Cisco Workload Automation Installation and Configuration Guide

Version 6.3.2

First Published: October 2017

Cisco Systems, Inc. www.cisco.com

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

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

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

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

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

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Preface

This guide describes how to install and configure the basic components of Cisco Workload Automation (CWA).

Audience

This guide is for IT administrators who are responsible for installing and configuring software in the enterprise environment.

Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution: Means *reader be careful.* In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning: IMPORTANT SAFETY INSTRUCTIONS

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Related Documentation

See the *Cisco Workload Automation Documentation Overview* for a list of all CWA 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, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/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.

Document Change History

The table below provides the revision history for the *Cisco Workload Installation and Configuration Guide*.

Version Number	Issue Date	Reason for Change
6.2	May 2014	Updates for 6.2 release.
6.2.1 (SP2)	May 2015	■ New Installation Overview chapter that gives general guidance about TES product components, how they relate to each other and what is required, how to obtain them, installation processes, and general system requirements. ■ Replaced the platform support and minimum requirements with references to the new *TES Product Compatibility Guide* document as the "single source of truth" and the most current updated information. This is available with the TES documentation on cisco.com at: ■ http://www.cisco.com/c/en/us/support/cloud-systems-management/tidal-enterprise-scheduler/products-documentation-roadmaps-list.html ■ New consolidated Licensing chapter. ■ New Versions and Patching chapter for how to apply new service packs and hot fixes. ■ Added MPE/iX Adapter installation and configuration information. ■ Expanded the master.props and service.props documentation. ■ General content validation and editorial improvements throughout.
6.2.1 (SP2)	August 2015	■ Added the JD Edwards Adapter section to the Installing Adapters chapter. Configuring the JDE API prior to startup, debugging, and HTTPS are covered. ■ Added a section in the Installing Client Manager chapter for configuring the index tablespace when using Oracle as the cache database.

Version Number	Issue Date	Reason for Change
6.2.1 (SP3)	January 2016	■ Added a new Configuring the CWA Java Client section for controlling the users and performance of the TES Java Client. ■ Added the Installing a CWA Cache Database section for installing MSSQL and Oracle cache databases. ■ Revised how to obfuscate SSL passwords in a new Obfuscating Passwords for SSL section. ■ Added new properties to Configuring the Master Parameters (master.props). ■ Added Troubleshooting a Unix Agent that Fails to Start. ■ Added Upgrading from Java 7 to Java 8. ■ Moved adapter-specific configuration information to the adapter-specific guide. ■ Miscellaneous bug fixes.
6.3	June 2016	■ Rebranded “Cisco Tidal Enterprise Scheduler (TES)” to “Cisco Workload Automation (CWA)”. ■ Updates to the DataMover Job Support section. ■ Added the new Installing the Hadoop Client Libraries section for DataMover Hadoop support. ■ Added new sections to the Configuring the CWA Java Client to help manage slow Java Clients. ■ Added new configuration parameters to the master.props table in Configuring the Master Parameters (master.props). ■ Updated installation procedures and screenshots. ■ Miscellaneous updates and bug fixes for the 6.3 release.
6.3.1	May 2017	■ SSL protocol is supported between the CWA Java Client and Masters. ■ Miscellaneous bug fixes.
6.3.2	Oct 2017	■ Added support for installation and deployment of CWA components on AWS platform on Virtual Private Cloud (VPC). ■ Added support for enabling workloads to be automated in public and hybrid cloud environments. ■ Added support for integration with key AWS services. ■ Added support for installation and deployment of CWA components on MS Azure platform with launch types – Classic and Resource Manager. ■ Added support for integration with key MS Azure services. ■ Added Kerberos SSO authentication support for web client, Transporter, and CLI in Windows and Linux. ■ Added new configuration parameters to the master.props table in Configuring the Master Parameters (master.props).

Document Change History

1

Installation Overview

This chapter introduces the Cisco Workload Automation (CWA) components and gives you a brief overview of the installation processes and requirements.

The rest of this installation guide provides comprehensive installation details for each component including platform support, procedures, configuration, user definition, upgrading, and security.

See the *Cisco Workload Automation Essential Knowledge Guide* for an overview of how to work with TAC and the basic processes you need to follow to start using CWA.

