brackets < > with the name of your agent owner and agent instance and the directory pathname to the agent files.

Monitor the Health of the Agent Instance

Check the status of the agent with the `tagent <agent>` status command as illustrated in the sample script below:

```
#!/bin/sh
cd /agentdir/bin/
./tagent $1 status | grep "Down"
if [ $? -eq 0]
then
echo "Agent $1 is down"
exit 1
fi
exit 0
```

Stopping the Agent Instance

Stop an agent instance with the following command:

<agent install location>/bin/tagent <agent instance name> stop

Replace the text in brackets < > with the name of your agent instance and the directory pathname to the agent files.

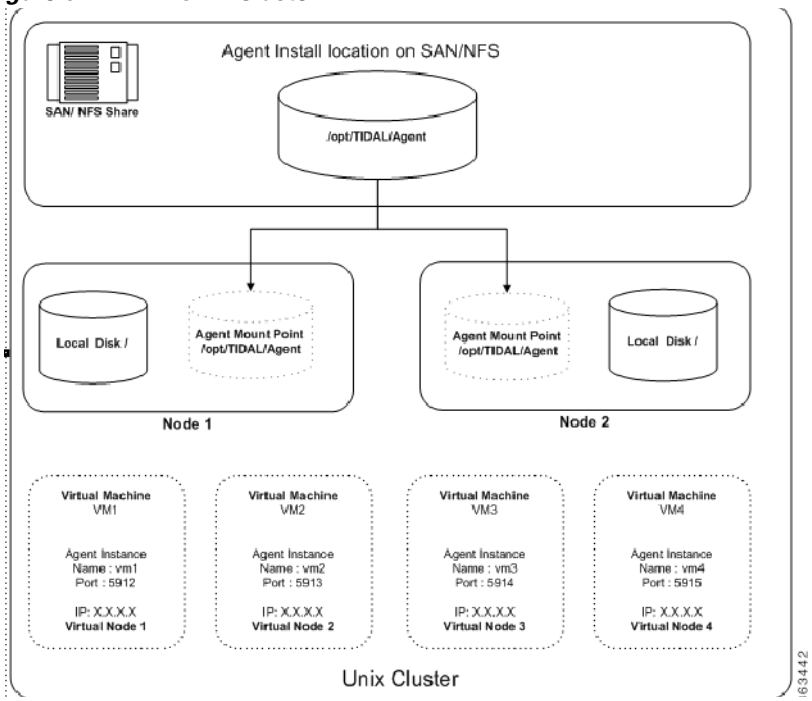
Configure Scheduler to Connect to Agent Instances on a Virtual Machine

Configuring the connection to the Agent instances in the Scheduler client is the same procedure as configuring other agent connections with the following exceptions:

- Use the virtual machine hostname/IP address instead of the physical node hostname.
- Use the agent instance port number for the agent instance that is associated with the virtual machine.

The following diagram illustrates an agent installed on a two node cluster with four virtual machines.

Figure 6-4 Unix Cluster



Agent/Master Secure Connection

In order to provide strict control over which Tidal Enterprise Schedulers (Enterprise Scheduler) Masters can connect to a specific agent, a *Masters.cfg* file has been implemented at the Agent. By specifying the Master 'alias', the Master 'alias' and a specific 'local' TCP/IP address or the Master 'alias', the specific 'local' TCP/IP address and a 'global' TCP/IP address you can uniquely identify the specific Enterprise Scheduler Masters that a Enterprise Scheduler Agent will create connections to.

The *Masters.cfg* file must be created in the Agents local directory. This directory is in the install path of the Agent and has the name of the Agent as it was specified when the Agent was defined. For example, by default, this would be something like:

- For Unix (Linux, z/OS)

  `/opt/TIDAL/Agent/TidalAgent1`

- For Windows

  C:\Program Files\TIDAL\Agent\TIDAL_AGENT_1

- For OVMS

  sys$sysdevice:[tidal.agent.tidalagent1]

This file should have limited access using native system access control definitions.

Agent Connect Protocol

The following describes the normal connection sequence for an Agent to Master connection to be established.

The Master connects to the Agent well-known port (default 5912, configurable). The Master sends a registration message to the Agent specifying the Masters IP address and listening port (and some other configuration information). This connection is then terminated.

For each Master that has registered as above, the Agent will attempt to connect using the information from the registration. This will happen each time the connection is lost for any reason.

The Agent will attempt to connect to the IP and port provided by the Master in the registration message. If this fails, the Agent will attempt to connect to the IP obtained from the network as the source IP (may be firewall IP) and the port provided in the registration message.

When the connection is made, the Agent will generate an encryption key based on a random seed. This encryption key and other configuration information about the Agent will be sent to the Master. The encryption key is 'wrapped' by a method that the Master knows how to 'unwrap' in order to get the raw key. This key is used to encrypt the body of all future messages (encryption is a configurable option that is on by default).

Masters.cfg

The *Masters.cfg* file contains the following structure:

Optional INCLUDE or EXCLUDE statement on first line. If specified, these one word entries must be on the first line. INCLUDE is the default if nothing is specified.

- INCLUDE - only the specified Masters with optionally specified IP addresses will be connected to by the Agent.
- EXCLUDE - the specified Masters will be specifically excluded from being connected to by the Agent.

Master entries of the form:

- MasterAlias

  The MasterAlias typically has the form 'ES_<hostname of master>_1' and is case-insensitive. If specified alone on the line, then only the MasterAlias will be verified that it matches what was presented by the Master in its registration message.

- MasterAlias:IPaddress1

  For connections that are 'local', i.e. their Master host machine IP addresses are directly accessible by the Agent, then only IPaddress1 needs to be specified. This address will be verified against the IP address presented by the Master in its registration message and the IP address obtained from the network as the origination of the connection that provided the registration message.

- MasterAlias:IPaddress1;IPaddress2

  For connections that must traverse a firewall, then IPaddress2 must be specified. IPaddress2 will be the externally known address of the firewall. The externally known address of the firewall is what will be obtained by the Agent when it retrieves the IP address of the origination of the connection through which the registration message was delivered .

For situations where a Master could have multiple IPs, Failover scenarios, or disaster recovery situations, the same MasterAlias can be specified with different IPaddress parameters.

Following is an example of a *Masters.cfg* file:

INCLUDE

hou-testvm-531:192.168.48.111;172.19.25.125

hou-testvm-531:192.168.55.211;172.19.25.125

zostest:192.168.95.92

zostest:192.168.42.92

catest

Troubleshooting

Verifying the Version of the Agent

When consulting with Technical Services about a problem with an agent, one of the most basic pieces of information they need is which version of the agent is being used.

To verify the version of the agent:

Step 1 From the Navigator pane of the client, choose **Administration > Connections** to display the Connections pane.

Step 2 In the various connections listed in the pane, locate the agent with the problem.

Step 3 Look in the Version column of that agent to see the version of the agent being used.

Diagnostics

Unix Agent

The first line of every Unix agent shell script must adhere to standard Unix scripting guidelines and refer to a shell; for example, **#!/bin/sh**. For more information, refer to your Unix system documentation or consult your System Administrator.

When the Agent for Unix generates errors and doesn't operate properly, you need to contact Technical Services to help you resolve the technical issues. However, Technical Services requires specific information on how the Agent for Unix is operating before they can track down the source of the problem. Before contacting Technical Services about an agent issue, you should turn on diagnostic logging to collect information about the way the agent is functioning. This is the first step that Technical Services will have you do, if you have not done it before contacting them.

To turn on diagnostic logging:

Step 1 On the agent machine type the following command to stop the agent:

./tagent <agent name> stop

Step 2 Go to the */bin* directory and locate the *tagent.ini* file for the desired agent.

Step 3 Inside the *tagent.ini* file, under the port setting, type the following:

ovb=Tidaldebug

Step 4 Save the file and its changes.

Step 5 Start the agent:

./tagent <agent name> start

Ideally, you want to reproduce the situation that caused the issue so the diagnostics can log what occurred in the system at that time. As soon as the problem reoccurs, contact Technical Services.

Step 6 Once the problem repeats itself and the diagnostic information is recorded, turn off the agent diagnostics by commenting out the debugging parameter:

#ovb=Tidaldebug

Step 7 Go to the *Log* directory to get the diagnostic file to send to Technical Services:

cd <agent directory>/<agent name>/logs

Each agent instance has its own directory. The diagnostic files are named *<FTP>.log*, *<agent name>.log* and *<master server>.log*.

Restarting the agent does not override the recorded information. Though only a small amount of information is normally recorded without the debug parameter, the file will continue to grow in size. You should delete or rename the file after you finish debugging the agent.

Note Whenever diagnostic logging is being used, you must carefully monitor the amount of disk and database space being consumed. Diagnostic logging can generate large amounts of data and affect system performance.

Windows Agent

To run diagnostics for the Windows agent:

Step 1 Login to the agent console as an authorized user.

Step 2 Using Service Manager, select the Agent that you wish to use diagnose.

Step 3 Add the following string to the end of the **Path:** field.

Debug=high

Step 4 Click **OK** at bottom of panel and respond yes to the "Would you like to restart the service?" pop-up.

To stop diagnostics, close the agent application window and restart the agent from the Service Control Manager.

Working With Agents

You can start and stop agents in your network at any time. A yellow agent status light at the bottom of the client screen indicates that you need to restart your agent(s).

Note Before starting or stopping the agent, check the agent's status using the Tidal Service Manager.

Checking Agent Status

The following steps are for Windows Agents only.

To check the agent status:

Step 1 On the agent machine, click the Windows **Start** button and then select **Programs > Tidal Software > Tidal Service Manager** to display the Tidal Service Manager.

Step 2 In the **Service** drop-down list, select the agent you wish to check so that it displays in the Service field.

Step 3 At the bottom of the Tidal Service Manager, the status of the selected service displays.

Note The Agent for Unix does not use the Tidal Service Manager so the command line is used to start, stop and check the status of the agent. Use the following commands:
To start: **./tagent <agent name> start**
To stop: **./tagent <agent name> stop**
To check agent status: **./tagent <agent name> status**

Starting the Agent

The following steps are for Java-based Agents only (**tagent** command).

To start the agent:

Step 1 From the Windows Start menu, choose **Programs > Tidal Software > Tidal Service Manager** to display the Tidal Service Manager.

Step 2 From the Service list, choose the correct agent if it is not displayedand click the **Start** button. The light will turn green when the agent starts.

Note The Agent for Unix does not use the Tidal Service Manager so the command line is used to start, stop and check the status of the agent. Use the following commands:
To start: **./tagent <agent name> start**
To stop: **./tagent <agent name> stop**
To check agent status: **./tagent <agent name> status**

Stopping the Agent

The following steps are for Windows Agents only (Service Manager).

To stop the agent:

Step 1 From the Windows Start menu, choose **Programs > Tidal Software > Tidal Service Manager** to display the Tidal Service Manager.

Step 2 From the Service list, choose the correct agent if it is not displayedand click the **Stop** button. The light will turn red when the agent stops.

DataMover Job Support

Note DataMover jobs are only supported on Unix/Linux agents.

By default, when the 3.1.0.02+ agent is installed, it can run with Java 1.4.x as previous agents, but it will not support Amazon S3 (AS3) or Hadoop DFS (HFS) DataMover operations. DataMover jobs sent to the default agent will fail with a 'wrong agent' indication.

In order to utilize AS3 or HFS DataMover functionality, you must be running the appropriate level of Java and you must copy the associated support files into the Agent/ lib directory. AS3 functionality requires Java 1.5 as a minimum and HFS functionality requires Java 1.6 as a minimum.

There are new subdirectories on the DVD image under the Agent/unix directory. There is a new DataMover directory with three subdirectories - AS3, HFS-A (Apache Hadoop) and HFS-C (Cloudera Hadoop) that contain the associated files to support the DataMover functionality, if the associated support is needed.

AS3 Functionality

The TAgent.AS35 file in the installed *Agent/lib* directory is the *TAgent.jar* file that is compiled with Java 1.5 and contains the AS3 interface support.It will replace the existing *TAgent.jar* file in the installed *Agent/lib* directory. Rename the existing *TAgent.jar file* (not using the .jar extension), if desired, and then copy or rename the *TAgent.AS35* file to *TAgent.jar*. The *tagent.ini* file for this installation of the agent must point to a Java 1.5 (or higher) or the default Java must be 1.5 (or higher).

Copy all files from the above referenced AS3 subdirectory into the *Agent/lib* directory.

AS3 Usage Notes

The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from 1 byte to 5 terabytes. The largest object that can be uploaded in a single PUT is 5 gigabytes. For objects larger than 100 megabytes, customers should consider using the Multipart Upload capability.

When using Multipart upload, each part must be at least 5 MB in size, except the last part. So, in the list of files provided on the dialog box, each must be at least 5MB other than the last file in the list.

HFS Functionality

The *TAgent.HFS6* file in the installed *Agent/lib* directory is the *TAgent.jar* file compiled with Java 1.6 and contains the Hadoop Distributed File System interface support. It will replace the existing *TAgent.jar* file in the installed *Agent/lib* directory. Rename the existing *TAgent.jar* file (not using the .jar extension), if desired, and then copy or rename the *TAgent.HFS6* file to *TAgent.jar*. The *tagent.ini* file entry for this installation of the agent must point to a Java 1.6 (or higher) or the default Java must be 1.6 (or higher). You can also run AS3 DataMover jobs with this *TAgent.jar*, but you must copy all the files from the AS3 subdirectory into the *Agent/lib* directory also in order to run AS3 jobs.

Apache Hadoop

HFS-A subdirectory contains jars related to apache.

It contains multiple sub directories - 1.1, and 1.1.2, each representing the corresponding version of Apache, that is, Apache 1.1, and Apache 1.1.2.

Copy all files from the above referenced *HFS-A* subdirectory into the *Agent/lib* directory.

Cloudera Hadoop

HFS-C subdirectory contains jars related to Cloudera.It contains subdirectories supporting CDH3 and CDH 4 versions.Copy all files from the above referenced *HFS-C* subdirectory into the *Agent/lib* directory.

MapR Hadoop

In order to use DataMover for MapR Hadoop, the MapR Client must be installed on the machine running the TES agent. The TES agent supports MapR Client versions 1.2.9 and 2.0.0. It is the user's responsibility to ensure that the MapR Client is installed properly and is communicating with the MapR Cluster. The following Web page contains information on how to set up the MapR Client:

http://www.mapr.com/doc/display/MapR/Setting+Up+the+Client

There are no files to be copied for MapR Hadoop. However, updates to the *tagent.ini* file are required. See "HFS Usage Notes" for details.

HFS Usage Notes

Agent Ini File

Kerberos Configuration

If the Agent is going to access any Hadoop file system that is secured by Kerberos, then the Kerberos Realm and Kerberos KDC Name must be specified in the Agent's *tagent.ini* file. The new parameters are **`KerberosRealm`** and **`KerberosKDC`**. Like other *tagent.ini* parameters, these values can be specified at a global (all) agent level and/or on a per agent basis. Unless both of these parameters are defined, the agent will not attempt Kerberos authentication even if the Hadoop Data Mover Job has checked the **Use Kerberos Authentication** check box.

MapR Configuration

When using MapR Hadoop on a 64-bit machine, add the following line to your *tagent.ini* file (assuming the MapR Client is installed in the default location):

jvmpara=-Djava.library.path=/opt/mapr/hadoop/hadoop-0.20.2/lib/native/Linux-amd64-64

When using MapR Hadoop on a 32-bit machine, add the following line to your *tagent.ini* file (assuming the MapR Client is installed in the default location):

jvmpara=-Djava.library.path=/opt/mapr/hadoop/hadoop-0.20.2/lib/native/Linux-i386-32

To use MapR Hadoop, you must also specify the location of the MapR Hadoop jar files. Use the *MapRClasspath* parameter to specify the full path to the required MapR Hadoop jar file directory.

Add the following line to your tagent.ini file (assuming the MapR Client is installed in the default location):

maprclasspath=/opt/mapr/hadoop/hadoop-0.20.2/lib/*

User Configuration File

With this release of the Agent, there is a new user configuration file, *TdlUser.cfg*, that specifies parameters for the runtime user associated with a job. It is located in the agent's root directory, for example, /opt/TIDAL/Agent/<name of agent>.

The user configuration file has the following layout:

parameter=value

parameter=value

[user-1]

parameter=value

parameter=value

.

.[user-2]

parameter=value

parameter=value

A parameter value is specified in a parameter/value line which has the form parameter=value. Default configuration parameters to be applied to all users are specified before the first user specific parameter values. This is referred to as the “default section”. To specify parameter values and/or to override a default parameter value for a particular user, add a section for that user. A user section starts with a "user section" line that contains the user name enclosed in brackets (“[", “]”) followed by a number of parameter/value lines. All parameter/value lines following a user section line up until the next user section line (or end of the file) are applied to that specific user. Parameter values specified in a user section override parameter values that are specified in the default section. Lines that start with the "#" character are ignored.

The new user configuration parameters are KerberosPrincipal and KeyTabFilePath. These parameters specify the Principal and KeyTab file for the Agent to use when performing Kerberos authentication.

Tidal Agent for z/OS

The Tidal z/OS agent component of the z/OS adapter provides the following services to a master:

- Submits JCL (JES2)
- Executes USS (OMVS) scripts and programs
- Executes system (console) commands
- Tracks current state and status of Scheduler submitted jobs
- Monitors file dependencies (HFS and exist/non-exist for datasets)
- Transfers job output to the master

This agent is implemented using Tidal Java agent technology and is stored along with configuration and logging files in the hierarchical file system (HFS) of USS. The z/OS agent uses IBM’s implementation of TCP/IP to communicate with the Scheduler master.

z/OS Agent Requirements

The following is a list of minimum hardware and software requirements for using the z/OS agent:

	Requirement
Hardware	S/390 or compatible architecture
	Approximately 4MB of available disk space. At least 40MB for production (logs, working files, etc.) is recommended.
	Network connectivity between the Scheduler agent and Scheduler master machines

	Requirement
Software	OS/390 V2R10 with JES2 and z/OS Unix system services
	Workload Manager must be running in **goal** mode to use the workload balancing and job control (stop and resume) features
	TCP/IP network protocol
	The Scheduler master system must be able to ping the Scheduler agent system, and the Scheduler agent system must be able to ping the Scheduler master system
	z/OS UNIX system services
	JVM 1.4.2+ (recommended) (To download the JVM file (PTF) with its instructions, visit IBM's website at: www.ibm.com/servers/eserver/zseries/software/java

Note The z/OS agent cannot work properly unless all software prerequisites are installed and configured properly.