CWA Components

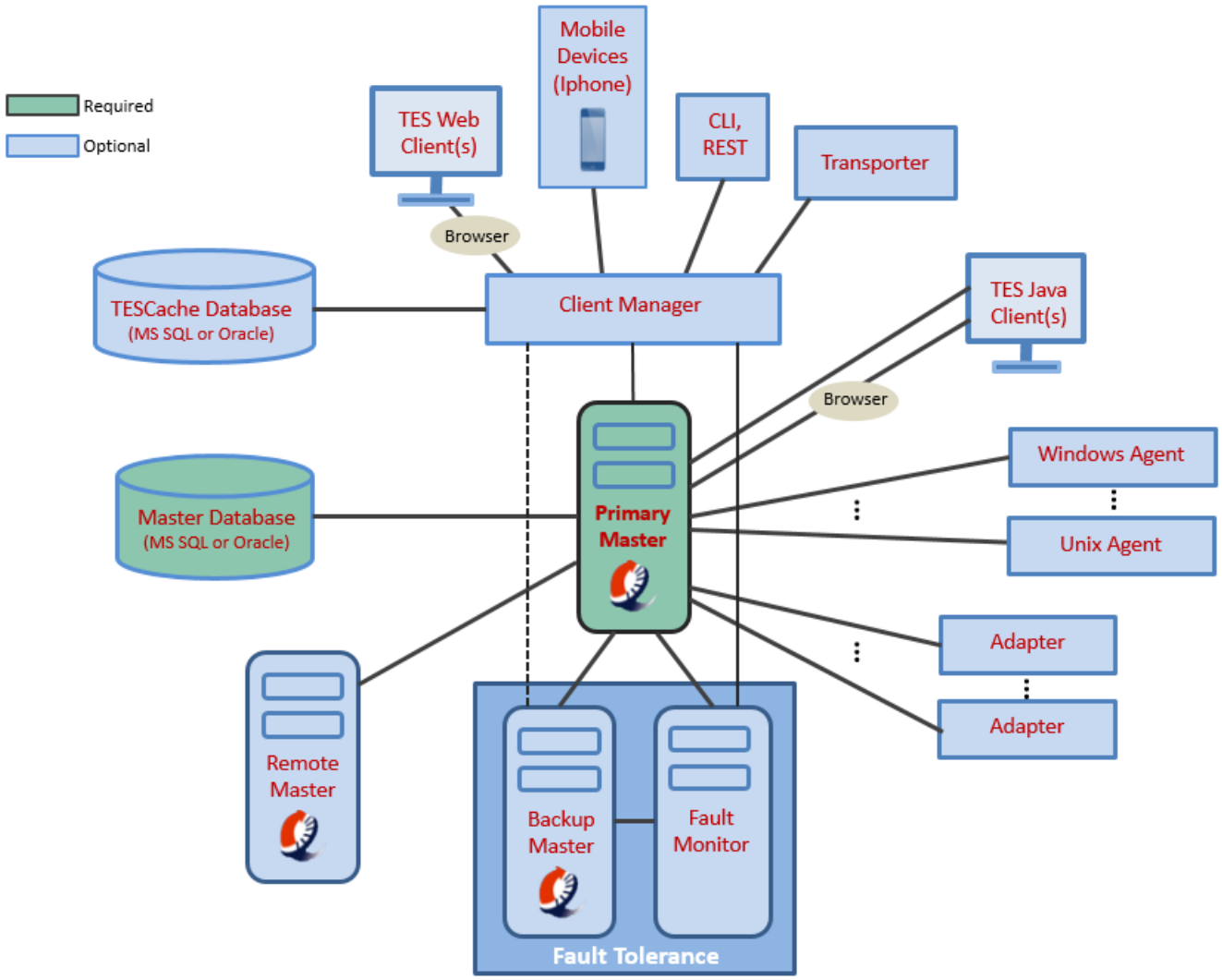
CWA has many different components and provides the flexibility to support many different customer environments. You can tailor your own system to have multiple Masters, multiple agents, additional adapters, install fault tolerance for each Master, and so on.

The diagram below shows the basic CWA system components potentially involved in a system installation. There are two required CWA components:

- Primary Master
- Client Manager OR Java Client

All other CWA components are optional and depend on your environment and job scheduling needs.

Figure 1 Overview of CWA Components



Note: When using Fault Tolerance, the connections between the components can change from what is depicted above. Initially, the connections are as shown. However, when the Backup Master takes over as the Primary Master, the Master Database, Agents, and Adapters connect to the Backup Master. See Installing Fault Tolerance for details.

The sections below define each component. As a minimum requirement, you must install at least one Primary Master and either one Client Manager which supports the CWA Web Client **or** the CWA Java Client as your main interface to CWA. All other components are optional, although many are necessary depending on your environment and needs.

Master Database

The database is where CWA stores the job scheduling objects and metadata. CWA supports Microsoft SQL Server and Oracle (see Database Support for specific versions). Windows platforms can use either Microsoft SQL Server or Oracle; Unix platforms must use Oracle. The database software must be installed on a separate server from the Master server and must be up and running before installing the Master. For installations using an Oracle DB, the 32-bit Oracle client needs to be installed on Master as well. The default Master database name is “Admiral”.

CWA Cache Database

The database where the Client Manager stores the job scheduling objects and cache data. CWA supports Microsoft SQL Server and Oracle (see Database Support for specific versions). Windows platforms can use either Microsoft SQL Server or Oracle; Unix platforms must use Oracle. The database software must be installed on the Master server machine prior to installation of the CWA Master. The default CWA Cache database name is “TESCache”.

Master (or Primary Master)

The Master is the primary CWA component that conducts all scheduling tasks. You can have one or more Masters in your network. The Master can be installed on either the Windows platform or the Unix platform. The basic functionality of CWA remains the same regardless of the platform of the Master.

Each Master computer must supply a unique port number to which Client Managers connect. This port number ensures that communication between the Client Manager and Master is clear.

Client Manager

The Client Manager allows the Master to achieve higher performance and scalability. The purpose of the Client Manager is to service requests from user initiated activities, such as through the CWA Web Client, CWA Transporter and from other external sources that utilize the Command Line Interface (CLI) or published CWA Web services. The Client Manager allows the 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. The Client Manager constantly syncs the information from the Master database into its own TESCache database that it then uses to provide all CWA Web Client users with current information. Multiple Client Managers connected to the same Master can be deployed to address additional performance needs.

The Client Manager is required if you want to use the CWA Web Client, the Transporter, the Command Line Interface (CLI), REST, or mobile applications. The Client Manager is not required if you are only using the Java Client.

CWA Web Client

The CWA Web Client is the main user interface for managing CWA jobs, scheduling, connections, configuration, and so on. The CWA Web Client connects to the Client Manager using a browser.

You can use both the CWA Web Client and the CWA Java Client with the same Master.

CWA Java Client

The CWA Java Client is a standalone application that provides the same user interface as the CWA Web Client to manage CWA jobs, scheduling, connections, configuration, and so on. However, the Java Client connects directly to the CWA Master and not through the Client Manager. You can run the Java Client as an application, or you can launch it using a browser.

The CWA Java Client is typically more responsive than the CWA Web Client because it is connected directly to the Master. However, this increases the RAM used by the Master process as the Master is now doing the work instead offloading it to the Client Manager.

You can use both the CWA Java Client and the CWA Web Client with the same Master. Note that an environment exclusively using the CWA Java Client will not be able to utilize features that require the Client Manager like the Transporter, Command Line Interface, and the WebService API.

Mobile Devices

CWA supports accessing the Master and scheduling data using a mobile IOS device. You must install the Cisco Workload Automation application on your device that you obtain from the Apple store.

Command Line Interface (CLI)

The Command Line Interface program provides access to CWA using the *sacmd.cmd* (Windows) or *sacmd.sh* (Unix/Linux) program through the MS-DOS command prompt or Unix command utility. You can do things like automate CWA job control functions by including commands in scripts or by embedding job control functions in the code running your company processes. The command line program can also be used from the CWA Web Client.

The Command Line Interface program is fully documented, including installation, in the *Cisco Workload Automation Command Line Program Guide.*

Agents

An agent is a separate installation of CWA that runs jobs on behalf of the Master. Agents help you to automate the execution of jobs that you know need to be performed on a regular basis, Offloading jobs to agents frees the Master for intensive scheduling tasks such as production compiles. Agents exist for various platforms. For the current list of the types of agents available for CWA, see Platform Support for Agents. The Windows Agent and the Unix Agent are the two most commonly used agents.

Each agent can connect to a Master by specifying the Master-to-agent communication port and the Master-to-agent file transfer port numbers.

Adapters

CWA provides adapters for many software products to enable connectivity to and access by CWA. The Master has an Adapter Host it uses to manage the adapters and is the interface that the adapters use to connect to the Master. Adapters are provided with the base CWA installation but must be licensed and configured. For a list of the adapters provided for CWA, see Supported Adapters.

Backup Master

The Backup Master is used in a fault tolerance configuration. Fault tolerance requires one Backup Master for each Primary Master. The Backup Master operates exactly like the Primary Master, but is activated only if the Primary Master experiences a system, network or machine failure. The Backup Master must run on the same platform and version of software used by the Primary Master. The hardware specifications of the backup machine should be equal or greater than the specifications for the primary machine.

The Backup Master must specify the Backup-to-Master port number for transferring scheduling data from the Primary Master to keep the Masters synchronized.

Fault Monitor

The Fault Monitor is part of the CWA fault tolerance configuration. The Fault Monitor continually monitors a Primary Master and Backup Master for error conditions. If a failure indicator appears on the Primary Master, the Fault Monitor transfers control to the Backup Master. The Fault Monitor must be installed on a separate machine independent from the primary and backup machines.

Remote Master

A Remote Master is simply an additional CWA Master that is installed in a different environment. The Remote Master allows a connection to another CWA Master for sharing global CWA variables between CWA environments. Variables definitions must have “Publish value to remote masters” selected in the CWA environment where they reside prior to being available through a remote master connection.

Transporter

The Cisco Workload Automation Transporter application transports scheduling objects from one CWA instance (source) to another CWA instance (destination). For example, you can use the Transporter to promote jobs from a test instance to a production instance. The primary strength of Cisco Workload Automation Transporter is its ability to automate the copying of job data, although it can copy other data types as well.

Beginning with CWA 6.3, the Transporter can also export jobs as XML files and import the jobs back from XML files.