Prerequisites for Installation

There will be two user IDs involved in installing and running the agent. The first user ID that is needed to install the agent must have the following capabilities:

- Utilize OMVS environment
- UID 0 authority
- APF authority (BPX.FILEATTR.* facility read access in RACF or equivalent)

The userid that is created or chosen to own and run the Agent must have the following capabilities:

- OMVS segment
- BPX.DAEMON facility read access (in RACF or equivalent)
- OPERCMDS authority (RACF or equivalent) at a minimum, requires:
  - Submit jobs
  - Display job status
  - Cancel jobs
  - Suspend jobs
  - Restart jobs
  - Monitor jobs

Note Both, the installer and the owner of the agent, need an assigned GID.
The user installing the agent requires the Superuser UID of 0.
The owner of the agent, however, should not have the UID of 0 (superuser) associated with it.
The user name associated with the agent owner's UID should not be more than six characters long.

The z/OS agent requires APF authorization to issue JES2 and MVS operator commands to control and monitor an MVS job's execution. These authorization rights for the agent must include:

- submitting jobs
- displaying job status
- canceling jobs
- suspending jobs
- restarting jobs that execute in a known address space
- monitoring jobs

Create a USS Directory

Before installing the z/OS agent on a z/OS system, you must create a directory in the USS HFS that conforms to the following:

- It is recommended that you use the directory **/TIDAL/Agent** when installing the agent. The agent installation will create multiple subdirectories under that directory.
- The volume dedicated to the z/OS agent should be at least 20 MB in size but may need to be larger depending on the number of jobs running and the volume of their output.
- The owner of the z/OS agent product files must have **READ** and **EXECUTE** access rights to the directory under which they were installed; otherwise, the installation will fail.

Note Both, the installer and the owner of the agent, need an assigned GID.
The user installing the agent requires the Superuser UID of 0.
The owner of the agent, however, should not have the UID of 0 (superuser) associated with it.
The user name associated with the agent owner's UID should not be more than six characters long.

Verify that Workload Manager is in Goal Mode (optional)

To verify that Workload Manager is in Goal mode:

Step 1 To display the current mode, enter the following from the system console:

```
D WLM,SYSTEMS
```

Step 2 If the agent system is not running in goal mode, you can modify the mode from the console by entering the following command:

```
F WLM,MODE=GOAL
```

Step 3 If you want your system to automatically run Workload Manager in goal mode, remove the **IPS=xx** parameter from the IEASYSxx member in PARMLIB.

During IPL, the absence of this parameter causes Workload Manager to run in goal mode.

Step 4 If Workload Manager on your system runs in compatibility mode and you do not want your system to run in goal mode, the workload balancing feature and the stop/resume job control feature are not available. If you want to use the agent workload balancing feature and the stop and resume job control feature, Workload Manager must be running in goal mode.

Installing the z/OS Agent

To install the z/OS agent, perform the following steps:

Step 1 From the **z/OS Agent** folder on the Scheduler DVD-ROM, copy or FTP (binary mode) the installation files, *install.sh* and *install.tar*, to the temp directory you created for the installation in the HFS.

Step 2 Change to the directory where you FTPed the installation files.

Step 3 Log on to TSO or ISPF.

When you log on, be sure to allocate at least two MB of memory (SIZE=2048000) for your session. This amount of memory is required during installation and is needed anytime the agent is started.

Step 4 Invoke the USS shell from TSO (do not use **rlogin**).

You must be a user with Superuser authority (UID=0) and change to the directory you created for the agent or the directory where the agent is already installed.

For example:

```
READY
OMVS
IBM
Licensed Material - Property of IBM
5647-A01 (C) Copyright IBM Corp. 1993, 2000
(C) Copyright Mortice Kern Systems, Inc., 1985, 1996.
(C) Copyright Software Development Group, University of
Waterloo, 1989.
All Rights Reserved.
U.S. Government users - RESTRICTED RIGHTS - Use,
Duplication, or Disclosure restricted by GSA-ADP schedule
contract with IBM Corp.
IBM is a registered trademark of the IBM Corp.
=> cd /opt/<temp directory>
```

Step 5 Change mode on *install.sh* so it can be executed.

```
chmod 755 install.*
```

Step 6 Run the installation script by entering:

```
./install.sh
```

After starting the installation script, you may have to wait a few moments. Do *not* press **ENTER**.

Step 7 You will see a banner and a message about making a current backup before installing new software. If you have not backed up your files before beginning the installation, quit the installation by typing **n** and back up your files. To proceed with the installation, type **y**.

Note Throughout this installation, default responses to prompts are shown in brackets.

Step 8 Enter the name of the user who will own the agent files (agent owner).

Step 9 Enter the directory location where the files should be installed. It is recommended that default location (**/TIDAL/Agent**) be used. Entering **y** will begin installing the agent files.

Information on the files being installed is displayed. Once the files are installed, the **Agent Configuration Menu** is displayed with options for adding, editing and deleting agent instances.

Note You must add at least one agent instance and configure it.

Step 10 After selecting the option to add an agent instance (1), you must enter a name for the agent, a port number and the directory path to the Java binaries directory.

Step 11 It is recommended to use the default port number, **5912**, if possible. If you have used the default locations when installing, you can just press the **ENTER** button.

Step 12 Once you confirm the selections, you are returned to the **Agent Configuration Menu**. Quit the **Agent Configuration Menu** by typing **Q** and pressing **ENTER**.

Non-Stop Kernel (NSK) Agent

The Non-Stop Kernel (NSK) system has two user environments, Guardian and Open System Services (OSS) that run on the base operating system called **NonStop**. The Tidal Agent for NSK uses Java Virtual Machine (JVM) and runs in the OSS user environment.

Like all Tidal agents, the following four services of the NSK agent are available to the master for scheduling processes and monitoring files.

- Jobs (OSS environment and Guardian environment using the **gtacl** command)
- File state monitoring
- FTP and SFTP Jobs
- File monitoring

Prerequisites for Installation

The following requirements must be met prior to installation and operation of the agent for NSK:

- NSK S-series or NSK Itanium machine
- Java Virtual Machine (JVM) 1.4.2_7+
- Agent machines require a minimum of:
  - 512 MB of RAM
  - 100 MB of disk space for the product and its log files
- A license file for the agent should be available to apply after installation.
- A *super.super* user alias to install the agent and another user alias to own and control the agent. This agent owner must have right to access the JVM.

Installing the NSK Agent

Before installing the Tidal Agent for NSK, backup your files and gather the following information:

- Name of the user alias who will own the agent
- Port number for the agent
- Directory path for the Java Virtual Machine (JVM)

To install the agent from the command line:

Step 1 If you have not already done so, backup your files before beginning the installation procedure.

Step 2 Insert the installation DVD-ROM into the machine you want to install the agent on.

Step 3 Login as *system.system* user alias.

Step 4 Copy the *install.com* and *install.tar* files from the directory on the DVD-ROM (`<DVD-ROM>\agent\NSK\command`) to your `Temp` directory.

Step 5 Change the permissions on the *install.sh* file in the directory to make the file executable.

```
chmod 755 install.sh install.tar
```

Step 6 To begin the installation, type the following and press ENTER to display the initial screen:

```
./install.sh
```

Step 7 To continue the installation, type `y` and press **ENTER**.

Note You can exit the installation program at any time by pressing `CTRL+C`.

Step 8 Type the user alias who will own the agent and press **ENTER**.

Step 9 Enter the user's password and press **ENTER**.

Note Do not unpack the *install.tar* file. This file will automatically unpack during the installation process.

A directory recommendation for the agent files displays.:

Type the name of the directory where you want to install the agent files and press **ENTER**.

It is recommended that you use the default directory path.

The default directory is displayed inside of brackets. If you wish to install into the default directory, press **ENTER** without typing anything.

Step 10 Type y and press **ENTER**.

Step 11 Review the information that you have entered.

If the information is correct, begin installing the agent files by typing `y` at the command prompt and pressing **ENTER**.

The `Agent Configuration` menu displays.

Step 12 Enter `1` to add an instance and press **ENTER**.

Step 13 Enter the name to call the agent and press **ENTER**.

Step 14 Enter the number of the port the agent will use and press **ENTER**.

Step 15 Enter the Java binaries (JVM) directory path and press **ENTER**.

To use the default directory path, do not type a directory path and press **ENTER**.

Step 16 Enter `y` to accept the selections.

If the information is not correct, type `n`. You are prompted again for the name, port number and directory path for the agent.

Tidal Agent for OVMS

Installation Prerequisites

The following requirements must be met prior to installation and operation of the agent for OVMS:

- OVMS Alpha 7.2.2 with JVM 1.4.1OVMS Alpha 7.3.2 with JVM 1.4.2(Be sure the user has the rights to access the JVM.)
- Agent machines for the OVMS agent require a minimum of:
  - 1 Gig of RAM on the agent machine dedicated to the OVMS agent
  - 100 MB of disk space dedicated to the OVMS agent and its log files
- A user needs the following privileges to run jobs on the OVMS agent:
  - NETMBX
  - TMPMBX
- A user needs the following additional privileges to manage the agent:
  - CMKRNL
  - GRPPRV
  - IMPERSONATE NETMBX
  - SYSPRV
  - TMPMBX
- A license file for the agent should be available to apply after installation.
- A root user account to install the agent with an OVMS user account to own and control the agent. (Be sure the user has the rights to access the JVM.)

Installing the Agent

Before installing the Tidal Agent for OVMS, backup your files and gather the following information:

- Name of the user who will own the agent
- Port number for the agent
- Directory path for the Java Virtual Machine (JVM)

To install the agent from the command line:

Step 1 If you have not already done so, backup your files before beginning the installation procedure.

Step 2 Login as system or the account that the account will run as.

Step 3 Copy the *install.com* and *pduct.bck* files to your system. The two files require different formats when they are FTPed.

- Send the *install.com* file in ASCII format
- Send the *pduct.bck* file in binary format.

Step 4 After downloading the *pduct.bck* file at the OVMS machine, set the Logical Record Length by applying the following command:

```
set file/attrib=(lrl:32256) pduct.bck
```

Step 5 To begin the installation, type the following and press ENTER to display the initial screen:

```
$ @install
```

Step 6 To begin the installation process, type **2** and press **Enter**.

Note You can exit the installation program at any time by pressing CTRL + c

If the installation program cannot find the Java Runtime Engine (JRE), the installation will not proceed and the following message is displayed:

```
"Java Run Time not found. Please install Java Run Time first."
```

Step 7 Type the name of the disk of your system where you want to install the agent files and press **Enter**. The default disk is displayed inside of brackets. If you wish to install into the default disk, press **Enter** without typing anything; however, if your system does not have a disk with this name than the installation process will stop.

Step 8 Type the name of the directory where you want to install the agent files and press **Enter**. The default directory is displayed inside of brackets. If you wish to install into the default directory, press **Enter** without typing anything.

The installation procedure will create the OVMS agent files in the designated location.

Step 9 Type the name of the user who will own the agent and press **Enter**.

Step 10 The installation program will prompt for the version of Java being used. If your system is using OVMS alpha version 7.2.2 you need to use JVM 1.4.1. If your system uses OVMS alpha version 7.3, you need to use JVM 1.4.2. Type the JVM version you are using and press **Enter**.

Once the JVM is determined, the installation program starts creating the agent files.

Step 11 Type a name for the agent.

Step 12 Type the number of the port that the OVMS agent should use and press **Enter**. The default port number is **5912**.

The installation of the OVMS files is complete.

Step 13 Run the following command in the directory where the agent was installed:

```
$ @AGENT_SYM.COM
```

Step 14 Verify that the OVMS agent is correctly installed by running the agent in debug mode.

Note The agent can only be started and stopped from its *.bin* directory. Be sure that you are in the *.bin* directory when starting and stopping the agent.

Step 15 Type the following, replacing the brackets and the text between them with the name of the agent, and press ENTER.

```
$ tagent <name of OVMS agent> debug
```

Installing Adapters

This chapter describes prerequisites and installation information for the TES adapters that require manual setup.

Informatica Adapter

The TES Adapter for Informatica integrates with PowerCenter using Informatica's Load Manager SDK (a set of application programming interfaces/APIs that allows interaction with the PowerCenter Server for workflow management). Via this programming interface, the Informatica Adapter communicates with the Load Manager component of the PowerCenter to run and monitor workflows. To provide for user access to Repository data such as Folder, Workflow and Workflow Task definitions, the Informatica Adapter also requires a database connection to the PowerCenter Repository Database. Database connectivity is provided via Java Database Connectivity (JDBC) programming interface.

Installing the Informatica Adapter

To install the Informatica adapter:

Step 1 Stop the master.

For Windows:

a. Click the **Start** button and then select **Programs>TIDAL Software>Scheduler>Master>Service Control Manager**.

b. In the Service list, verify that the master is displayed and click **Stop** to stop the master.

For Unix:

a. Stop the master by entering **tesm stop**.

b. Verify the master is stopped by entering **tesm status**.

Step 2 Copy the .pkg file into the config folder located in the master installation directory (there should already be a master.props file there).

Step 3 Restart the master:

a. a For Windows, click Start in the Service Control Manager.

b. b For Unix, restart the master by entering tesm start.

The Master will deploy the .pkg file and will move it from the config folder to the Services folder. An Adapter GUID directory is also created under the Services folder.

For example:

For Windows: **C:\Program Files\TIDAL\Scheduler\master\services\{7640B420-5530-11DE-8812-7B8656D89593}**

For Unix: **/opt/TIDAL/Scheduler/master/services/ {7640B420-5530-11DE-8812-7B8656D89593}**

Step 4 Restart the Enterprise Scheduler Client by clicking the Windows Start button and selecting Programs>TIDAL Software>Client>Client. When the Client connects, it will download the new package.

The next several steps involve configuring the system for use with the Informatica Adapter. Once the .pkg has been deployed you must stop the Master service and restart it after completing the following steps.

Configuring the Informatica Adapter

To Install and configure the Informatica Libraries:

Note For Unix, add the following entries in user's profile located in the user's home directory. For example: .profile or .bash_profile (Linux).
You will need to source the profile after applying all profile updates. For example, .~/.profile. Once the following steps are performed, this will require a restart of the master for the configurations to take affect.

Step 1 Extract the library from the **infalib** archive to the master machine

a. Create a directory under the master services directory called **infa**.

b. Windows Example: **C:\Program Files\TIDAL\master\services\infa**

c. Unix Example: /opt/tidal/master/services/infa

d. Extract the archive to this location. The archive distribution contains directories: lib and locale. The system will be configured to refer to these locations in the next steps.

Step 2 Configure the System Path to include the Informatica Library Path (i.e. **lib** directory.)

Windows Example: **C:\Program Files\TIDAL\master\services\infa\lib**

For Windows, include the library path in the "Path" Environment Variable.

Unix Example: **/opt/master/services/infa/lib or master/services/infa/lib**

For Solaris/Linux, include the library path in **LD_LIBRARY_PATH**.

For AIX, include the path in **LIBPATH**. For 64-bit also include **LD_LIBRARY_PATH**.

For HPUX, include the path for **SHLIB_PATH**.

Step 3 Create or update the **INFA_DOMAINS_FILE** Environment Variable to the location of the Informatica *domains.infa* file for the PowerCenter configuration.

This requires that the *domains.infa* file be local to the Master machine; copy it from your PowerCenter installation as needed. Put this file in the infa directory created in step 1a).

Note To configure connections to multiple PowerCenter servers, modify the local domains.infa file that was copied to the Master machine. Add values for the vector xml tag corresponding to each Server that will be configured as an Informatica Adapter.

The following example includes server information to two PowerCenter servers, one to Dev and another for Prod. These are referred to as **dev-infa** and **prod-infa**, respectively in the sample *domains.infa* file.

```
<Portals xmlns:common="http://www.informatica.com/pcsf/common"
xmlns:usermanagement="http://www.informatica.com/pcsf/usermanagement"
xmlns:domainservice="http://www.informatica.com/pcsf/domainservice"
xmlns:logservice="http://www.informatica.com/pcsf/logservice"
xmlns:domainbackup="http://www.informatica.com/pcsf/domainbackup"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:metadata="http://www.informatica.com/pcsf/metadata"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:domainconfigservice="http://www.informatica.com/pcsf/domainconfigservice"
xmlns:alertservice="http://www.informatica.com/pcsf/alertservice"
xmlns:licenseusage="http://www.informatica.com/pcsf/licenseusage"
xmlns:webserviceshub="http://www.informatica.com/pcsf/webserviceshub"
xsi:type="common:PCSFVector"  objVersion="1.1.19">
<vector xsi:type="domainservice:Portals"  objVersion="1.1.19">
<domainName>Domain_dev-infa</domainName>
<address xsi:type="metadata:NodeRef"  objVersion="1.1.19">
<host>dev-infa</host>
<port>6001</port>
</address>
</vector>
<vector xsi:type="domainservice:Portals"  objVersion="1.1.19">
<domainName>Domain_prod-infa</domainName>
<address xsi:type="metadata:NodeRef"  objVersion="1.1.19">
<host>prod-infa</host>
<port>6001</port>
</address>
</vector>
</Portals>
Example on Windows:
INFA_DOMAINS_FILE=C:\ Program Files\ TIDAL\master\services\infa\domains.infa
Example on Unix:
Export INFA_DOMAINS_FILE=/opt/TIDAL/master/services/infa/domains.infa
```

Step 4 Configure the Locale Path for the Informatica Library by setting the `TDLINFA_LOCALE` `service.props` value of the Informatica Adapter. In the `config` directory located under the Adapter's GUID directory, create or update the *service.props* file, create both the directory and file if it does not yet exist. Include an entry for `TDLINFA_LOCALE` that points to the `Load Manager Library` locale directory.

Windows Example:

```
C:\Program
Files\TIDAL\Scheduler\master\services\{7640B420-5530-11DE-8812-7B8656D89593}\config\ser
vice.props
```

Unix Example:

```
/opt/tidal/master/services/{7640B420-5530-11DE-8812-7B8656D89593}/config/service.props
```

Service.props entry example:

For Windows:

```
TDLINFA_LOCALE=C:\\Program Files\\TIDAL\\Scheduler\\master\\services\\infalib\\locale
```

For Unix:

```
TDLINFA_LOCALE=/opt/tidal/master/services/infa/locale
```

Step 5 You will need access to the Database JDBC Drivers for connectivity to the PowerCenter Repository database. Obtain the JDBC jar files from the vendor as needed and copy the corresponding *.jar* files to the services **lib** directory.

Windows Example:

```
C:\Program
Files\TIDAL\Scheduler\master\services\{7640B420-5530-11DE-8812-7B8656D89593}\lib
```

Unix Example:

```
/opt/tidal/master/services/{7640B420-5530-11DE-8812-7B8656D89593}/lib
```

Step 6 Reboot the Master machine on Windows as needed. Source the profile file as needed on Unix.

Step 7 Restart the master.

SAP Adapter

While the SAP adapter software is already installed as part of a normal installation of TES, you must download and install the Java connector software provided by SAP, called the JCO 3.0 component. SAP JCO 3.0 is necessary for a Java application (like the Enterprise Scheduler) to work with SAP.

Installing SAP JCO

The master requires Java connector (JCO) software from SAP. SAP's JCO middleware allows a Java application to communicate with an SAP system. Each operating system requires its own version of the JCO that can be downloaded from SAP.

To download SAP JCO:

Step 1 In your web browser, go to the following URL: *http://service.sap.com/patches*.

A Client Authentication dialog displays to request an authentication certificate.

a. If you have such a certificate, select it and click **OK**.

b. If you do not have a certificate, click **OK** to display the **Enter Network Password** dialog.

Step 2 Enter the user name and password supplied by SAP into the respective text fields and click **OK**.

The SAP Support Packages and Patches Web page displays.

Step 3 Navigate to 3.x SAP Java Connector Download Page.

Step 4 Various operating systems are listed. Click on the appropriate operating system to access its archive file for downloading. Follow the instructions for installing the JCO that are included in the archive file.

Step 5 In the initial setup of SAP JCO 3.0, two files from the *SAP JCO.zip* file are necessary:

- *sapjco3.jar* (Windows and Linux)
- *sapjco3.dll* (Linux: *libsapjco3.so*)

After installing the JCO, add the *{sapjco-install-path}/sapjco3.jar}* to your CLASSPATH environment variable, and then specify the path to the location when you have
JCO 3.x libraries installed. You may need to reboot your system.

OS400 Adapter

To operate properly, the OS/400 adapter from Enterprise Scheduler has the following prerequisites.

Minimum Software Requirements

The minimum software releases for the Scheduler OS/400 adapter implementation is OS/400 version v5R2M0.

See your Tidal Enterprise Scheduler Reference Guide for a full list of requirements.

There are different authorities required depending on whether the user is submitting the job or having the job submitted for them.

The following services must be running on the OS/400 machine:

- Command
- File
- Print
- Dataqueue

A user defined on the OS/400 manages the connection to the OS/400 and submits jobs to run under different users. This user is strongly recommended to have QSECOFR authorities and be able to issue the **SBMJOB** command. This user must have:

- *USE authority to the other user's profile
- *USE authority to the command specified in the Command parameter and *EXECUTE authority to the library containing that command
- *READ authority to the job description (JOBD) and *EXECUTE authority to the library containing that job description
- *USE authority to the job queue (JOBQ) and *EXECUTE authority to the library containing that job queue
- *USE and *ADD authority to the message queue (MSGQ) and *EXECUTE authority to the library containing that message queue
- *USE authority to the sort sequence table (SRTSEQ) and *EXECUTE authority to the library containing that sort sequence table
- *EXECUTE authority to all auxiliary storage pool (ASP) device descriptions in the initial ASP group (INLASPGRP)

The user that the job is being submitted for (as specified in the User text box on the Page 4 tab) must have the following authorities:

- *USE authority to the job description (JOBD)
- *READ authority to the output queue (OUTQ) and *EXECUTE authority to the library containing that output queue
- *USE authority to all auxiliary storage pool (ASP) device descriptions in the initial ASP group (INLASPGRP)
- *USE authority to the library specified for the current library (CURLIB) parameter
- *USE authority to all the libraries specified for the initial library list (INLLIBL) parameter

OS/400 Configuration

While the OS/400 adapter software is already installed as part of a normal installation of Scheduler, you must perform the following steps to license and configure the adapter before you can run OS/400 jobs:

- License the connection(s) to the AS/400 machine. You cannot define an OS/400 connection until you have applied the OS/400 license from TIDAL Software. For details, refer to the *Cisco Tidal Enterprise Scheduler 6.2 Online Help*.
- Define an OS/400 connection so the master can communicate with a AS/400 machine. For details, refer to the *Cisco Tidal Enterprise Scheduler 6.2 Online Help*.
- Define an OS/400 user as a runtime user in TES and add this user to other users' runtime users list.

zOS Adapter

The Gateway component of the z/OS adapter provides the following features:

- Installs without an IPL
- Full sysplex support
- Monitors SMF records
- Modification of parameters and processes without restarting
- SMF processing is independent of other concurrent SMF processes and prior to any process that may alter SMF data
- Fault tolerance
- Supports OS/390 and z/OS

The Gateway uses three Started Tasks:

- **`TSISPACE`**
- **`TSIRECRD`**
- **`TSESCHED`**

Installing the zOS Gateway

The Gateway sits between the Scheduler master and the Systems Management Facilities (SMF) component on z/OS. The Gateway component tracks job dependencies on batch jobs that execute on z/OS. These job dependencies can be tracked not only by job but by individual job steps that comprise a job. The Gateway can run without the SDSF component of z/OS. If the network connection between Scheduler and the Gateway is broken, the Gateway continues to process the SMF job data and archive all job information so that it can be relayed to the master whenever the connection is restored.

To install the Gateway

Step 1 Insert the installation DVD into the DVD-ROM drive of a Client Manager machine.

Step 2 On the installation DVD, locate in the **zOS Agent\zOS Gateway** directory the following three files:

- *unlcntl.bin* (JCL library)
- *unload.bin* (authorized load)
- *unlparm.bin* (parameter control)

This will look like the following screen:

```
Directory of <DVD-ROM>:\zOSAgent\zos Gateway

05/09/2002  07:39p          5,553,600 unload.bin
04/01/2002  11:15a 5,600 unlcntl.bin
04/01/2002  11:15a 4,320 unlparm.bin

3 File(s)      5,563,520 bytes
0 Dir(s)     396,230,656 bytes free
```

Preallocate the size of these three data sets or ensure your site's defaults are large enough that you do not receive a B37 abend when FTPing the files. (All three data sets are FB-80-3120.)

For example:

```
hlq.UNLOAD.BIN   120 tracks
hlq.UNLCNTL.BIN 1 track
hlq.UNLPARM.BIN 1 track
```

Step 3 Select the three files and FTP them to the z/OS server and desired HLQ directory, using the binary transfer mode. (By default, this directory is usually the same as the user name you connect with.)

The following is an example of FTPing the files:

```
ftp <host name>
Connected to <host name>.
220-FTPD1 IBM FTP CS V2R10 at STRONG.COM, 17:41:44 on 2002-05-10.
220 Connection will close if idle for more than 5 minutes.
User <host name>: <user name>
331 Send password please.
Password:
230 <user name> is logged on.  Working directory is <"directory">.
ftp> bin
200 Representation type is Image
ftp> put unload.bin
200 Port request OK.
125 Storing data set IBMUSER.UNLOAD.BIN
250 Transfer completed successfully.
ftp: 1599840 bytes sent in 2.26Seconds 706.96Kbytes/sec.
```

```
ftp> put unlcntl.bin
200 Port request OK.
125 Storing data set IBMUSER.UNLCNTL.BIN
250 Transfer completed successfully.
ftp: 473200 bytes sent in 0.45Seconds 1049.22Kbytes/sec.
ftp> put unlparm.bin
200 Port request OK.
125 Storing data set IBMUSER.UNLPARM.BIN
250 Transfer completed successfully.
ftp: 27200 bytes sent in 0.00Seconds 27200000.00Kbytes/sec.
ftp> quit
221 Quit command received. Goodbye.

D:\TIDAL>d:
```

Step 4 Once the files have been FTPed to data sets, you must unload and create the library files. Use the **TSO RECEIVE** command on each data set to create partitioned data sets (PDS). These three files will create the following libraries:

- **hlq.LOADLIB**
- **hlq.CNTL**
- **hlq.PARMLIB**

Start with the *UNLCNTL* file first because it contains the JCL, Started Tasks, PROCS and miscellaneous CLISTS needed to create the other hlq.JOBDATA VSAM data set and sample JOBS.

This step might look like the following example:

```
tso receive indsn('hlq.unload.bin')

INMR901I Dataset hlq.LOADLIB from TIDAL on PLUTO,
INMR906A Enter restore parameters or 'DELETE' or 'END' +,

response by pressing enter or use the dsn('dataset.net')
```

If you get the following message respond with an **R** to overwrite the members.

```
, IEBCOPY MESSAGES AND CONTROL STATEMENS
PAGE     1,
,IEB1135I IEBCOPY  FMID HDZ11F0  SERVICE LEVEL NONE     DATED
20000815 DFSMS 02
10.00 OS/390  02.10.00 HBB7703  CPU 1247,
,IEB1035I IBMUSER  ISPFPROC DBSPROC  13:26:13 FRI 10 MAY 2002
PARM='',
, COPY INDD=((SYS00018,R)),OUTDD=SYS00016,
,IEB1013I COPYING FROM PDSU  INDD=SYS00018 VOL=OS39M1
DSN=SYS02130.T132612.RA00
.IBMUSER.R0100505,
,IEB1014I           TO PDS  OUTDD=SYS00016 VOL=OS39M1 DSN=IBMUSER
LOADLIB
,IEB167I FOLLOWING MEMBER(S) LOADED FROM INPUT DATA SET REFERENCED BY
SYS00018,
,IEB154I DEINIT   HAS BEEN SUCCESSFULLY LOADED,
...
IEB154I TVAVTOC1 HAS BEEN SUCCESSFULLY LOADED,
IEB1098I 156 OF 156 MEMBERS LOADED FROM INPUT DATA SET REFERENCED BY
SYS00018,
IEB144I THERE ARE 45 UNUSED TRACKS IN OUTPUT DATA SET REFERENCED BY
SYS00016,
```

```
IEB149I THERE ARE 5 UNUSED DIRECTORY BLOCKS IN OUTPUT DIRECTORY,
IEB147I END OF JOB - 0 WAS HIGHEST SEVERITY CODE,
INMR001I Restore successful to dataset '<User>.LOADLIB',
***,R
```

Oracle Applications Adapter

The TES adapter for Oracle Applications integrates Oracle Applications into TES using a concurrent manager bridge.

The Oracle Applications Adapter from TES uses Net*8 (SQL*NET) to connect directly to Oracle databases when accessing Oracle Applications.

Oracle databases compile and store procedures and functions in units called packages. The Oracle Applications Adapter uses Oracle's packages and other packages customized by TES in combination with SQL statements to integrate the TES job scheduler with the Concurrent Manager process that monitors and controls the Oracle Applications job. The Concurrent Manager monitors and responds to the data stored within the Oracle database using the packages available to it.

The customized packages supplied by TES must be compiled in Oracle Applications before a connection between TES and Oracle Applications can be established. An error occurs in TES if you try to establish a connection to an Oracle Applications instance before the proper customized packages are installed on the designated Oracle Applications instance.

Any inserting and updating to the standard tables of Oracle Applications is done using standard APIs present in the Oracle Applications database. Nothing is deleted from the standard Oracle Applications database just as no database schema objects are modified.

Minimum Software Requirements

The minimum software requirements for the Oracle Applications Adapter for TES are:

- Oracle Applications software 11.5.8, 11.5.9, 11.5.10, 12 - 12.04
- Oracle database 9.2, 10g 11g
- MKS Toolkit 7.1 or higher installed on all of the Forms Servers
- TES version 6.0 or later

Installing and Configuring the Adapter

There are two components to the Oracle Applications adapter. One component is the Oracle Applications adapter itself while the other part is a bridge component that provides a link between the adapter and the Oracle Applications program. The Oracle Applications adapter is part of the normal TES installation and does not require a separate installation. However, the Bridge component does require installation and the procedure to install it is described in the following section.

Completing the Bridge Prerequisites

The Oracle Applications Bridge is comprised of various PL/SQL stored procedures and forms used to pass job parameters to the Oracle database. The Bridge component of the Oracle Applications adapter is not part of the regular TES installation and requires a separate installation procedure.

The following prerequisites must be completed before installing the Oracle Applications Bridge:

- The user must be logged on to Windows/Unix as the application owner (usually **applmgr**).
- Run the application environment file (usually *Appsora.env* under **$APPL_TOP**) in the current shell.
- Grant the execute privilege on *sys.dbms_obfuscation_toolkit* file to the **APPLSYSPUB** user. This package is used by the Bridge to encrypt and decrypt the data. To grant this privilege, connect to the database as system (or **SYSDBA**) and from the SQL prompt, enter:

  ```
  SQL>grant execute on sys.dbms_obfuscation_toolkit to applsyspub;
  SQL>commit;
  ```

- Create tablespace for the Table and Index spaces before starting installation. To configure the tablespaces to autoextend:

  ```
  SQL>CREATE TABLESPACE sabdg_data DATAFILE '/do1/oracle/testdata/sabdg_data.dbf' SIZE
  100M AUTOEXTEND ON NEXT 20M MAXSIZE UNLIMITED;
  SQL>CREATE TABLESPACE sabdg_index DATAFILE '/do1/oracle/testdata/sabdg_idx.dbf' SIZE
  50M AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED;
  SQL>commit;
  ```

- While no existing **$APPL_TOP** objects/files are modified when installing the Bridge, three new objects/files that start with **SABDG** are created.

Note The database schema names used above are only examples. You can use your own names for the database schemas.

Installing the Bridge for 11i or R12

The batch file that installs the Bridge requires the following parameters:

- **APPS user** (or equivalent) – The equivalent Apps user in the Oracle Applications program.
- **APPS password** – The password of the Apps user used to access Oracle Applications.
- **Data tablespace** – The name of the data tablespace (sabdg_data).
- **Index tablespace** – The name of the index tablespace (sabdg_index).
- **TNS name** – The TNS string to connect to the database (Windows only)
- **Temp tablespace** – The temporary tablespace for the user **SABDG**.
- **System password** – The database user system password. This is required for when the installation process creates the **SABDG** user in the database to own tables, sequences and indexes.

Use these parameters when running the batch file to install the Bridge. The installation and upgrade procedures for both Windows and Unix forms servers are described next.

Initial Installation–Windows Forms Server

Copy the 11i or R12 Bridge files from the **\OraAppsBridge\Windows** directory in the installation DVD-ROM to a temporary directory on the forms server. The temporary directory must be on the same drive as the **APPL_TOP**.

Step 1 On the command line, using the listed parameters, enter:

```
install_11i <APPS User> <APPS Password> <Data Tablespace> <Index Tablespace> <TNS Alias
Name> <Temp Tablespace> <System Password>
```

-or-

```
install_R12 <APPS User> <APPS Password> <Data Tablespace> <Index Tablespace> <TNS Alias
Name> <Temp Tablespace> <System Password>
```

Bridge Upgrade Procedure

Step 1 On the command line, using the listed parameters, enter:

```
upgrade_11i <APPS User> <APPS Password> <Data Tablespace> <Index Tablespace> <TNS Alias
Name> <Temp Tablespace> <System Password>
```

-or-

```
upgrade_R12i <APPS User> <APPS Password> <Data Tablespace> <Index Tablespace> <TNS Alias
Name> <Temp Tablespace> <System Password>
```

Initial Installation–Unix Forms Server

Copy the 11i or R12 Bridge *TdlOraAppsBdg.tar* file from the **/OraAppsBridge/Unix** directory in the installation DVD-ROM to a temporary directory on the forms server.

To install:

Step 1 Extract files from *TdlOraAppsBdg.tar* file:

```
tar xvf TdlOraAppsBdg.tar
```

Step 2 From the temporary directory where you copied the Bridge files, at the cursor, enter:

```
chmod 755*
```

Step 3 At the cursor, using the listed parameters, enter:

```
sh ./install_11i.sh <APPS User> <APPS Password> <Data Tablespace> <Index Tablespace>
<Temp Tablespace> <System Password>
```

-or-

```
sh ./install_R12.sh <APPS User> <APPS Password> <Data Tablespace> <Index Tablespace>
<Temp Tablespace> <System Password>
```

Upgrading the 11i or R12 Bridge–Unix

To upgrade:

Step 1 Extract files from *TdlOraAppsBdg.tar* file

```
tar xvf TdlOraAppsBdg.tar
```

Step 2 From the temporary directory where you copied the Bridge files, at the cursor, enter:

```
chmod 755*
```

Step 3 At the cursor, using the listed parameters, enter:

```
sh ./upgrade_11i.sh <APPS User> <APPS Password> <Data Tablespace> <Index Tablespace>
<Temp Tablespace> <System Password>
```

-or-

```
sh ./upgrade_R12.sh <APPS User> <APPS Password> <Data Tablespace> <Index Tablespace>
<Temp Tablespace> <System Password>
```

Note If you have a multi-tier architecture off Oracle Apps containing multiple form servers, then the Bridge for Oracle Apps must be installed on only one of the forms server and upgraded on the rest of the form servers to ensure distribution of the Bridge forms.