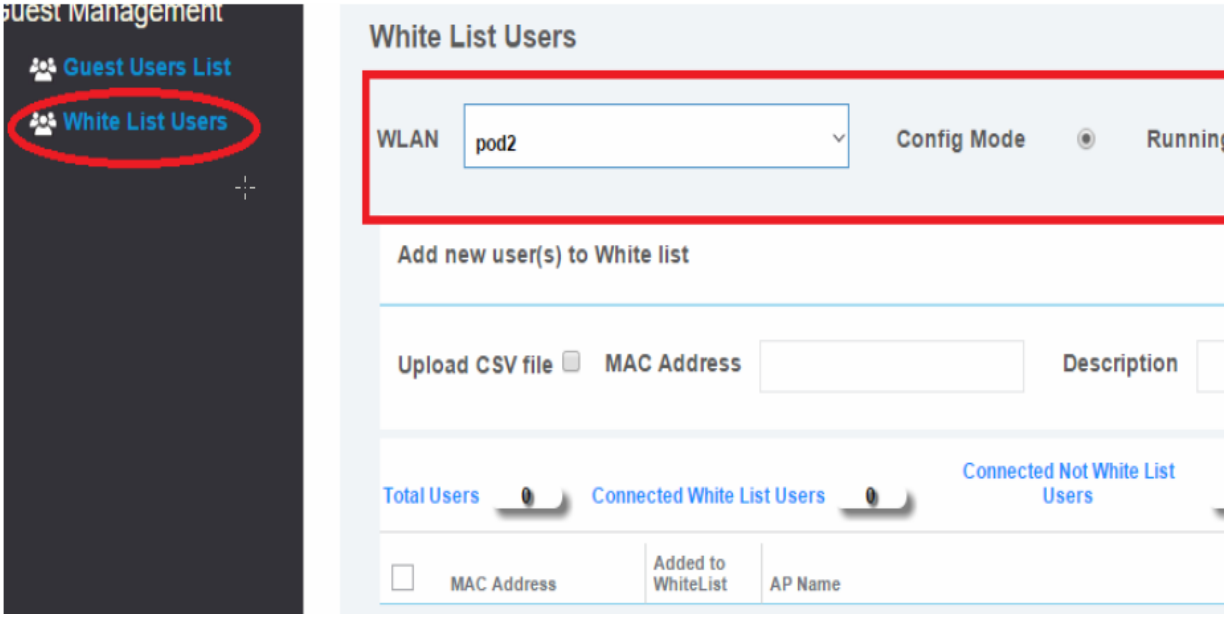
All features of the Transporter are fully documented, including installation, in the *Cisco Workload Automation Transporter User Guide.*

Network Configuration

CWA can be configured on a network in many different ways. You can connect any number of licensed Masters using any number of licensed agents, each located anywhere on your network.

An example of the network connections for a basic system are shown below. Static port numbers are shown; no port number means the port is dynamically assigned.

Figure 2 Basic CWA Component Connections



Fault Tolerance Configuration

Fault tolerance can be added to a CWA network to provide an extra degree of scheduling reliability. In a fault tolerant environment, each Primary Master is connected to a dedicated Backup Master and a Fault Monitor machine.

In this setup, the Primary Master periodically shares data with the Backup Master during normal operation. Only one Master (normally the Primary Master) has control of scheduling at any time. If the Primary Master has a network, power, or software failure, control is transferred to the Backup Master.

See Installing Fault Tolerance for more information.

Installation Processes

This section describes the download prerequisites, how to obtain the software, an overview of how to install a new Cisco Workload Automation system, and an overview of how to upgrade an existing installation.

It also describes how to obtain the CWA documentation on cisco.com.

Download Prerequisites

To download the Cisco Workload Automation software, you must be able to log into cisco.com and have a valid service contract associated to your Cisco.com profile. If you do not have a service contract you can get one through:

- Your Cisco Account Team if you have a direct purchase agreement with Cisco.
- Your Cisco Partner or Reseller

Once you have the service contract you must associate your service contract to your Cisco.com user ID with Profile Manager.

Obtaining the Software

All Cisco Workload Automation installation software is available from on cisco.com web site. Most CWA components are bundled in one download package. However, you must license some components separately before you can use them as shown in the following table. Some components also have service packs and hot fixes.

Software Package	Contains...	Platforms	Requires License?
Cisco Workload Automation Base Product	Master	Windows and Unix	Y
	Client Manager	Windows and Unix	N
	Java Client	Windows and Unix	N
	Backup Master	Must match the Primary Master	N
	Fault Monitor	Windows and Unix	Y
	Transporter	Windows and Unix	N
	Adapters	Installed with the Master **Note:** Additional configuration is required for some adapters (see Installing Adapters)	Y **Note:** All adapters require separate licenses <*except*> Email and SSH. See your Cisco sales rep.
	Command Line Interface	Installed with the Master	Y

Software Package	Contains...	Platforms	Requires License?
Cisco Workload Automation Agent for Windows	Windows Agent	Windows	Y
Cisco Workload Automation Agent for Unix	Unix Agent	Unix	Y
Service Pack 2	6.2.1.x	Windows and Unix	N
Hotfix	Latest hotfixes which are cumulative for the release.	Windows and Unix	N

Downloading the CWA Software

The CWA software is available on cisco.com. Most CWA products are provided in the CWA Base Product bundle. The CWA Agent software is provided as separate installation packages. As new features and improvements are made to the CWA products, service packs and hotfixes are also made available. You must first obtain the CWA Base Product package and the Agent software, then apply the latest service pack and hotfixes. These procedures are described below.

CWA Base Product Software

To obtain the CWA base product software:

1. In your browser, navigate to the Cisco software download site at:

   http://software.cisco.com/download/

2. In the Find search box, enter **Cisco Workload Automation**, then click the link.
3. For software type, click **Cisco Workload Automation (CWA) Product Install**.
4. In the Navigation pane on the left, choose **6.3.2** (or the version you need).
5. Click **Download** and extract the zip file to a temp directory on a machine where your CWA system can access it.
6. See Installing a New CWA System, page 8 for guidance on the order to install CWA components.