Verifying Successful Installation/Upgrade

Installation and upgrade procedures can be verified by checking a log file that is created when the Bridge is installed. This log file, called *Verify_post.log*, is created in the same directory where the Bridge was installed.

Open the *Verify_post.log* file.

There are three values displayed in the log file:

- TOT(Total Objects)
- VAL(Valid Objects)
- INV(Invalid Objects)

The TOT and VAL values should read 36.

The INV value should read 0.

If the values displayed in the log file are the proper values, then installation/upgrade was successful. Any deviation from these values indicates that the installation/upgrade was unsuccessful.

Uninstalling the Bridge

To uninstall the Bridge component of the Oracle Applications adapter, you must delete all of the Bridge objects, the Bridge owner and all of the forms on the forms server. The procedures to delete the Bridge owner and its objects are the same for both the Windows and Unix platforms but the procedures for deleting forms from the forms server differ for each platform.

To delete the Bridge objects (Windows and Unix):

Step 1 Login as **Apps** to the apps database.

Step 2 Run the *sabdg_drobj.sql* script that is found in the **\OraAppsBridge\Windows\sabdg_obj.sql** file in the Windows directory on the installation DVD-ROM.

To delete the Bridge owner (Windows and Unix):

Step 1 Login as **system** to the apps database.

Step 2 Drop user sabdg cascade.

To delete all forms on the forms server:

- For Windows:

```
rm %AU_TOP%\forms\US\SABDG\*.fmb
rm -r %FND_TOP%\forms\US\sabdg
rm -r %APPL_TOP%\sabdg
```

- For Unix:

```
rm $AU_TOP/forms/US/SABDG/*.fmb
rm -r $FND_TOP/forms/US/sabdg
 rm -r $APPL_TOP/sabdg
```

MapReduce Adapter

Hadoop MapReduce is a software framework for writing applications that process large amounts of data (multi-terabyte data-sets) in-parallel on large clusters (up to thousands of nodes) of commodity hardware in a reliable, fault-tolerant manner.

A Cisco Tidal MapReduce Adapter job divides the input data-set into independent chunks that are processed by the map tasks in parallel. The framework sorts the map's outputs, which are then input to the reduce tasks. Typically, both the input and output of the job are stored in a file-system. The framework schedules tasks, monitors them, and re-executes failed tasks.

Minimally, applications specify the input/output locations and supply map and reduce functions via implementations of appropriate interfaces and/or abstract-classes. These, and other job parameters, comprise the job configuration. The Hadoop job client then submits the job (jar/executable) and configuration to the JobTracker.

The client then assumes the following responsibilities:

- Distributes the software/configuration to the slaves
- Schedules and monitors tasks
- Provides status and diagnostic information to the job -client

The MapReduce Adapter serves as the job client to automate the execution of MapReduce jobs as part of a Tidal Enterprise Scheduler (TES) managed process. The Adapter uses the Apache Hadoop API to submit and monitor MapReduce jobs with full scheduling capabilities and parameter support. Alternatively, the Adapter may be configured to connect to a Cloudera Hadoop or MapR distribution. As a platform independent solution, the Adapter can run on any platform where the TES master runs.

Installing the MapReduce Adapter

The MapReduce Adapter software is not installed as part of a standard installation of TES, and you must install, and configure the adapter before you can schedule and run MapReduce jobs.

To install and configure the MapReduce adapter:

Step 1 Stop the master.

Step 2 Delete the directory {D9AC03 D5-41ED-4B1E-8A45-B2EC8BDE3EA0} and Mapreduceservice.pkg under the directory /TIDAL/Scheduler/Master/services.

Step 3 Place the new *mapreduceservice.pkg* file at /TIDAL/Scheduler/Master/config.

Step 4 Start the Master.

The /TIDAL/Scheduler/Master/services/{D9AC03D5-41ED-4B1E-8A45-B2EC8BDE3EA0} directory is created.

Step 5 In the {D9AC03D5-41ED-4B1E-8A45-B2EC8BDE3EA0} directory, create a subdirectory named *Config*.

Step 6 Create the *service.props* file in the Config directory.

Step 7 (For Apache 1.1.2 distribution only) Add the following lines in the service.props file:

```
jarlib=apache1.1.2
CLASSPATH=C:\\Program
Files\\TIDAL\\Scheduler\\Master\\services\\{D9AC03D5-41ED-4B1E-8A45-B2EC8BDE3EA0}\\lib\
\*;${CLASSPATH}
```

Step 8 (For Cloudera 3 distribution only) Add the following line in the *service.props* file:

```
jarlib=cloudera
```

Step 9 (For Cloudera 4 distribution only) Add the following lines in service.props file:

```
jarlib=cdh4
CLASSPATH=C:\\Program
Files\\TIDAL\\Scheduler\\Master\\services\\{D9AC03D5-41ED-4B1E-8A45-B2EC8BDE3EA0}\\lib\
\*;${CLASSPATH}
```

Step 10 (For MapR Distribution only) Install MapR client in the TES master machine, and add the following lines in the *service.props* file

```
jarlib=mapr
JVMARGS=-Djava.library.path=C:\\opt\\mapr\\hadoop\\hadoop-0.20.2\\lib\\native\\Windows_
7-amd64-64
CLASSPATH=C:\\opt\\mapr\\hadoop\\hadoop-0.20.2\\lib\\*;${CLASSPATH}
```

Step 11 Restart the Master.

Hive Adapter

The Cisco Tidal Enterprise Scheduler Hive Adapter provides the automation of HiveQL commands as part of the cross-platform process organization between Tidal Enterprise Scheduler (TES) and the TES Hadoop Cluster.

The Hive Adapter allows you to access and manage data stored in the Hadoop Distributed File System (HDFS™) using Hive's query language, HiveQL. HiveQL syntax is similar to SQL standard syntax.

The Have Adapter, in conjunction with TES, can be used to define, launch, control, and monitor HiveQL commands submitted to Hive via JDBC on a scheduled basis. The Adapter integrates seamlessly in an enterprise scheduling environment.

The Hive adapter includes the following features:

- Connection management to monitor system status with a live connection to the Hive Server via JDBC
- Hive job and event management includes the following:
  - Scheduling and monitoring of HiveQL commands from a centralized work console with Enterprise Scheduler
  - Dynamic runtime overrides for parameters and values passed to the HiveQL command
  - Output-formatting options to control the results, including table, XML, and CSV

- Defined dependencies and events with Enterprise Scheduler for scheduling control
- Runtime MapReduce parameters overrides if the HiveQL command results in a MapReduce job.

Installing the Hive Adapter

The Hive adapter software is not installed as part of a standard installation of TES, and you must install, and configure the adapter before you can schedule and run Hive jobs.

To install and configure the Hive adapter:

Step 1 Stop the master.

Step 2 Delete the {207463B0-179B-41A7-AD82-725A0497BF42} directory and *hiveservice.pkg* in the /TIDAL/Scheduler/Master/services directory.

Step 3 Place the new *hiveservice.pkg* file at TIDAL/Scheduler/Master/config.

Step 4 Start the master.

The /TIDAL/Scheduler/Master/services/{207463B0-179B-41A7-AD82-725A0497BF42} directory is created.

Step 5 In the {207463B0-179B-41A7-AD82-725A0497BF42} directory, create a Config subdirectory.

Step 6 Create the service.props file in the Config directory.

Step 7 In the service.props file, add the jarlib properties as follows:

a. For Apache 1.1.2, add: `jarlib=apache1.1.2`

b. For cloudera 4, add: `jarlib=cdh4`

c. For MapR add: `jarlib=apache1.1.2`

Step 8 Restart the master.

Sqoop Adapter

The Cisco Tidal Enterprise Scheduler (TES) Sqoop Adapter provides easy import and export of data from structured data stores such as relational databases and enterprise data warehouses. Sqoop is a tool designed to transfer data between Hadoop and relational databases. You can use Sqoop to import data from a relational database management system (RDBMS) into the Hadoop Distributed File System (HDFS), transform the data in Hadoop MapReduce, and then export the data back into an RDBMS. Sqoop adapter allows users to automate the tasks carried out by Sqoop.

The import is performed in two steps as depicted in figure below. In the first Step Sqoop introspects the database to gather the necessary metadata for the data being imported. The second step is a map-only Hadoop job that Sqoop submits to the cluster. It is this job that does the actual data transfer using the metadata captured in the previous step.

Installing the Sqoop Adapter

The Sqoop adapter software is not installed as part of a standard installation of TES, and you must install, and configure the adapter before you can schedule and run Sqoop jobs.

To install and configure the Sqoop adapter:

Step 1 Stop the master.

Step 2 Delete the {722A6A78-7C2C-4D8B-AA07-B0D9CED6C55A} directory and the *sqoopservice.pkg* file in the /TIDAL/Scheduler/Master/services directory.

Step 3 Place the new *sqoopservice.pkg* file at /TIDAL/Scheduler/Master/config.

Step 4 Start the Master.

The /TIDAL/Scheduler/Master/services/{722A6A78-7C2C-4D8B-AA07-B0D9CED6C55A} directory is created.

Step 5 In the {722A6A78-7C2C-4D8B-AA07-B0D9CED6C55A} directory, create a Config subdirectory.

Step 6 Create the *service.props* file in the Config directory.

Step 7 (For Apache 1.1.2 distribution only) Add the following lines in the service.props file:

```
jarlib=apache1.1.2
CLASSPATH=C:\\Program
Files\\TIDAL\\Scheduler\\Master\\services\\{722A6A78-7C2C-4D8B-AA07-B0D9CED6C55A}\\lib\
\*;${CLASSPATH}
```

Step 8 (For Cloudera 3 distribution only) Add the following line in the service.props file:

```
jarlib=cloudera
```

Step 9 (For Cloudera 4 distribution only) Add the following lines in the service.props file:

```
jarlib=cdh4
CLASSPATH=C:\\Program
Files\\TIDAL\\Scheduler\\Master\\services\\{722A6A78-7C2C-4D8B-AA07-B0D9CED6C55A}\\lib\
\*;${CLASSPATH}
```

Step 10 (For MapR Distribution only) Install MapR client in TES master machine, and add the following lines in the service.props file

```
jarlib=mapr
JVMARGS=-Djava.library.path=C:\\opt\\mapr\\hadoop\\hadoop-0.20.2\\lib\\native\\Windows_
7-amd64-64
CLASSPATH=C:\\opt\\mapr\\hadoop\\hadoop-0.20.2\\lib\\*;${CLASSPATH}
```

Step 11 Restart the Master.

Note Make sure jdk is installed in the machine and set the JAVA_HOME, and add JAVA_HOME/bin to the system PATH. The path to the database drivers and the sqoop jars must be added to the HADOOP_CLASSPATH

Basic Configuration

Before you run TES, you should customize its configuration to suit the needs of your organization. You can add or adjust production schedule parameters, mail configuration, default job properties, security restrictions and many other details. One of TES's many strengths is its flexible architecture.

During installation of TES, one user account is created containing the installer's user name. Included in the user record is a security policy which is a list of the TES functions that are available to you. By default, this account is considered the TES Administrator and has the ability to perform all functions (Super User).

Basic configuration is complete when you have finished adding users. Advanced configuration options include creating and editing security policies, setting logging options and creating queues and agent lists. The *Cisco Tidal Enterprise Scheduler User Guide* contains detailed information about using and configuring TES.

You can configure most properties of the master through the System Configuration dialog box of the Tidal Web client while other major master parameters are managed through the *master.props* file on the master machine as described later in this chapter.

Note Ensure that the regional settings used by the Tidal Web clients are the same as the regional settings used on the Window master. Different regional settings may use different formatting for dates and time. If the master is not using the same regional settings, alerts and job activity may not operate correctly.

Database Connection Pool Configuration

The number of database connections on the Master needs to match the expected load of the system. For example, if the number of database connections is set to 2 on the Master and the number of sync threads is set to 12 on the Tidal Web client, there will be 12 simultaneous threads spawned on the Master competing for 2 database connections. Depending on how long the 2 connections are held, there will be times when one or more of these Master threads will fail processing sync requests due to not being able to get a connection. Thus, it's important to set the number of database connections on the Master to meet the needs of both regular Master processing and for the sync. If the Tidal Web client has 12 sync threads, the number of connections on the Master should be set slightly higher than 12. The number of database connections can be set using the DatabaseConnections setting in *master.props*.

Configuring Tidal Web client

Launching the Tidal Web client

To launch the Tidal Web client:

Go to http://<servername>:8080/client and log on using install Super User's network credentials.

System Configuration

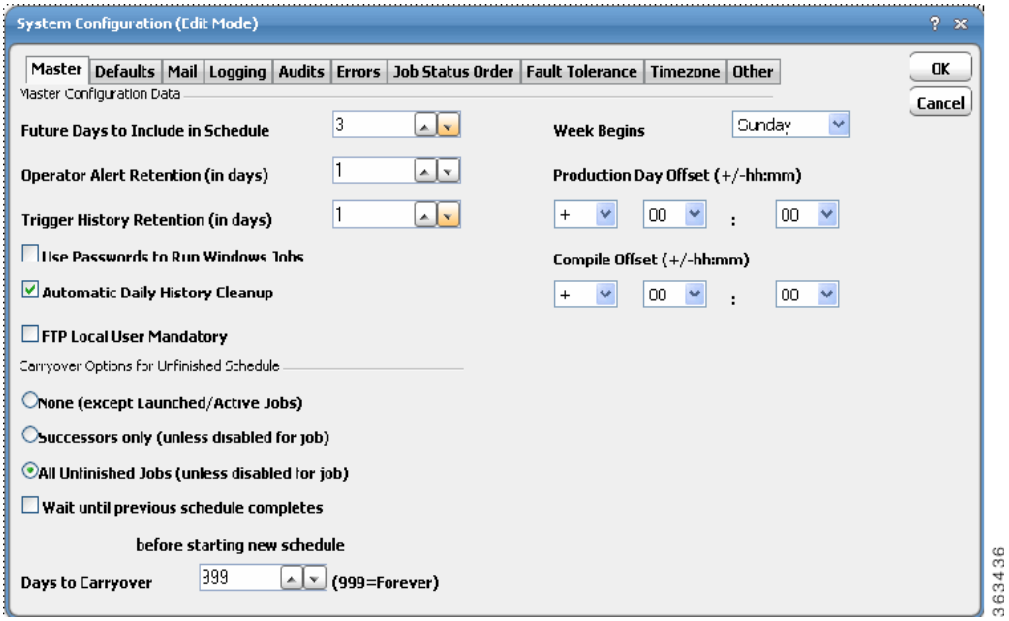
Before using TES, configure master operation parameters, job defaults, mail system connections (if you are using email), and job status sort order.

To configure:

Step 1 Launch the Tidal Web client.

Step 2 From the Activities menu, choose **System Configuration**. The System Configuration dialog box displays.

Figure 8-1 System Configuration Dialog Box



Refer to the *Getting Started* chapter in the *Cisco Tidal Enterprise Scheduler User Guide* for more information on the options in the System Configuration dialog box.

Master Tab

Basic operational behavior of the master is controlled by the settings on this tab.

This tab contains the following elements:

Element	Description
Master Configuration Data Panel	
Future Days to Include in Schedule	Controls the number of future days to include in the production schedule when the master does its daily compilation. Larger values let you schedule jobs farther into the future. Lower values reduce compilation time. **Note** When you change the Future Days to include Schedule value, the new value will not take effect until the production schedule is compiled. Compilation takes place at midnight, by default.
Operator Alert Retention	The number of days to keep operator alert information in the Job Activity pane. **Note** By default, alerts are kept for seven days. Alerts that are older than the Operator Alert Retention value are purged daily.
Trigger History Retention (in days)	Sets the default number of days to maintain event trigger history on the Trigger History tab of the Event Details dialog box. The maximum length of time to keep trigger history information is 9,999 days but this length of time requires ***very large amounts of hardware and resources*** and hampers performance. The default setting is for 30 days.
Use Passwords to Run Windows Jobs	Enables (if checked) Windows agents to use Windows passwords. Windows agents can be configured to use a per-job password. Each scheduled job can be configured to run under a specific username and password (runtime users). The job inherits the permissions and resources of the assigned user account. This means that all runtime users require valid passwords. Any jobs that log on as users with invalid or missing passwords will fail with a status of "Error Occurred." TES stores the passwords in encrypted form within its own database. At no time is an unencrypted password echoed to the screen or made otherwise accessible to any user. Passwords are also encrypted when passed from a master to an agent. For more information on the security rights needed to run Windows jobs refer to the "User Security Requirements". ⚠ **Caution** Checking the passwords of multiple users when running jobs restricts the Windows agent to only processing 30 jobs concurrently. If passwords are not used when running Windows jobs, the Windows agent can handle up to 80 concurrent jobs. TES stores the passwords using 64-bit block cipher encryption within its own database. At no time is an unencrypted password echoed to the screen or made otherwise accessible to any user. Passwords are also encrypted when passed from a master to an agent.