Agent Software

Software for the supported agents is bundled with the CWA base software package. However, we recommend that you download the individually provided agent software packages as described in this section.

To obtain the Agent software:

1. In your browser, navigate to the Cisco software download site at:

   http://software.cisco.com/download/

2. In the Find search box, enter **Cisco Workload Automation**, then click the link.
3. In the right pane, click one of these:

- **Agent for Windows**
- **Agent for Unix**
- Agent for OVMS

4. Under Select a Software Type, click **Cisco Workload Automation (CWA) Product Install**.

5. In the Navigation pane on the left, choose the latest version.

   Note: Every agent version works with any CWA version.

6. Click **Download** and extract the zip file to a temp directory on a machine where your CWA system can access it.

See Installing a New CWA System, page 8 for guidance on the order to install CWA components.

See Installing Agents for information about how to install agents.

Service Pack and Hotfix Software

To obtain the latest CWA Service Pack and Hotfix software:

1. Backup your CWA system.
2. Stop all CWA software.
3. In your browser, navigate to the Cisco software download site at:

   http://software.cisco.com/download

4. In the Find search box, enter **Cisco Workload Automation 6.3.2**, then click the link.
5. In the Navigation pane on the left, choose **6.3.x** or the version you need.
6. Apply the Service Pack updates if there are any:
   a. Next to the CWA 6.3.x SP<x> Release, click **Download.**
   b. **Extract** the zip file to a temp directory on a machine where your CWA system can access it.
   c. Locate and read the **readme.txt** file in the Service Pack files you just extracted and follow the instructions in it.
7. Apply the Hotfix updates if there are any:
   a. Next to the CWA 6.3.x SP<x> Hotfix bundle release (if one exists), click **Download.**
   b. **Extract** the zip file to a temp directory on a machine where your CWA system can access it.
   c. Locate and read the **readme.txt** file in the Hotfix files you just extracted and follow the instructions in it.

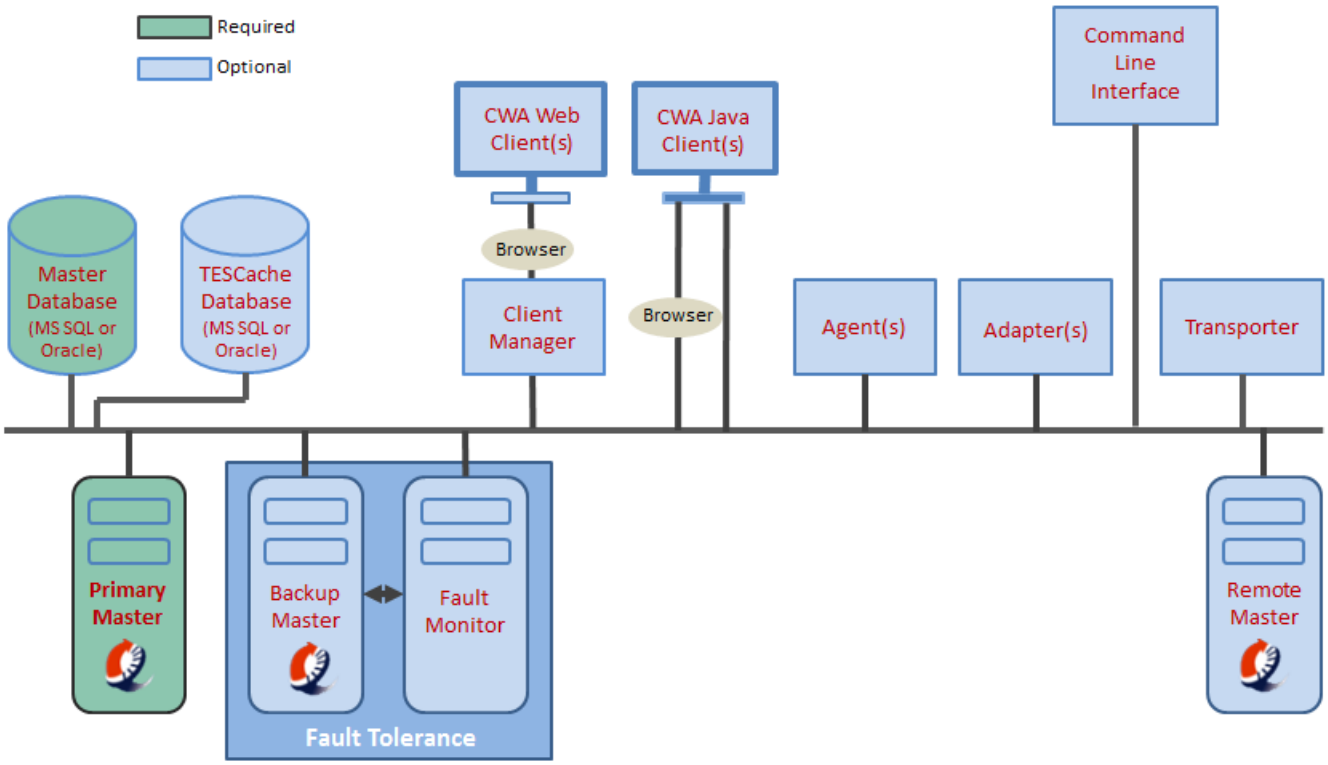
Installing a New CWA System

The CWA components you install for a new CWA system is flexible and based on your environment and needs. The illustration below shows the order of component installation for a basic system.

Note: Only the Master database and the Primary Master are required, in addition to either the Client Manager or the Java Client. All other components are optional. Also note that you can add the optional components at any time.

Be sure to read the General Installation Requirements, page 10 in this chapter, and review the information in the Installation Prerequisites chapter prior to starting the installation.

Figure 3 Basic CWA Component Order of Installation



CWA Component Installation Checklist

1. Install the Master. See the chapter for your platform:

   Installing the CWA Master for Windows, page 35

   Installing the CWA Master for Unix, page 51

2. If you are using Fault Tolerance, install the Backup Master and the Fault Monitor. See:

   Installing Fault Tolerance, page 101

3. Install at least one of these components:

   – The Client Manager. See:

   Installing the Client Manager, page 63

   – The CWA Java Client. See:

   Installing a CWA Java Client, page 91

4. Optionally, install one or more Agents. See:

   Installing Agents, page 119

5. Optionally, install one or more Adapters. See:

   Installing Adapters, page 155

6. Optionally, install the Command Line Interface Program. See the *Cisco Workload Automation Command Line Program Guide*.
7. Optionally, install the Transporter. See the *Cisco Workload Automation Transporter User Guide*.

Configuration Steps

8. Configure the CWA system. See:

   Basic CWA Configuration, page 167

9. Define users. See:

   Defining Users, page 177

10. License the components.

    CWA Licensing, page 163

Upgrading an Existing CWA (TES) System

If you're upgrading your release with a new service pack or hotfixes, see Versions, page 161.

If you're upgrading from one major release to another, see the Upgrading Components, page 191.

Obtaining the Documentation

You can see what documentation is available and download PDFs for the CWA software.

To obtain documentation for your CWA software:

1. In your browser, navigate to the Cisco Workload Automation Documentation Overview at:

   http://www.cisco.com/c/en/us/support/analytics-automation-software/workload-automation-6-3/model.html

General Installation Requirements

Prior to installation, follow these steps to meet the general installation requirements for CWA:

- Determine which components you are going to install and where you are going to install them before you install CWA. Because the InstallShield Wizard/CWA 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 CWA can communicate with the other machines on the network. If you cannot ping to and from each component machine, CWA cannot function properly. Network conditions affect the operation of CWA.
- Make sure that a supported database is installed on your machine. See Database Support, page 14 for what is supported.
- Make sure that you can log on with an account that has Administrator privileges.
- Download the latest set of service pack and hotfixes for Cisco Workload Automation from cisco.com.
- Review any supplementary documentation provided with your software such as the Release Notes or readme.txt file. Last-minute instructions might be contained in these documents.

- If you are upgrading CWA(Cisco Workload Automation), install the program in the same directory in which the previous version was installed to keep your data intact. See Upgrading Components, page 191 for information about upgrading.
- Exit all Windows programs before running any installation.
- Contact Cisco Support if you have any questions.

2

Installation Prerequisites

This chapter provides details about the minimum system requirements, database support, and user security requirements for the Cisco Workload Automation (CWA) version 6.3.2.

CWA System Requirements

CWA Compatibility Guide

You can find the most current and complete platform compatibility and requirements information for current CWA versions in the *Cisco Workload Automation Product Compatibility Guide.* The platform requirements are provided for these CWA components:

- CWA Master
- Client Manager
- Fault Monitor
- Agent
- CWA Java Client
- CWA Web Client
- Databases
- Browser
- Adapter
- Transporter

You can download this document from Cisco.com at:

http://www.cisco.com/c/en/us/support/analytics-automation-software/workload-automation-6-3/model.html

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 32-bit Oracle client software (the same client version as your database version) in order to connect to the Oracle database. After installing, the Master does not require the 32-bit client software to run.

Database Support

Before installing CWA you should already have database software installed. The Master and Client Manager support the following databases:

- Microsoft SQL Server
- Oracle

Windows platforms can use either Microsoft SQL Server or Oracle; Unix can only use Oracle.

See the *Cisco Workload Automation Product Compatibility Guide* for specific supported versions which is provided with the CWA documentation on cisco.com at:

http://www.cisco.com/c/en/us/support/analytics-automation-software/workload-automation-6-3/model.html

Note: CWA 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

Supported Database Configurations

The following DB configurations are supported:

Master on UNIX	Oracle DB on UNIX
Master on Windows	Oracle DB on UNIX Microsoft SQL Server on Windows Oracle on Windows

Microsoft SQL Server Database Requirements

Microsoft SQL (MSSQL) Server users should verify the following items before installing CWA:

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

If you are installing a CWA Master, MSSQL 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

Here are the requirements for using an Oracle database with CWA:

- The Master uses only JDBC to connect to any Oracle-related database. CWA requires that the OLE providers for the Oracle 10g and 11gR2 database be installed on each CWA machine. These OLE providers are normally installed only during a full Oracle client install (also known as Oracle Admin Client). Have your Oracle administrator install these drivers on each machine that will run CWA. 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 needs to know the Oracle tablespace datafiles to be used with CWA. The following three Oracle tablespace data files are created by CWA 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 CWA 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 CWA Master. Verify that the Oracle bin folder is in your system path before installing CWA.
- Because CWA 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.
- If you are using Oracle 12c as your CWA database, you must add these lines to the sqlnet.ora file:

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

Browser Compatibility

Generally, CWA supports Internet Explorer and Firefox. See the *CWA Product Compatibility Guide* for specific supported versions which is provided with the CWA documentation on cisco.com at:

http://www.cisco.com/c/en/us/support/analytics-automation-software/workload-automation-6-3/model.html

Note: Safari is not supported.