Element	Description
Automatic Daily History Cleanup	When this option is selected, TES automatically purges the database everyday. By default, the purge is executed at the beginning of the new production day. **Note** The master will log any errors when purge is performed automatically. When this option is not selected, TES will not automatically purge your database of old information history. It is up to the user to manually perform the purge. The user can script or manually execute the purge.
FTP Local User Mandatory	Requires that a local (or runtime) user be selected on the Run tab of FTP job definitions. Using a runtime user adds additional security to FTP jobs. The default is to not use a runtime user (unselected). If this option is selected, any previous FTP jobs that were defined without assigning a local user, will error out until a local user is assigned to the job.
Carryover Options for Unfinished Schedule Panel	
Note The following exceptions apply to these global carryover settings: • The carryover configuration of a parent job overrides the settings in its child jobs. So if the carryover option is disabled in a child job but the parent job is set to the carryover, the child job will be set to carryover. • If a job is configured to run within a time window and the time window has passed when the job carries over then the job will not carryover once the job has timed out. • Individual jobs can override global carryover settings by selecting the Disable carryover option on the Options tab of a job definition.	
None (except Launched/Active Jobs)	Do not transfer any jobs from the current production schedule to the next production schedule unless the jobs have already launched or are in active status. (On an individual basis, jobs can be prevented from carrying forward by selecting the Disable carryover option from the Options tab of the Job Definition dialog box.)
Successors only (unless disabled for job)	Transfers to the following production schedule any successor jobs from active jobs in the current production schedule unless the Disable carryover option was selected in a job's definition.
All Unfinished Jobs (unless disabled for job)	Transfers any jobs that did not run in the current production schedule to the following production schedule unless the Disable carryover option was selected in a job's definition.
Wait until previous schedule completes before starting new schedule	This option prevents any jobs from a new production schedule regardless of their priority from running until all of the jobs from the previous schedule are completed or cancelled. If the production day rollover is held up while waiting for the previous day's jobs to complete, a warning is recorded in the Audit log. To rollover to a new production schedule after selecting this option, you must either cancel the previous day's jobs that are still running or change the jobs' status to completed.
Days to Carry Over	Use this option to specify the number of days to carry over unfinished jobs. When the number you specify is reached, TES will no longer include the jobs that have not run yet in the next production schedule.

Element	Description
Production Day Offset [+/- hh:mm]	The Production Day Offset value adjusts the beginning of the production "day" to start the specified number of hours/minutes before or after midnight of the "real" day. For example, if you enter a +03:00, your calendar for the day will not start until 3:00 am. **Note** If the production day offset is modified, you must recompile the current and future production schedule for the changes to take effect. If a negative offset is specified, the master should be restarted and then the current and future production schedules must be recompiled.
Compile Offset [+/- hh:mm]	This option adjusts your compile time to start the specified number of hours/minutes before or after the beginning of the production day. The default compile time is midnight, because midnight is the default time for the beginning of the production day. If you have set a Production Day Offset value (above) the Compile Offset value will be adjusted from the new beginning of the production day.
Week Begins	This option affects the starting date of all subset calendars that use weekly definitions. After changing the value in this tab, choose **Recalculate** from the Calendars pane context menu to have the changes take effect.

Defaults Tab

The Defaults tab allows you set default job properties that will apply whenever a user create a new job. These defaults can be changed for individual job definitions.

This tab contains the following elements:

Table 8-1 Defaults Tab Elements

Element	Description
Job Defaults Panel	
Agent Name	Sets the default agent for the Agent Name setting in the Job/Group Definition dialog boxes.
Job History Retention (in days)	Sets the default number of days of job history to keep. The Job History Retention setting can be individually configured for jobs on the Options tab of the Job/Group Definition dialog boxes. The maximum length of time to keep job history information is 9,999 days but this length of time requires *very large amounts of hardware and resources* and hampers performance.
Job Priority	Sets the default for the Job Priority setting in the Job/Group Definition dialog boxes.
If job is currently running	Sets the default for the If job is currently running setting (concurrency) in the Job Definition dialog boxes. There are four options: • Run Anyway Run another job instance even if the previous instance is still running. • Skip Do not run another job instance if the previous instance is running. • Defer until Normal Run another job instance only if the current job instance completes with a Normal status. • Defer Until Complete Run another job instance only after the current job instance completes.

Element	Description
Base time needed to run job on	Sets the default basis for evaluating whether jobs will complete before a scheduled outage. Whether jobs have adequate time to run can be based on either of the following factors: • Estimated Duration The estimated duration for the command or executable as specified in the job definition. If the job has run more than once with the same command or executable, the estimated duration is the historical average of the job's previous run times. You can also manually set the estimated duration time of a job in its definition. • Maximum Duration The maximum duration for the command or executable as specified in the job definition. If the job has run more than once with the same command or executable, the estimated duration is the historical average of the job's previous run times. You can also manually set the estimated duration time of a job in its definition.
If not enough time before outage	Sets the default action for occasions when a job may run into an outage window as based on the evaluation option set in the Base time needed to run jobs on field. There are three options: • Run Anyway Run the job instance even at the risk that the job may not complete before the outage window. • Skip Do not run the job instance if it may run into an outage window. • Defer Wait to run the job until after the outage window has ended.
Unscheduled allowed	Sets the default for the Unscheduled Allowed setting in the Job Definition dialog boxes.
Disable carryover	Prevents any jobs that did not run during the current production schedule from being carried over to the next production schedule. If you wish to carry over jobs to the next production schedule, refer to the Carryover Options for Unfinished Schedule section on the Master tab to configure which jobs should carry over to the next day's production schedule.
For Unix, source user's profile	Allows you to execute Unix user profiles. This global option provides for the execution of all variables in a Unix user's profile. This option is available in individual job definitions on the Options tab so that job instances do not have to default to a source user's profile. Without this option, any Unix user profile variables that are referenced by scripts will not be executed, causing a job to fail in TES.
Save Output	Sets the default handling of job output. • Discard Does not save the job output. (Default) • Append Saves the complete output from each job instance, adding the output to the previous job instance's output. • Replace Saves the complete output from each job instance, overwriting the previous job instance's output.
Summary Only for ERP Jobs	This check box only applies to SAP, PeopleSoft and Oracle Applications jobs. Selecting this option saves the job output in a summary form. This option is useful when ERP jobs have long job output and you do not want the entire output file. Not available if the Discard option is selected.
Other Defaults Panel	
Public	Sets the public option default in the Variables, Calendars, Job Events, System Events and Actions dialog boxes. Public items are available to all users of TES with an appropriate security policy.

Mail Tab

If you install TES in a network that supports email, the TES master can send messages to any user of that email system through the Mail tab.

You can send email outside of the company to any user or group of users (mailing list) with a valid email address.

Note If you are running Fault Tolerance, test email on the backup master as well as on the primary master. This ensures that in a failover situation, all email notifications will continue to function

.For TES to use Internet Mail effectively, the master machine must have a continuous Internet connection. If the mail system goes offline, you will miss email notifications.

Note It is acceptable for the master to be configured to use the LocalSystem option when using SMTP mail.

Prerequisites

Before using TES's email functions:

Step 1 Select a user mail account for the TES master. Verify that this user can send email from outside of TES before designating it for use by the master. When the TES master sends email messages, the From: field of the message header will display this user name.

Step 2 Specify a user account in the Mail tab of the System Configuration dialog box. The account must be recognized by your existing email system.

Step 3 Using the Tidal Service Manager, set the TES master service to run as a user. The user must have access to the mail system and the advanced local user right Logon as a service.

For systems using Simple Mail Transport Protocol:

Step 1 Choose **Internet Mail (SMTP)** from the Mail System list.

Step 2 Enter an address separator into the Address Separator field. Enter a character that your mail system understands as a delimiter between multiple email addresses that are entered on one line. TES can accept only one character in the Address Separator field, although your mail system may understand more than one character as an address separator. For example, you may be able to use either a comma or a semi-colon between email addresses

Step 3 Type the directory path to your SMTP server location into the SMTP Server Address field.

Step 4 Type your internet email address in the Return Address field. This will be in a form similar to: username@yourcompany.com.

Logging Tab

In the Logging tab, you can set preferences related to TES audit, error and diagnostic messages.

Note It is recommended that anti-virus software either be disabled during diagnostic logging or configured to not check the diagnostic files that are created during diagnostic logging. The constant writing of diagnostic information to these files will consume too much attention from the anti-virus software and consume an extensive amount of system resources. By default, the diagnostics file for the Tidal Web client, *sadiags.txt,* is located at *C:\Program Files\TIDAL\Scheduler\client*. The default location for diagnostic logs on the master machine is *C:\Program Files\TIDAL\Scheduler\master\logs*. More information about diagnostic logging is available in "Troubleshooting".

Table 8-2 Logging Tab Elements

Element	Description
Log Message Retention (in days) Panel	
Audits	The length of time to keep audit information. The maximum length of time to keep audit information is 9,999 days but this length of time requires ***very large amounts of hardware and resources*** and hampers performance. The default is seven days.
Errors	The length of time to keep error information. The maximum length of time to keep audit information is 9,999 days but this length of time requires ***very large amounts of hardware and resources*** and hampers performance. The default is 30 days.
Audits Panel	Select this check box to activate audit logging. When checked, auditing information will be collected and can appear in the Logs pane. The following is a list of available auditing sources: • Master Displays audit messages that originate from the master. • Client Displays audit messages that originate from all Tidal Web clients connected to the master. • Agent Manager Displays audit messages that originate from licensed agents that run jobs. The Agent Manager:CQD category displays messages dealing with the underlying agent communications protocol. • Fault Tolerance Displays audit messages from the Fault Monitor machine. • Dependency Manager Displays messages about when dependencies for jobs and job groups are met. • Job Manager Displays messages about the status of jobs. • Action Manager Displays messages about all configured actions. • Queue Manager Displays messages about queue activity. • Agent Messenger:CQD Because of the volume of CQD diagnostic messages, you can clear the Agent Messenger: CQD source for messages while still gathering information regarding your agent(s) from the Agent Manager source.
Diagnostic Panel	The following components can be monitored and their activity logged.
Scheduler Log	Records system level messages regarding the master
Client Manager Log	Records messages about Client Manager activity
Agent Manager Log	Records messages about the status of production schedules being compiled.
Compiler Log	Records messages about the status of production schedules being compiled.

Element	Description
Job Manager Log	Records messages about the status of jobs
Event Manager Log	Records messages about events defined in TES.
Queue Manager Log	Records messages about queue activity.
Database Log	Records messages relating to the state of the database.
Communications Log	Records messages concerning all defined connections and sockets. Be aware that setting this component to a high level of logging results in a large amount of information that consumes large amounts of disk space.
Each component within the Diagnostic panel has a list with seven levels of progressively more detailed logging. Each level includes the messages of the previous levels of logging. The levels of logging are: • None No logging for the component. • Severe Logs only serious problems for that component. (default) • Warning Logs potential problems for the component as well as messages from the Severe logging level. • Info Logs status messages about the normal operation as well as messages from lower logging levels. • Low Debug Logs important debugging messages as well as messages from lower logging levels. • Medium Debug Logs an increasing amount of debugging information as well as messages from lower logging levels. • High Debug Logs the largest amount of debugging information as well as messages from lower logging levels.	
Client Diagnostics Panel	Enables diagnostics for the Tidal Web client. Creates a text file called *sadiags.txt* in the directory where the Enterprise TES files reside. The *sadiags.txt* file can be opened in any text editor. This option replicates the Debug option available in the Poll Activity pane of the Master Status pane.
Log Message Retention (in days) Panel	
Audits	The length of time to keep audit information. The maximum length of time to keep audit information is 9,999 days but this length of time requires ***very large amounts of hardware and resources*** and hampers performance. The default is seven days.
Errors	The length of time to keep error information. The maximum length of time to keep audit information is 9,999 days but this length of time requires ***very large amounts of hardware and resources*** and hampers performance. The default is 30 days.

Note Do not delete the current log file, which is always the log file with the latest timestamp. Even if the file does not exist, the master will continue to relay diagnostic information to the log file until it has relayed 1 MB of information. At that point, the master starts a new log file but any diagnostic information from the time between the deletion of the current log file and the creation of a new log file is lost.

Audits Tab

The Audits tab lists all of the audit messages that can be issued by TES. You can exclude any single message from being issued. For each message, you can also specify whether it will be posted to the Windows event log, which can be seen in the Windows Event Viewer.
It is recommended that you keep the defaults on this tab. For more information about audit, error and diagnostic messages, refer to the *Cisco Tidal Enterprise Scheduler User Guide*.

Errors Tab

The Errors tab lists all of the error messages TES can issue.
Error messages can be viewed from the Logs pane. The first error message listed (with the 2000 ID number) is blank because it is available for creating a custom error message. Here you can instruct TES to exclude specific error messages.

It is recommended that you keep the defaults on this tab. For more information about audit, error and diagnostic messages, refer to the *Cisco Tidal Enterprise Scheduler User Guide*.

Job Status Order Tab

The Job Status Order tab allows you set the job status order used for sorting jobs and job groups by status in the Job Activity pane.

In the Job Status Sort Order panel, the default when sorting jobs by status is to sort alphabetically.

A recommended sort order would be to place jobs in the following categories:

- Jobs that require immediate attention placed at the top of the list.
- Jobs that were operated on placed second.
- Jobs that failed based on normal conditions placed third.
- Jobs that are proceeding normally placed last in a typical status order

This tab contains the following elements:

Figure 8-2 Job Status Tab Elements

Suggested Sort Order	Description
Group 1	Jobs that need immediate attention
Waiting On Operator	Jobs that are waiting for the operator to release them.
Error Occurred	Jobs that could not be started.
Agent Inactive	Jobs whose agents are currently not enabled.
Agent Unavailable	Jobs whose agents are unavailable.
Orphaned	Jobs whose agents became unavailable during execution.
Externally Defined	Jobs whose completion status needs to be set.
Completed Abnormally	Jobs that completed abnormally
Group 2	Jobs that were operated on
Held	Operator put waiting job on hold.
Cancelled	Operator cancelled waiting job.
Stopped	Operator paused active job.

Suggested Sort Order	Description
Aborted	Operator aborted active job.
Group 3	Jobs that failed based on other external circumstances
Timed Out For Day	Job dependencies not met within time window. Will try to run again tomorrow.
Timed Out	Job dependencies not met within time window.
Skipped	Job skipped because another occurrence was already running.
Deferred	Job waiting for its previous occurrence to finish.
Group 4	Jobs proceeding normally
Scheduled	Limited status for jobs in the Production Schedule.
Waiting On Dependencies	Jobs waiting on dependencies to be met.
Waiting On Children	Job groups with at least one child waiting to run.
Waiting On Group	Jobs waiting on group dependencies to be met.
Waiting On Resource	Jobs waiting for a system resource slot to run.
Launched	Jobs that have been submitted to an agent to run.
Active	Jobs running.
Completed Normally	Jobs completed normally.

SAP Tab

This tab is for configuring the SAP adapter. The SAP Adapter requires a special license.

OracleApps Tab

This tab is for configuring the Oracle Applications Adapter. The Oracle Applications Adapter requires a special license.

Fault Tolerance Tab

This tab is for configuring failover to a backup master Scheduler.

Timezone Tab

The Timezone tab of the System Configuration dialog box allows you to define timezones where target application environments are based. This allows you to schedule a job or job group across a different timezone.

Other Tab

The Other tab has the following options that present job information.

This tab contains the following elements:

Element	Description
Job Definition Confirmations Panel	
Confirm Job Enable	Displays a confirmation message whenever a job is enabled
Confirm Job Disable	Displays a confirmation message whenever a job is disabled
2.5.3 Compatibility	
Allow Job Rerun on any Completed Normally and Completed Abnormally Status	Select to allow a rerun of a job that has completed with a status of Completed Normally or Completed Abnormally.
Wait	Specified interval in seconds after a connection is lost to either an agent or an adapter before the system event Lost connection to agent/adapter is triggered. The default value is a zero delay
Remove the Browse button for Command and File parameters	Select to disable the Browse option when entering Command an File parameters.

Configuring the Master Parameters

You can change the properties of the master that were set during installation. Circumstances may force you to change the configuration of the master as it was originally installed.

The properties of the master are managed in a file called *master.props* that resides in the *config* directory on the master machine. A complete list of parameter settings and their default values managed by the *master.props* file is provided in *Appendix C* of the *User Guide*.

The *master.props* file on the master looks like the following example:

JdbcURL=jdbc:sqlserver://SJC-Q8-WVM3:1433;responseBuffering=adaptive

JdbcDriver=com.microsoft.sqlserver.jdbc.SQLServerDriver

Classpath=${TIDAL_HOME}\lib\Scheduler.jar;${TIDAL_HOME}\lib\sqljdbc.jar;${TIDAL_HOME}\lib\ojdbc14.jar;${CLASSPATH}

CMDMasterPort=6600

JAVA_HOME=C:\Program Files\Java\jre6

JVMARGS=-Xms1024m -Xmx2048m

You change the configuration properties of the master by manually adding a new property or modifying the value for an existing property. Be careful when changing the properties of the master, incorrect entries to the *master.props* file may prevent the proper operation of the master. Do not add a master property to the *master.props* file and leave it blank after the equals (=) sign.

Table 8-3 contains a subset of the properties that are managed in the *master.props* file are listed below:

Table 8-3 master.props properties

Property	What it controls
JdbcDriver	Database connection driver
JdbcURL	Database connect string

Property	What it controls
classpath	The path to the packages used in the program
JAVA_HOME	The path to the Java home directory
JVMARGS	Property that sets the JVM argument (Windows only)
snmphost	Name of the machine where the SNMP software was installed.
snmpport	Number of the port used by the SNMP software.
CMDMasterPort	Number of the port that the command line program uses to connect to the master machine.
EncryptAgent	By default, the master will send data to the agent in encrypted form, without need to specify this parameter. To disable encryption, add this parameter with value (N) to *master.props* file and restart master service.
AgentHeartBeatInt	Seconds between heartbeats.
AgentHeartbeatFailureCount	Number of missed heartbeats allowed before declaring the connection bad.
AgentResendMsgInt	Time interval after which an unasked message is resent to the master.
FileMonitorInt	Specifies the time interval (in seconds) for an agent to check for files.
DirectoryMonitorInt	Specifies the time interval (in seconds) for an agent to check directories for files (file events).
GWStartedTaskExclude	Any job names that match the criteria listed in the GWStartedTaskPrefix parameter but that should not be considered a Started Task are listed here. The jobs listed in this parameter continue to be considered JES jobs. Each prefix in the list is separated by a comma.
GWStartedTaskPrefix	Any job names that match the criteria listed, will be monitored as Started Tasks unless explicitly excluded by GWStartedTaskExclude parameter. Each prefix in the list is separated by a comma.

Configuring SSL Messaging

This section discusses the procedure to configure SSL messaging on a TES 6.2 system. TES uses Java Messaging Service (JMS) to implement communications among its components, including:

- Primary Master
- Remote Master
- Backup Master
- Fault Monitor
- Client Manager

This document discusses SSL configuration for each of these components.

Obtaining Server Keys and Certificates

You will need a pair of server key and certificate for each of the following components:

- Client Manager
- Primary Master

If you are setting up a Remote Master, you will need a pair of server key and certificate for it too.

If you are setting up a fault tolerant system, you will also need a pair of server key and certificate for each of the following components:

- Backup Master
- Fault Monitor

All of these servers require keys and certificates be stored in Java Keystore (JKS) files.

You may generate key and certificate by yourself or obtain them from a trusted certificate authority (CA).

1. Generating Key and Certificate

   There are various tools that allow you to generate keys and certificates, among them the Java Keytool that comes with JRE installation.

   Java Keytool Example: generating key & certificate in a keystore

   keytool -keystore my_keystore -alias my_alias -genkey -keyalg RSA

   You can use the keys and certificates you generate to get your implementation and testing going quickly. However, to set up a production grade server, it's recommended you request a well known certificate authority (CA) to sign the keys and certificates.

2. Obtaining Key and Certificate from a Trusted CA

   There are many trusted CA's, such as AddTrust, Entrust, GeoTrust, RSA Data Security, Thawte, VISA, ValiCert, Verisign, beTRUSTed. Each CA has its own instructions which should be followed (look for JSSE section), but all will involve a step to generate a certificate signing request (CSR).

   Java Keytool Example: generating CSR

   keytool -certreq -alias my_alias -keystore my_keystore -file my_csr.csr

3. Exporting and Importing Certificate

   When SSL messaging is enabled, each of TES servers will only send messages to and accept messages from the servers it trusts. To authorize messaging between two servers, you must make sure the certificate of one server is registered in the other's trust store, and vice versa. Java Keytool provides certificate import and export options to help you accomplish this goal.

   Java Keytool Example: exporting certificate from a key store to a file

   keytool -export -alias my_alias -file my_cer.cer -keystore my_keystore -storepass my_keystore_password

   Java Keytool Example: importing certificate from a file to a trust store

   keytool -import -v -trustcacerts -alias my_alias -file my_cer.cer -keystore my_truststore -storepass my_truststore_password

   Each of the following sections describes configuration for each TES server. It will indicate what other TES server's certificates must be imported into TES server's trust store.

Configuring SSL on the Primary Master

In this section, you will enable SSL on the Primary Master with the key stores you obtained from earlier section.

To enable:

Step 1 Shut down the Primary Master.

Step 2 Copy the key store for the Primary Master to the **config** directory in the Master's installation directory.

Step 3 Create a trust store by importing Client Manager's certificate. Follow the instructions in "Obtaining Server Keys and Certificates".

If you are setting up Remote Master, import the certificate of the Remote Master into this trust store too.

If you are setting up a fault tolerant system, import the certificate of the Fault Monitor into this trust store too.

When done, copy the trust store to the **config** directory in the Master's installation directory.

Step 4 Use a text editor to open the property file *master.props* located in the Master's installation directory.

Note It may be a good idea to back up this file before editing it to ensure there is a good copy to fall back to.

Step 5 In the editor, locate the segment of SSL properties that looks like the following.

#MessageBroker.SSL.enabled=Y

#MessageBroker.SSL.keyStore=

#MessageBroker.SSL.keyStorePassword=

#MessageBroker.SSL.keyPassword=

#MessageBroker.SSL.trustStore=

#MessageBroker.SSL.trustStorePassword=

If such segment can't be found, manually insert these lines.

Uncomment each property starts with "#MessageBroker.SSL." by removing the leading pound sign '#' character.

The property MessageBroker.SSL.enabled determines whether to activate other SSL properties and enable SSL messaging. Value 'Y' means yes, and 'N' no. You can use this property switch between SSL and non SSL messaging modes.

Step 6 For each of the above SSL properties, assign value applicable to your certificate.

MessageBroker.SSL.keyStore: Path to the key store

MessageBroker.SSL.keyStorePassword: Password needed to open the key store

MessageBroker.SSL.keyPassword: Password needed to read the key, if it's different from the password of the key store

MessageBroker.SSL.trustStore: Path to the trust store

MessageBroker.SSL.trustStorePassword: Password needed to open the trust store

Note You must obfuscate the passwords before storing them in the property files. Refer to Securing Key Store Passwords for instructions.

Step 7 Save the property file.

If you are setting up Remote Master, continue on to Configuring SSL on Remote Master.

Otherwise, if you setting up a fault tolerant system, continue on to Configuring SSL on the Backup Master.

Otherwise, continue on to “Configuring SSL on the Client Manager”.

Configuring SSL on Remote Master

In this section, you will enable SSL on Remote Master with the key stores you obtained from earlier section.

To enable:

Step 1 Shut down the Remote Master.

Step 2 Copy the key store for the Remote Master to the *config* directory in the Master's installation directory.

Step 3 Create a trust store by importing the certificates of Primary Master. Follow the instructions in "Obtaining Server Keys and Certificates".

If you are setting up a fault tolerant system, import the certificates of the Backup Master and Fault Monitor into this trust store too.

When done, copy the trust store to the **config** directory in the Master's installation directory.

Step 4 Use a text editor to open the property file *config/master.props* located in the Master's installation directory.

Note It may be a good idea to back up this file before editing it to ensure there is a good copy to fall back to.

Step 5 In the editor, locate the segment of SSL properties that looks like the following.

#MessageBroker.SSL.enabled=Y

#MessageBroker.SSL.keyStore=

#MessageBroker.SSL.keyStorePassword=

#MessageBroker.SSL.keyPassword=

#MessageBroker.SSL.trustStore=

#MessageBroker.SSL.trustStorePassword=

If such segment can't be found, manually insert these lines.

Uncomment each property starts with "#MessageBroker.SSL." by removing the leading pound sign '#' character.

The property MessageBroker.SSL.enabled determines whether to activate other SSL properties and enable SSL messaging. Value 'Y' means yes, and 'N' no. You can use this property switch between SSL and non SSL messaging modes.

Step 6 For each of the above SSL properties, assign value applicable to your certificate.

MessageBroker.SSL.keyStore: Path to the key store

MessageBroker.SSL.keyStorePassword: Password needed to open the key store

MessageBroker.SSL.keyPassword: Password needed to read the key, if it's different from the password of the key store

MessageBroker.SSL.trustStore: Path to the trust store

MessageBroker.SSL.trustStorePassword: Password needed to open the trust store

Note You must obfuscate the passwords before storing them in the property files. Refer to Securing Key Store Passwords for instructions.

Step 7 Save the property file.

If you setting up a fault tolerant system, continue on to Configuring SSL on the Backup Master. Otherwise, continue on to Configuring SSL on the Client Manager.

Configuring SSL on the Backup Master

In this section, you will enable SSL on the Backup Master with the key stores you obtained from earlier section.

To ena ble:

Step 1 Shut down the Backup Master.

Step 2 Copy the key store for the Backup Master to the **config** directory in the Master's installation directory.

Step 3 Create a trust store by importing Client Manager's certificate. Follow the instructions in "Obtaining Server Keys and Certificates"e. Import the certificate of the Fault Monitor into this trust store too.

If you are setting up Remote Master, import the certificate of the Remote Master into this trust store too.

When done, copy the trust store to the *config* directory in the Master's installation directory.

Step 4 Use a text editor to open the property file *config/master.props* located in the Master's installation directory.

Note It may be a good idea to back up this file before editing it to ensure there is a good copy to fall back to.

Step 5 In the editor, locate the segment of SSL properties that looks like the following.

#MessageBroker.SSL.enabled=Y

#MessageBroker.SSL.keyStore=

#MessageBroker.SSL.keyStorePassword=

#MessageBroker.SSL.keyPassword=

#MessageBroker.SSL.trustStore=

#MessageBroker.SSL.trustStorePassword=

If such segment can't be found, manually insert these lines.

Uncomment each property starts with "#MessageBroker.SSL." by removing the leading pound sign '#' character.

The property MessageBroker.SSL.enabled determines whether to activate other SSL properties and enable SSL messaging. Value 'Y' means yes, and 'N' no. You can use this property switch between SSL and non SSL messaging modes.

Step 6 For each of the above SSL properties, assign value applicable to your certificate.

MessageBroker.SSL.keyStore: Path to the key store

MessageBroker.SSL.keyStorePassword: Password needed to open the key store

MessageBroker.SSL.keyPassword: Password needed to read the key, if it's different from the password of the key store

MessageBroker.SSL.trustStore: Path to the trust store

MessageBroker.SSL.trustStorePassword: Password needed to open the trust store

Note You must obfuscate the passwords before storing them in the property files. Refer to Securing Key Store Passwords for instructions.

Step 7 Save the property file.

Step 8 Continue on to Configuring SSL on the Fault Monitor.

Configuring SSL on the Fault Monitor

In this section, you will enable SSL on the Fault Monitor with the key stores you obtained from earlier section.

To enable:

Step 1 Shut down the Fault Monitor.

Step 2 Copy the key store for the Fault Monitor to the **config** directory in its installation directory.

Step 3 Create a trust store by importing Client Manager's certificate. Follow the instructions in Exporting and Importing Certificate. Import the certificates of the Primary Master and Backup Master into this trust store too.

When done, copy the trust store to the *config* directory in the installation directory.

Step 4 Use a text editor to open the property file *config/master.props* located in the installation directory.

Note It may be a good idea to back up this file before editing it to ensure there is a good copy to fall back to.

Step 5 In the editor, locate the segment of SSL properties that looks like the following.

#MessageBroker.SSL.enabled=Y

#MessageBroker.SSL.keyStore=

#MessageBroker.SSL.keyStorePassword=

#MessageBroker.SSL.keyPassword=

#MessageBroker.SSL.trustStore=

#MessageBroker.SSL.trustStorePassword=

If such segment cannot be found, manually insert these lines.

Uncomment each property starts with "**#MessageBroker.SSL**." by removing the leading pound sign '#' character.

The property MessageBroker.SSL.enabled determines whether to activate other SSL properties and enable SSL messaging. Value 'Y' means yes, and 'N' no. You can use this property switch between SSL and non SSL messaging modes.

Step 6 For each of the above SSL properties, assign value applicable to your certificate.

MessageBroker.SSL.keyStore: Path to the key store

MessageBroker.SSL.keyStorePassword: Password needed to open the key store

MessageBroker.SSL.keyPassword: Password needed to read the key, if it's different from the password of the key store

MessageBroker.SSL.trustStore: Path to the trust store

MessageBroker.SSL.trustStorePassword: Password needed to open the trust store.

Note You must obfuscate the passwords before storing them in the property files. Refer to Securing Key Store Passwords for instructions.

Step 7 Save the property file.

Step 8 Continue on to Configuring SSL on the Client Manager.

Configuring SSL on the Client Manager

In this section, you will enable SSL on the Client Manager with the keystores you obtained from earlier section.

Step 1 Shut down the Client Manager.

a. Copy the key store for the Client Manager to the *config* directory in the Client Manager's installation directory.

b. Create a trust store by importing Primary Master's certificate. Follow the instructions in "Obtaining Server Keys and Certificates".

If you are setting up a fault tolerant system, import the certificates of the Backup Master and Fault Monitor into this trust store also.

When done, copy the trust store to the *config* directory in the Client Manager's installation directory.

Step 2 Use a text editor to open the property file *config/clientmgr.props* located in the Client Manager's installation directory.

Note It may be a good idea to back up this file before editing it to ensure there is a good copy to fall back to.

Step 3 In the editor, locate the segment of SSL properties that looks like the following.

#MessageBroker.SSL.enabled=Y

#MessageBroker.SSL.keyStore=

#MessageBroker.SSL.keyStorePassword=

#MessageBroker.SSL.keyPassword=

#MessageBroker.SSL.trustStore=

#MessageBroker.SSL.trustStorePassword=

If such segment can't be found, manually insert these lines.

Uncomment each property starts with "`#MessageBroker.SSL.`" by removing the leading pound sign '`#`' character.

The property MessageBroker.SSL.enabled determines whether to activate other SSL properties and enable SSL messaging. Value '**Y**' means yes, and '**N**' no. You can use this property switch between SSL and non SSL messaging modes.

Step 4 For each of the above SSL properties, assign value applicable to your certificate.

MessageBroker.SSL.keyStore: Path to the key store

MessageBroker.SSL.keyStorePassword: Password needed to open the key store

MessageBroker.SSL.keyPassword: Password needed to read the key, if it's different from the password of the key store

MessageBroker.SSL.trustStore: Path to the trust store

MessageBroker.SSL.trustStorePassword: Password needed to open the trust store

Note You must obfuscate the passwords before storing them in the property files. Refer to Securing Key Store Passwords for instructions.

Step 5 Save the property file.

Securing Key Store Passwords

For Client Manager

Perform the following steps if you are configuring SSL on Client Manager.

To configure:

Step 1 Open a command shell window and change directory to the *lib* directory under Client Manager's installation directory.

Step 2 Issue the following commands:

java -cp ClientManager.jar com.tidalsoft.framework.util.Pwd <your_password>

where **<your_password>** is the password to be obfuscated.

Step 3 Copy the entire line of command output and paste it into the value field of that password in property file.

Step 4 Repeat step 1 to 3 for each of the other passwords.

For Fault Monitor Or Any Master

Perform the following steps if you are configuring SSL on Fault Monitor or any Master.

To configure:

Step 1 Open a command shell window and change directory to the **lib** directory under Enterprise Scheduler's installation directory.

Step 2 Issue the following commands:

java -cp Scheduler.jar com.tidalsoft.framework.util.Pwd <your_password>

where `<your_password>` is the password to be obfuscated.

Step 3 Copy the entire line of command output and paste it into the value field of that password in property file.

Step 4 Repeat step 1 to 3 for each of the other passwords.

Defining Users

During installation of TES, one default user account is created containing the installer's user name. Included in the user record is a security policy which is a list of the TES functions that are available. This account is considered a TES Super User and has the authority to perform all functions.

Basic configuration is complete when you have finished adding users. Advanced configuration options include creating and editing security policies, setting logging options, and creating queues and agent connections. The *Cisco Tidal Enterprise Scheduler User Guide* contains detailed information about using and configuring TES.

User Configuration

The first time that you run TES, you have Super User capability which gives you full access to all TES functions.

User Definition Dialog Box

The User Definition dialog box allows you add and configure accounts for TES users.

Security Tab

This tab contains the following elements:

Element	Description
Super User	Select this option to give the user access to all available TES functions.
Other	Select this option to assign one of the defined security policies from the list.

Runtime Users Tab

The Runtime tab displays all defined TES users or user groups for this installation depending upon which option is selected on the tab. The runtime users (users for which this user is authorized to schedule and run jobs) are indicated by a check mark to the left of the listed name.

Typically the runtime users option is used by users who have the responsibility of running jobs for others, such as Schedulers or Operators. When you select runtime users for a user definition, the user will have rights and access to all of the runtime users' commands and environments, but only when scheduling and running jobs.

This tab contains the following elements:

Element	Description
Show Users	Select to show a list of user names.
Show Groups (Windows)	Select to show a list of group names.

Agents Tab

The Agents tab displays all defined TES agents for this installation. The agents on which this user is authorized to run jobs are indicated by a check mark to the left of the listed name.

Select the All Agents option when you want the user to have access to all available agents. When the All Agents option is selected, the check boxes to the left of each listed agent disappear.

Note If the All Agents option is not selected, and no individual agents are selected, the user will be unable to schedule any jobs.

Notification Tab

The Notification tab of the User Definition dialog box is used to specify and update user contact information such as phone number, pager number and email address. Scheduler or another user can use this contact information to notify you of the status of a job.

Passwords Tab

The Passwords tab allows for the maintenance of your Windows/FTP/DataMover and other adapter passwords.

This tab contains the following elements:

Element	Description
Add, Edit, Delete buttons	Add, edit and delete passwords for the adapters.
Windows/FTP/DataMover	Used for running jobs on Windows and FTP machines, when a password is required. Password characters appear as asterisks as you type them.
Confirm Password	Re-type the password you entered in Windows /FTP/DataMover to verify its accuracy.

Kerberos Page

Select the Kerberos tab if using a Hadoop cluster that is Kerberos secured.

This tab contains the following elements:

Element	Description
Kerberos Principal	Enter the Authentication URL to Hadoop.
Kerberos Key Page File	Enter the path to the Key Page file. This file is relative to the Master's file system and contains one or more Kerberos principals with their defined access to Hadoop.

Workgroups Tab

The Workgroups tab displays the workgroups under which the user is a member and the owner of the workgroup.

This tab contains the following elements:

Element	Description
Workgroup	The names of the workgroups under which the user is a member. To be a member of a workgroup, you must be added into that workgroup by the workgroup's owner.
Owner	The owners of the workgroups of which the user is a member.

Description Tab

The **Description** tab contains a free text box for any comments about the user.

User Configuration Procedures

Viewing Users

From the Navigator pane, choose **Administration > Interactive Users** to display all TES users. If the users do not display, you do not have the appropriate rights to view users.

Adding a User

To add a user:

Step 1 From the Navigator pane, choose **Administration > Interactive Users** to display all TES users.

Step 2 Click the **Add** button .

-or-

Right-click and choose **Add Interactive User** from the context menu. The User Definition dialog box displays.

Note If this option does not appear, you are not authorized to add users.

Step 3 Choose the new user name (a Windows logon name) from the User Name list.

Remember that this exact user name must have a matching Windows user account. This text box is case-sensitive.

Select the Group option if you want to select from a list of groups.

Step 4 Type the user's full name in the Full Name field. This name will be used in TES reports and some dialog boxes.

Step 5 Choose a domain name from the Domain list.

Step 6 Select the Security tab.

Step 7 Select the Security Policy for the user.

If the user needs full access to all TES functions, select the Super User option. Super User capability within TES is unrestricted.

Step 8 If this user needs to run jobs for others:

- **a.** Select the Runtime Users tab.
- **b.** Select the runtime users to add to the user's definition.
- **c.** The user will have access to the commands and environments of the runtime users you have assigned.

Step 9 Seelct the Agents tab and use the list on the Agents tab to authorize agents for this user.

Step 10 Additionally, you can select All Agents to authorize all agents.

Step 11 To enter contact information, select the Notification tab and enter the phone number, pager number and email address. This information can be used to notify the user of a job problem through an email or other action.

Step 12 To enter additional information, select the Description tab.

Step 13 Click **OK**.

Editing a User Definition

To edit a user definition:

Step 1 From the Navigator pane, choose **Administration > Interactive Users** to display all TES users.

Step 2 Double-click the user record to edit or select the user and click the **Delete** button on the TES toolbar.

-or-

Right-click the user record and choose **Edit Interactive User** from the context menu. The User Definition dialog box displays.

Step 3 Edit the user name if it does not match the Windows login name. Remember that the user name is case-sensitive.

Step 4 Edit the full name if necessary.

Step 5 Select the Security tab.

Step 6 To change the Security Policy, choose a new one from the list.

Note If you have the Super User option set, the list is disabled.

Step 7 Click the Super User option if you want the user to have access to all TES functions.

Step 8 To add or remove specific functions to a security policy, see "Security Tab".

Step 9 Select the Runtime Users tab to add or remove runtime users:

- Choose the runtime users to add to the user's definition from the Available Users list.
- To include users, select the checkbox next to the user you want to include.
- The user will have access to the commands and environments of the runtime users you have assigned.
- To exclude users, clear the checkbox next to the user you want to exclude.

Step 10 Select the Agents tab and use the list on the Agents tab to change the authorized agent for this user.

Step 11 Select the Notification tab to edit contact information for the user.

Step 12 Click the Description tab to edit the user's description.

Note You cannot edit Workgroups information from the User Definition dialog box. This is a security feature. For more information on Enterprise Scheduler workgroups, see your *Cisco Tidal Enterprise Scheduler User Guide*.

Step 13 Click **OK**.

Jobs in the production schedule that have not run yet will reflect the changes to the user data. Jobs that are running or that have completed retain the old user information.

Deleting a User

Note You cannot delete a user that presently owns a job, job event, system event, action, user defined variable or calendar.

To delete a user:

Step 1 From the Navigator pane, choose **Administration > Interactive Users** to display the Users pane, showing all TES users.

Step 2 Select the user and click the **Delete** button on the TES toolbar.

-or-

Right-click the user record and choose **Delete Interactive User** from the context menu.

A dialog box displays asking you to confirm your choice.

Step 3 Click **OK**..

Viewing Runtime Users

To view Runtime users:

Step 1 From the Navigator pane, choose **Administration > Runtime Users** to display all TES runtime users.

If the TES runtime users do not display, you do not have the appropriate rights to view users.

Step 2 Double-click the user name. The User Definition dialog box displays showing user information.

Impersonating Another User

To impersonate another user:

Step 1 From the Navigator pane, choose **Administration > Interactive Users** to display the User pane, showing all TES users.

If the TES users do not appear, you do not have the appropriate rights to view users.

Step 2 Right-click the user record to impersonate and choose **Impersonate** from the context menu.

A dialog box displays asking you to confirm your choice.

Step 3 Click **OK** in the confirmation dialog box.

To stop impersonating another user:

Choose **End Impersonate** from the Users context menu.

-or-

Choose **Activities > End Empersonate**.

Upgrading Components

Overview

This chapter discusses upgrade procedures.

The TES master and Client Manager must be on the ***SAME*** release to ensure compatibility and functionality.

Note Starting with the 6.1 release, the master running on Windows no longer uses database aliases as created by the Database Alias utility to connect to an alternate database. Instead the database connection information used by the master in 6.1 and later, is stored in the master.props file in the config directory where the master files are installed. The JdbcURL line in the master.props file is used to specify the type of database, the database server location and the port number used to connect to the database server

Upgrade Prerequisites

- Always make a backup of your data before upgrading.
- Stop the master and agent services. (Failure to terminate all TES processes will prevent the upgrade from proceeding normally.)
- Exit all TES components.
- When upgrading from previous versions, be sure that your system meets the minimum requirements for the latest version. The system requirements may have changed from the last version.
- Set your system queue to 0.
- Turn off fault tolerance so the database cannot be accessed.
- De-select the **Enable Failover** option on the **Fault Tolerance** tab of the **System Configuration** dialog in Client Manager.
- Keep your data intact by installing in the same directory in which the previous version was installed.
- Before upgrading to 6.2, ensure that the Tidal user has the right in Oracle to create triggers and sequences.
- Consult with the Licensing Administrator at Cisco. The old license file may not operate with the new version of TES that you have just installed.

Note Your shortcut icons may no longer work after an upgrade. If clicking a TES icon on the desktop does not start the component after upgrading, you need to recreate your TES shortcuts.

Note Be sure to back up your database before proceeding with this upgrade.

Upgrading the Windows Agent from 1.x to 3.x

When upgrading your Windows agent 1.x, we recommend that you uninstall the agent first, then perform a fresh install.

Upgrading the Windows Agent from 2.x to 3.x

Before upgrading the Tidal Agent for Windows, use the Tidal Service Manager to stop the agent.

To upgrade the Agent:

Step 1 Copy *Tidal Agent.msi* to the target machine, then run it.

Step 2 In the **File Download** dialog, click **Run**.

Step 3 In the **Security Warning** dialog, click **Run**.

Step 4 In the **Welcome** dialog, click **Next**.

The **Question** dialog displays.

Step 5 Click **Yes** to confirm that you want to upgrade the existing agent.

The **Wizard Complete** panel displays.

Step 6 Click **Finish**.

Upgrading the Unix Agent from 1.x to 3.x

When upgrading your Windows agent 1.x, we recommend that you uninstall the agent first, then perform a fresh install.

Upgrading the Unix Agent from 2.x to 3.x

Before the upgrade procedure, stop the Unix agent from the command line with the **`tagent <agent name> stop`** command.

To install the agent from the command line:

Note You will overwrite the existing agent files as you upgrade so be sure to install in the same directory where the existing agent files reside.

Step 1 Login as root.

Step 2 Transfer the *install.bin* and *install.sh* installation files to the target machine's **temp** directory.

Note Do not unpack the install.tar file. The file will automatically unpack during the installation process.

Step 3 Change the permissions on the two install files in the directory to make the file executable:

chmod 755 install.sh install.tar

Step 4 Begin the installation by entering:

./install.sh

An introduction screen displays as the installation program begins.

Step 5 Type `Y` to continue the installation and press **Enter**.

The **Users on this system** panel displays:

The top of the panel shows the users defined on the machine you are installing on. In some cases, you may want to select a user who is not defined on the local machine but is defined as a NIS user allowing the user to install over the network.

Step 6 Enter the name of the user to own the agent and press `Enter`.

Step 7 Designate the default directory path for installing the agent files.

If you installed the existing agent in a different directory, enter that directory path.

Step 8 Press **Enter**.

The **Agent Configuration Menu** screen displays.

Step 9 Type `1` to select the **Add Instance** option and press **Enter**.

Step 10 Enter the agent name.

Step 11 Enter the number of the port the agent should use.

Step 12 Enter the directory path for the Java binary files (JVM).

-or-

Press **Enter** to use the default Java binaries directory path.

A summary screen displays.

Step 13 Press **Enter**.

-or-

If the information is incorrect, type `n`. You are prompted again for the name, port number and directory path for the agent.

Upgrading the Windows Master from 5.3.1 to 6.2

Note Be sure to back up your database before proceeding with this upgrade.

The upgrade program upgrades both the master and the database. The database modifications are performed when the master is first started after the installation. Before upgrading, turn on diagnostic logging to collect information during the upgrade procedure. This precaution provides troubleshooting information if any difficulty is encountered during the upgrading process.

Turn on diagnostic logging by selecting the **Diagnostics** option on the **Logging** tab of the **System Configuration** dialog.

Note When upgrading the Windows master to version 6.2, the Microsoft SQL port number in the master.props file of the config directory is changed to **1433** by default. If your port number is not **1433**, change this setting in the *master.props* file to the port number you are using.

To upgrade the Windows master:

Step 1 Complete all prerequisites, including upgrading all agents.

Note The 6.2 and later versions of Scheduler have several prerequisite software components that were not required in earlier versions. The complete list of prerequisites is available in the section,Installation Prerequisites. If any of the prerequisites are not completed before installation, the upgrade procedure will not be successful.

If your installation uses an Oracle database, your database administrator must add the following Oracle privileges to the Tidal user account in Oracle before beginning the upgrade procedure or the upgrade will fail:

- Create sequence
- Create trigger

Step 2 Ensure that the system queue has been set to **0** so no new jobs will launch.

Step 3 Stop the master service through the Tidal Service Manager.

a. Click **Start>All Programs>TIDAL Software>TIDAL Service Manager**.

The **Tidal Service Manager** dialog displays.

b. Select **Scheduler Master** from the **Service** list.

c. Click **Stop**.

Step 4 Run the *setup.exe* file.

Step 5 Click **Run**.

The **Internet Explorer-Security Warning** dialog displays.

Step 6 Click **Run**.

The **Welcome** panel displays.

Step 7 Click **Next**.

The **Install Wizard Complete** panel displays.

Step 8 Click **Finish**.

The database modifications are performed when the master is first started after the installation.

Note If you face the following error while using Microsoft Server 2003, please apply the patch file from Microsoft site *http://support.microsoft.com/kb/925336*:

```
Error 1718.file C:\\WINDOWS\Installer\9d9734.msi was rejected by digital signature
policy.
```

Note If your system is using the SAP adapter, you need to verify that your system meets the new prerequisites for the SAP adapter including installing the Java Connector.

Upgrading the Unix Master from 5.3.1 to 6.2

Note Be sure to back up your database before proceeding with this upgrade.

The upgrade program upgrades both the master and the database. The database modifications are performed when the master is first started after the installation.

To upgrade to the latest version:

Step 1 Complete all prerequisites, including upgrading all agents.

Step 2 Ensure that the system queue has been set to **0** so that jobs will not launch.

Step 3 From the command line of the master machine, stop the master:

./tesm stop

Step 4 Copy *install.bin* to the target machine and change the permissions on the file:

chmod 755 install.bin

Step 5 Run the upgrade program that you copied to your machine:

sh./install.bin

The **Introduction** panel displays.

Step 6 Click **Next**.

The **Readme** panel displays.

Step 7 Verify that you have already done the prerequisites that are listed on the **Readme** screen.

If you have not completed all of the listed tasks, click **Cancel** to end the installation procedure and complete the listed prerequisites before beginning the upgrade procedure again. If you have completed the prerequisites,

Step 8 Click **Next**.

The **Choose Install Folder** panel displays.

Step 9 Enter the directory path to the **Master** folder where the master files were installed during the original installation of the master.

The Upgrade program cannot proceed without knowing where the master files it is modifying are located. You can manually enter the directory path or click **Choose** to browse through the file directory to the **Master** folder.

A confirmation message verifies that the required master directories are in the specified location.

Step 10 Click **OK**.

If the Upgrade program cannot find the master files at the specified location, an error message displays and the installation process is aborted as soon as you acknowledge the error message.

Once the directory path is confirmed, the **Pre-Installation Summary** panel displays.

Step 11 Click **Install**.

During the upgrade process, a progress bar is displayed.

When the upgrade is complete, the **Install Complete** screen displays.

Step 12 Click **Done**.

Step 13 Return to the location where you copied the *install.bin* file and delete the *install.bin* file.

It is no longer needed and may cause problems during other upgrades in the future.

Step 14 Restart the master.

./tesm start

The database modifications are performed when the master is first started after the installation.

Upgrading the Master for Unix from the Command Line

The Unix master can be installed using the installer program or by installing it from the command line.

To install from the command line:

Step 1 Copy *install.bin* to the target machine.

Step 2 Change the permissions on the *install.bin* file in the directory to make the file executable:

chmod 755 install.bin

Step 3 Open a command prompt window and enter:

 # sh ./install.bin -i console

Step 4 Press **Enter**.

The **Introduction** panel displays.

Step 5 Click **Next**.

The **Readme** panel displays.

Step 6 Verify that you have already done the prerequisites that are listed on the **Readme** screen.

If you have not completed all of the listed tasks, click **Cancel** to end the installation procedure and complete the listed prerequisites before beginning the upgrade procedure again. If you have completed the prerequisites,

Step 7 Click **Next**.

The **Choose Install Folder** panel displays.

Step 8 Enter the directory path to the **Master** folder where the master files were installed during the original installation of the master.

The Upgrade program cannot proceed without knowing where the master files it is modifying are located. You can manually enter the directory path or click **Choose** to browse through the file directory to the **Master** folder.

A confirmation message verifies that the required master directories are in the specified location.

Step 9 Click **OK**.

If the Upgrade program cannot find the master files at the specified location, an error message displays and the installation process is aborted as soon as you acknowledge the error message.

Once the directory path is confirmed, the **Pre-Installation Summary** panel displays.

Step 10 Click **Install**.

During the upgrade process, a progress bar is displayed.

When the upgrade is complete, the **Install Complete** screen displays.

Step 11 Click **Done**.

Step 12 Return to the location where you copied the *install.bin* file and delete the *install.bin* file.

It is no longer needed and may cause problems during other upgrades in the future.

Step 13 Copy the *upd.xml* file from <installation_download_directory>/Scheduler/files/config/ to the <master installation dir>/config/ directory.

When the master starts up, it checks the version of upd.xml in the config/ directory and compares it to the one in the master database. If upd.xml is newer, the database is updated.

Note Ensure that you hot fix your system to the latest hotfix available, so the master is on the same version that the *upd.xml* file is meant for.

Caution If you do not place the *upd.xml* file in the config/ directory, the following error message is displayed, and the master is shut down:

```
<master dir>\logs\scheduler.out:
The SYSVAL table entry for the database version (xx) does not match the
required version (yy). Shutting down.
```

Step 14 Restart the master.

./tesm start

The database modifications are performed when the master is first started after the installation.

Upgrading the Windows Master from 6.x to 6.2

Note Be sure to back up your database before proceeding with this upgrade.

The upgrade program upgrades both the master and the database. The database modifications are performed when the master is first started after the installation. Before upgrading, turn on diagnostic logging to collect information during the upgrade procedure. This precaution provides troubleshooting information if any difficulty is encountered during the upgrading process.

Turn on diagnostic logging by selecting the **Diagnostics** option on the **Logging** tab of the **System Configuration** dialog.

Note When upgrading the Windows master to version 6.2, the Microsoft SQL port number in the master.props file of the config directory is changed to 1433 by default. If your port number is not 1433, change this setting in the master.props file to the port number you are using.

To upgrade the Windows master:

Step 1 Complete all prerequisites, including upgrading all agents..

Note The 6.1 and later versions of TES have several prerequisite software components that were not required in earlier versions. The complete list of prerequisites is available in the section,"Installation Requirements" on page 19. If any of the prerequisites are not completed before installation, the upgrade procedure will not be successful.

If your installation uses an Oracle database, your database administrator must add the following Oracle privileges to the Tidal user account in Oracle before beginning the upgrade procedure or the upgrade will fail:

- Create sequence
- Create trigger

Step 2 Ensure that the system queue has been set to **0** so no new jobs will launch.

Step 3 Stop the master service through the Tidal Service Manager.

a. Click **Start>All Programs>TIDAL Software>TIDAL Service Manager**. The Tidal Service Manager dialog displays.

b. Select **Scheduler Master** from the **Service** list.

c. Click **Stop**.

Step 4 Run the *setup.exe* file.

Step 5 Click **Run**.

The **Internet Explorer-Security Warning** dialog displays.

Step 6 Click **Run**.

The **Welcome** panel displays.

Step 7 Click **Next**.

The **Install Wizard Complete** panel displays.

Step 8 Click **Yes** to reboot the machine so the changes from the upgrade process can take effect.

Step 9 Click **Finish**.

The database modifications are performed when the master is first started after the installation.

Note If your system is using the SAP adapter, you need to verify that your system meets the new prerequisites for the SAP adapter including installing the Java Connector.

Upgrading the Unix Master from 6.0 to 6.2

Note Be sure to back up your database before proceeding with this upgrade.

The upgrade program upgrades both the master and the database. The database modifications are performed when the master is first started after the installation.

To upgrade to the latest version:

Step 1 Complete all prerequisites, including upgrading all agents.

Step 2 Ensure that the system queue has been set to `0` so that jobs will not launch.

Step 3 From the command line of the master machine, stop the master:

./tesm stop

Step 4 Copy *install.bin* to the target machine and change the permissions on the file:

chmod 755 install.bin

Step 5 Run the upgrade program that you copied to your machine:

sh./install.bin

The **Introduction** panel displays.

Step 6 Click **Next**.

The **Readme** panel displays.

Step 7 Verify that you have already done the prerequisites that are listed on the **Readme** screen.

If you have not completed all of the listed tasks, click **Cancel** to end the installation procedure and complete the listed prerequisites before beginning the upgrade procedure again. If you have completed the prerequisites,

Step 8 Click **Next**.

The **Choose Install Folder** panel displays.

Step 9 Enter the directory path to the **Master** folder where the master files were installed during the original installation of the master.

The Upgrade program cannot proceed without knowing where the master files it is modifying are located. You can manually enter the directory path or click **Choose** to browse through the file directory to the **Master** folder.

A confirmation message verifies that the required master directories are in the specified location.

Step 10 Click **OK**.

If the Upgrade program cannot find the master files at the specified location, an error message displays and the installation process is aborted as soon as you acknowledge the error message.

Once the directory path is confirmed, the **Pre-Installation Summary** panel displays.

Step 11 Click **Install**.

During the upgrade process, a progress bar is displayed.

When the upgrade is complete, the **Install Complete** screen displays.

Step 12 Click **Done**.

Step 13 Return to the location where you copied the *install.bin* file and delete the *install.bin* file.

It is no longer needed and may cause problems during other upgrades in the future.

Step 14 Copy the *upd.xml* file from <installation_download_directory>/Scheduler/files/config/ to the <master installation dir>/config/ directory.

When the master starts up, it checks the version of upd.xml in the config/ directory and compares it to the one in the master database. If upd.xml is newer, the database is updated.

Note Ensure that you hot fix your system to the latest hotfix available, so the master is on the same version that the *upd.xml* file is meant for.

Caution If you do not place the *upd.xml* file in the config/ directory, the following error message is displayed, and the master is shut down:

```
<master dir>\logs\scheduler.out:
The SYSVAL table entry for the database version (xx) does not match the
required version (yy). Shutting down.
```

Step 15 Restart the master.

./tesm start

The database modifications are performed when the master is first started after the installation.

Upgrading the Master for Unix from the Command Line

The Unix master can be installed using the installer program or by installing it from the command line.

To install from the command line:

Step 1 Copy *install.bin* to the target machine.

Step 2 Change the permissions on the *install.bin* file in the directory to make the file executable:

chmod 755 install.bin

Step 3 Open a command prompt window and enter:

 # sh ./install.bin -i console

Step 4 Press **Enter**.

The **Introduction** panel displays.

Step 5 Click **Next**.

The **Readme** panel displays.

Step 6 Verify that you have already done the prerequisites that are listed on the **Readme** screen.

If you have not completed all of the listed tasks, click **Cancel** to end the installation procedure and complete the listed prerequisites before beginning the upgrade procedure again. If you have completed the prerequisites,

Step 7 Click **Next**.

The **Choose Install Folder** panel displays.

Step 8 Enter the directory path to the **Master** folder where the master files were installed during the original installation of the master.

The Upgrade program cannot proceed without knowing where the master files it is modifying are located. You can manually enter the directory path or click **Choose** to browse through the file directory to the **Master** folder.

A confirmation message verifies that the required master directories are in the specified location.

Step 9 Click **OK**.

If the Upgrade program cannot find the master files at the specified location, an error message displays and the installation process is aborted as soon as you acknowledge the error message.

Once the directory path is confirmed, the **Pre-Installation Summary** panel displays.

Step 10 Click **Install**.

During the upgrade process, a progress bar is displayed.

When the upgrade is complete, the **Install Complete** screen displays.

Step 11 Click **Done**.

Step 12 Return to the location where you copied the *install.bin* file and delete the *install.bin* file.

It is no longer needed and may cause problems during other upgrades in the future.

Step 13 Copy the *upd.xml* file from <installation_download_directory>/Scheduler/files/config/ to the <master installation dir>/config/ directory.

When the master starts up, it checks the version of upd.xml in the config/ directory and compares it to the one in the master database. If upd.xml is newer, the database is updated.

Note Ensure that you hot fix your system to the latest hotfix available, so the master is on the same version that the *upd.xml* file is meant for.

Caution If you do not place the *upd.xml* file in the config/ directory, the following error message is displayed, and the master is shut down:

```
<master dir>\logs\scheduler.out:
The SYSVAL table entry for the database version (xx) does not match the
required version (yy). Shutting down.
```

Step 14 Restart the master.

./tesm start

The database modifications are performed when the master is first started after the installation.

Upgrading the Client Manager from 6.0.x to 6.2

The upgrade program described above upgrades both the master and the database, but does not upgrade the Client Manager. To upgrade the Client Manager, it must be uninstalled, then reinstalled.

To upgrade the Client Manager:

Step 1 Locate the *.dsp* and *.props* files in your TES **config** directory, and then save them.

Step 2 If using external cache, run clearcache.sql in the external cache database to drop the tables and view so they can be rebuilt. The *clearcache.sql* script is located in **<CM Install Directory>/cache/<plugin name>/cachesql.zip**.

Step 3 Uninstall the Client Manager. See "Uninstalling Client Manager" .

Step 4 Reinstall the Client Manager. See "Installation Procedures" .

Step 5 Return the *.dsp* and *.props* files that you saved in Step 1 to your Enterprise Scheduler **config** directory.

a. After reinstalling the Client Manager, stop the Client Manager service through the Tidal Service Manager. See "Starting and Stopping Client Manager" .

b. Return the *.dsp* and *.props* files that you saved in Step 1 to your Enterprise Scheduler **config** directory. to overwrite the existing *.dsp* and *.props* files.

Step 6 Delete the following Client Manager folders:

Note The uninstallation program only removes the Client Manager files installed at the time of installation. If you created other files in the master directory after installation, these files are not removed. You must manually delete these additional files.

- All folders under **<CM Install Directory>/plugins**.
- All folders under **<CM Install Directory>/webapps**.

Warning **DO NOT delete client.war.**

Step 7 Restart the Client Manager service through the Tidal Service Manager. See "Starting and Stopping Client Manager" .

Upgrading the Fault Monitor for Windows

To upgrade the fault monitor:

Step 1 Load the installation DVD-ROM into the DVD-ROM drive of the machine where the fault monitor is being installed. If no screen displays, locate the main.htm file in the DVD's root directory and open it.

Step 2 On the Scheduler screen, click the **Fault Monitor** link and select the **Run this program from its current location** option in the File Download dialog.

Step 3 Follow the upgrade instructions as they appear throughout the upgrade procedure.

Step 4 When you reach the end of the upgrade procedure, click **Finish**.

Upgrading the Fault Monitor for Unix

The upgrade procedure for the Unix fault monitor requires that you copy a file from the installation DVD/Cisco.com website to the fault monitor machine which is being upgraded. Once the file is copied, you can run the upgrade program. If you are currently running fault tolerance, you can upgrade to the latest version.

To upgrade the fault monitor:

Step 1 From the Fault Monitor pane of the Tidal Web client, right-click and select the **Stop Fault Monitor** option in the context menu.

Step 2 From the installation DVD/cisco.com website, copy the upgrade file to the fault monitor machine. A file called install.bin is located at **Upgrade/FaultMon/** in each of the Unix files: Solaris, Hpux and AIX. The file can be found on the DVD-ROM at **<DVDROMDRIVE>\Upgrade\FaultMon\<operating system>\install.bin**.

Step 3 Run the upgrade program that you copied to your machine:

```
sh./install.bin
```

The Introduction panel displays.

Step 4 Read the directions on how to proceed and click **Next**. The Prerequisites panel displays.

Step 5 Verify that the prerequisites that are listed are met.

If you have not completed all of the listed tasks, click **Cancel** to end the installation procedure and complete the listed prerequisites before beginning the upgrade procedure again.

Step 6 Click Next. The Choose Install Folder panel displays.

Step 7 Enter the directory path to the FMon folder where the fault monitor files were installed during the original installation of the fault monitor.

- Manually enter the directory path.

-or-

- Click Choose to browse through the file directory to the Fault Monitor folder.
  - The Select a Folder panel displays so you can navigate to the correct folder where you installed the master files.
  - When you locate the FMon folder, highlight the folder and click OK.

Caution Be sure to enter the correct directory path. Incorrect information will cause the Upgrade program to abort.

The Upgrade program will verify that the fault monitor files that it needs are in the specified location. If you have provided the correct directory path, a confirmation message verifies that the fault monitor directories that it requires are in the specified location.

If the Upgrade program cannot find the fault monitor files at the specified location, an error message displays and the installation process is aborted as soon as you acknowledge the error message.

Step 8 Click **OK**.

The Pre-Installation Summary panel displays.

Step 9 Click Install to begin the upgrade process.

During the upgrade process, a progress bar is displayed. When the upgrade is complete, the Install Complete screen displays.

Step 10 Click the Done button to complete the upgrade process.

Step 11 Return to the location where you copied the install.bin file and delete the install.bin file. It is no longer needed and may cause problems during other upgrades in the future.

Troubleshooting

Many problems with the installation and operation of Scheduler can be eliminated by strictly following the hardware and software specifications recommended by Cisco. Due to the variance between the environment of one customer system from another customer's system, many different issues may still occur during installation of Scheduler components. While all of the possible procedures for troubleshooting installation issues cannot be covered, some of the more common ones are listed in this chapter.

Java Path Mismatch

The "Adapter Host has gone down" message covers many cases.

One case which is not obvious from the error message is that the system cannot find the JAVA path (or similar).

By default, the system will try to reconnect the Adapter Host every 5 seconds.

Access Violation During Installation

Installation of TES components requires access to COM objects. The installation cannot proceed without access to COM objects. If you get an access violation during installation of any TES component, verify that the user doing the installation has access to COM objects and if necessary enable COM object access.

TES fails to install a copy of msvcr71.dll

Occasionally, TES fails to install a copy of *msvcr71.dll* in the same directory as *saMaster.exe*, instead it depends on this dll to already be installed in the *System32* directory by optional components which are not found in a fresh, fully patched, install of Windows 2003.

Any attempt to start TES without the .dll will fail , and the failure will occur so early in TES's launching process that TES will not write a log file. Most means of launching TES (services control panel, Tidal Service Manager) will fail without error, but attempting to run *saMaster.exe* from the command line will report the missing .dll in an error message.

Workaround:

Copy *msvcr71.dll* into the same directory as the *saMaster.exe* executable. A copy can be found next to the *java.exe* executable in the JVM install (as it too requires the Microsoft Visual C runtime, but Sun does not assume an optional Microsoft component is providing it via System32).

Unable to scroll using scroll buttons, Runtime User - FireFox 3.6.x

If you can use a slider to drag down the list, but not a down button of a scroll bar, this is happening because of the following bug in Firefox.

https://bugzilla.mozilla.org/show_bug.cgi?id=511075

This Firefox bug is already fixed by Firefox and is part of Firefox 3.6.4 Beta release.

http://www.mozilla.com/en-US/firefox/all-beta.html.

Verifying and enabling COM object access

To verify and enable COM object access:

Step 1 From the Windodws Start menu, choose **Run**. The Run dialog displays.

Step 2 In the Open field, enter **DCOMCNFG** and click **OK**. The Component Services dialog displays.

Step 3 Choose **Component Services > Computers.**

Step 4 Right-click **My Computer** and choose **Properties** from the resulting menu. The My Computer Properties dialog displays.

Step 5 Select the COM Security tab.

Step 6 In the Launch and Activation Permissions section, click **Edit Default**. The Launch Permissions dialog displays.

Step 7 In the Group or user names section, highlight your user account and verify that your account has Allow Launch access.

Step 8 If the account has a Deny value, select **Allow**.

Step 9 Click **OK**.

Step 10 If the user is not listed, click **Add** and add the user ensuring the user has Allow Launch access.

Step 11 Click **OK**.

Unable to Install the Unix Master from the Command Line

Installing the Unix master from the command line, results in the installation failing as displayed in the following screen text:

aixqa08:mkelly$chmod 755 install.bin
aixqa08:mkelly$./install.bin
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

Invocation of this Java Application has caused an InvocationTargetException. This application will now exit.(LAX)

This issue is caused by not using the proper command line parameters when installing the Unix master from the command line. Follow the procedure described in "Installing the Master for Unix from the Command Line" to successfully complete the installation.

Agents

Foreground Logging for the Unix Agent

You can watch the log messages that are generated while logging is increased when troubleshooting issues with the agent. Watching the log messages being recorded to the log file while running a job may help you identify the cause of your problem. Be aware that the agent may run slower during the debugging process.

To see the agent logging in the foreground:

Step 1 From the agent *bin* directory, type:

./tagent [name of your agent] debug

To stop the debugging option, stop the agent and start it again.

OCSEXIT Jobs

If you find that jobs created using the OCSEXIT variable, and that run on Windows agents, consistently end in Completed Abnormally you may need to update your system path.

To update your system path:

Step 1 Right-click **My Computer** and choose **Properties** from the resulting menu. The System Properties window displays.

Step 2 Select the Advanced tab and click **Environment Variables**. The Environment Variables dialog displays.

Step 3 Append **%systemroot%\system32** to your system's Path variable.

Step 4 Click **OK**.

Master Error

The TES master runs as a Windows service. Services need to be started and controlled through a service manager, such as the TES Tidal Service Manager utility. Double-clicking the *samaster.exe* file or an icon shortcut associated with this executable will result in application errors and an access violation.

To resolve this issue, always start and stop the TES master through the TES Tidal Service Manager.

Changing the System Clock

Before changing the system clock, please shut down any TES components installed on that machine. If you change the system time while a TES component on that machine is active, you might experience connectivity problems.

Database Issues

Oracle Databases

There are issues that commonly arise when working with Oracle databases.

Error: max open cursors exceeded

If you are using Oracle and you get the message Max open cursors exceeded, you need to increase the open_cursors value from the default (50) to a value of 1000. Contact your Database Administrator to have this value changed in your database initialization file.

Error: lost database connection

If your Oracle database is shut down while the TES master is still running, the TES master will lose its connection to the database without warning. Once you have brought the Oracle database back up, you need to recycle (stop and then start) the master services in order to reestablish the database connection. Failure to recycle the master could result in faulty operation of the client and master.

With TES version 6.2.0, you can deploy a stand-alone TES cache database (MSSQL 2005, 2008, 2012 or Oracle 11gR2), as opposed to using the default embedded cache database (Derby). Having a stand-alone cache database allows for faster synchronization time upon Client Manager startup. Additionally, a stand-alone cache database improves the overall UI experience by offering faster filtering and scrolling response times.

Manually Installing External Database for TES Cache

MSSQL

To switch to an MSSQL database:

Step 1 Locate the *createcachedb-mssql.sql* script. The datafile sizes should match those from the Master database.

Step 2 Edit the script for datafile locations and user password. The default password is "tidalcloud888".

Step 3 Save the script.

Step 4 Execute the script in MSSQL server to create the new database.

Step 5 Locate the plugin *<ClientManagerInstallDir>/config/<cache>.dsp* configuration file. For example, *C:\program files\TIDAL\ClientManager\config\tes-6.2.dsp*.

Step 6 Add the following properties to the *.dsp* file.

CacheDBType=MSSQL

CacheJdbcURL= jdbc:sqlserver://myservername:1433; databaseName=TESCache;SelectMethod=cursor

CacheJdbcDriver= com.microsoft.sqlserver.jdbc.SQLServerDriver

CacheUserName=TES

If a different password was used in Step 2, run the following command in **<ClientManagerInstallDir>/script** to update the password after saving the .dsp file.

cm.cmd setcmpwd <.dsp file name> tidalcloud888 NEWPASSWORD

Step 7 Copy the MSSQL JDBC driver, *sqljdbc4.jar*, into *<ClientManagerInstallDir>/lib*.

Step 8 Restart the Client Manager. The Client Manager's plugin cache database is now switched from the embeded Derby version to the MSSQL version configured here.

Oracle

To switch to an Oracle database:

Step 1 Locate the createcachedb-oracle.sql script in *<ClientManagerInstallDir>/cache/<cache>/cachesql.zip*.

Step 2 Edit the script for datafile locations and user password. The datafile sizes should match those from the Master database. The default password is “tidalcloud888”.

Step 3 Save the script. The user (schema) name must be TES. This cannot be changed.

Step 4 Execute the script as Oracle SYSTEM user (or equivalent).

Step 5 Locate the plugin *<ClientManagerInstallDir>/config/<cache>.dsp* configuration file. For example, *C:\program files\TIDAL\ClientManager\config\tes-6.2.dsp*.

Step 6 Add the following properties to the .dsp file. Enter the actual port number and SID from your environment for the CacheJDBCURL property.

CacheDBType=ORACLE

CacheJdbcURL=jdbc:oracle:thin:@myoracleserver:1521:TES

CacheJdbcDriver=oracle.jdbc.driver.OracleDriver

CacheUserName=TES

If a different password was used in step #2, run the following command in *<ClientManagerInstallDir>/bin* directory to update the password after saving the .dsp file.

./cm setcmpwd <.dsp file name> tidalcloud888 NEWPASSWORD

Step 7 Copy the Oracle JDBC driver, *ojdbc6.jar*, into *<ClientManagerInstallDir>/lib.*

Step 8 Restart the Client Manager. The Client Manager’s plugin cache database is now switched from the embeded Derby version to the ORACLE version configured here.

Note It is recommended you start the Oracle "open_cursors" setting at 2000. Use 3000 for larger systems. To speed up the release of cursors after an operation, the setting "DataCache.StatementCacheSize=1" can be added to the dsp configuration file.

Monitoring TES Java Application Performance

JConsole is recommended for capturing/monitoring any performance related issue. JConsole, a GUI-based software, does not provided a way to capture performance data in a non-interactive way. To capture JMX MBean Attribute values as displayed below, for the purposes of generating alarms when the software exceeds thresholds, use the following command-line alternatives to the JConsole.

- **Jmxterm** (http://wiki.cyclopsgroup.org/jmxterm)
- **cmdline-jmxclient** (http://crawler.archive.org/cmdline-jmxclient)

jmxterm retrieves MBean Attribute values in an interactive shell, whereas **cmdline-jmxclient** retrieves it non-iteractiavely. The syntax of cmdline-jmxclient is as follows:

```
Z:\>java -jar cmdline-jmxclient-0.10.3.jar
Usage: java -jar cmdline-jmxclient.jar USER:PASS HOST:PORT [BEAN] [COMMAND]
Options:
USER:PASS Username and password. Required. If none, pass '-'.
E.g. 'controlRole:secret'
HOST:PORT Hostname and port to connect to. Required. E.g. localhost:8081.
```

List registered beans if only USER:PASS and this argument.

BEANNAME Optional target bean name. If present we list available operations and attributes.

COMMAND Optional operation to run or attribute to fetch. If none supplied, all operations and attributes are listed. Attributes begin with a capital letter: e.g. 'Status' or 'Started'. Operations do not. Operations can take arguments by adding an '=' followed by comma-delimited params. Pass multiple attributes/operations to run more than one per invocation.