Ports Used by CWA

CWA uses the following ports which must be available for successful operation.

- Master listens on...
  - 5591 - Agents - Master connection definition in Client
  - 6215 - Client Manager
  - 6702 - Clients - Master connection definition, and Client shortcut
  - 6704 - Backup Master, or Primary Master (if it is backup)
  - 6980 - Adapter Host (5.3.1)
  - 8080 - Web server to facilitate Web launch of Java Client
- Agents listen on

  - 5912 (default) – for Master initiation connections
- Client Manager listens on...
  - 8080 – CWA Web Client
- Fault Monitor listens on...
  - 6703 – Master (Primary Master and Backup Master) – master.props
  - 6705 – Client
- Adapter Host listens on...
  - 6950 – Master (5.3.1)

The other side of all ports is randomly assigned.

User Security Requirements

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

CWA Component	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
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
Java Client	■ Local Administrator	N/A	General user rights

Permissions after Installation

- The installation of CWA requires the 'tidal' account to be sysadmin for the database creation. For normal operation, the product uses select, update, insert, and delete statements on the user tables present in the CWA data schema. During product upgrades, CWA needs DBO privileges to perform the structural changes to the CWA schema.

  The product has been tested and verified with the 'tidal' user having DBO privileges as testing and regression testing involves upgrading from prior versions of the product as part of our verification process.

  If a customer chooses to run with altered privileges, they must be aware that this customization has not been tested. If a support issue arises, the customer will be asked to revert to the supported/tested configuration to obtain formal support from Cisco.

- The schema for the Client Manager TESCache database requires DBO only account permissions for day-today-operations and any install/upgrades require sysadmin kind of privileges similar to the Master database.

Database Access

- If you are planning to use an Oracle or Microsoft SQL database, your database administrator will be required during installation of the Client Manager 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.

Installation

- The Client Manager and agent should be installed under the same user name with equivalent capabilities.

Unix-Specific Considerations

- When installing CWA Agent for Unix, you must be able to log in as root.
- The CWA 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.

Windows-Specific Considerations

- 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, page 207 in the *Troubleshooting* chapter.

LDAP Considerations

- LDAP users can be imported into CWA 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 has three distinct entries for adding users, “Interactive Users”, “Runtime Users” and “LDAP Groups”. CWA 6.x allows for the setup of a user that authenticates against Active Directory/LDAP. CWA also supports AD/LDAP only users.
- At login, user credentials are validated against Active Directory/LDAP. Once authenticated, CWA obtains the users AD/LDAP groups and other information such and phone number and email.

- Once login has completed, a record is established in CWA 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 CWA. 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.
- CWA LDAP groups are supported by the creation of groups within the CWA application.

Security Policies

- Security policies can be defined and specialized by application administrators.
- Each group within CWA can be assigned one security policy.

Caution: The security capabilities of a user are based upon the cumulative 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 CWA not imported from AD/LDAP.

Workgroups and Security Policies

- Workgroups are also available within the CWA 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).

3

Installing the CWA Master for Windows

CWA can be configured on a network in many different ways. The CWA Master is installed with default parameters that provide most users with optimum performance, but environment circumstances might 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, page 43 for information on modifying the main Master properties.

This chapter covers:

Installation Prerequisites

The following requirements must be met for successful installation of the CWA Master:

- User with local Administrator privileges
- One of the Windows operating systems listed in CWA System Requirements, page 13.
- 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 Database Support, page 14 for further information.)
- Apply all patches supplied in the latest hotfix.
- If the MSSQL DB server is **Azure SQL database**, install the Microsoft SQL Server Native Client 11.0 in the Master installation environment.
- 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:

1. Right click **My Computer**, and choose **Properties**.
2. Click the **Advanced system settings** link in the left pane. The System Properties dialog box displays.
3. Click **Environment Variables**, and select the path to edit in the Environment Variables dialog box.
4. Click **Edit** and provide the complete Java path, down to the bin directory.

Note: During Java 8 installation, the following path is added to the system path by default:

```
C:\ProgramData\Oracle\Java\javapath
```

This path must be removed to have multiple Java versions installed on the master machine. If this path is not removed the Adapter host fails to start and throws the following error:

```
Adapter host fails to start the service having incorrect JRE in registry.
```

Installing the Windows Master

The installation procedure for installing the Windows Master differs depending upon whether the database being used is Microsoft SQL Server or Oracle. Both procedures are documented:

- Using a Microsoft SQL Database, page 36
- Using an Oracle Database, page 41

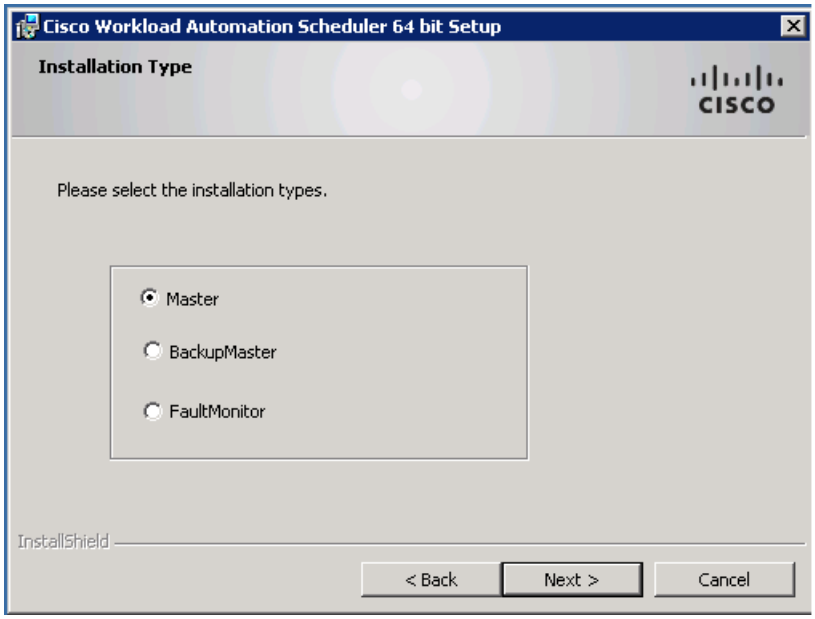
Using a Microsoft SQL Database

To install the Master component using a Microsoft SQL database:

1. Obtain the Cisco Workload Automation Base Product software for your environment from cisco.com. See Obtaining the Software, page 6.
2. Extract the files onto the target machine.
3. Navigate to the **\Scheduler\<your platform>** directory.
4. Run *setup.exe*.
5. On the **Internet Explorer Security Warning** dialog box, click **Run**.
6. On the **Welcome** panel, click **Next**.

   The CWA installer displays the **Installation Type** panel:

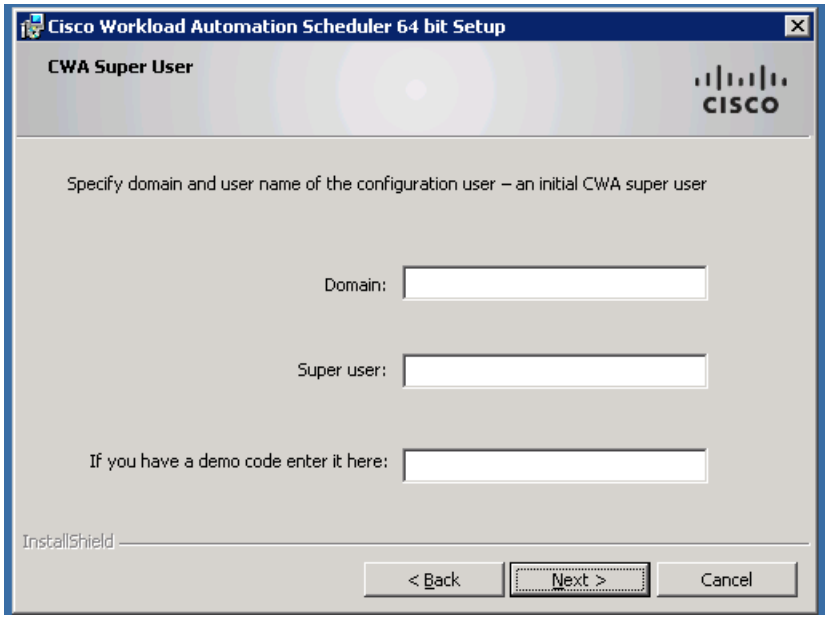
Figure 1 Installation Type Panel



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

   The CWA installer displays the **CWA Super User** panel:

Figure 2 CWA Super User Panel



8. On the **CWA Super User** panel, enter the following, then click **Next**.
   - **Domain**–Enter the domain name for your Master into the Domain field.
   - **Super user**–Enter the name of the Super user for this Master.

- **If you have a demo code enter it here**—Enter the code into the field.

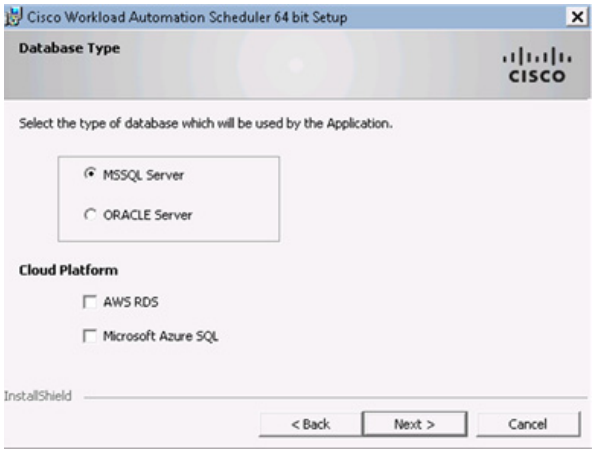
9. On the **Destination Folder** panel, select the directory where the CWA files will reside, then click **Next**.
   - Accept the default location at **C:\Program Files\TIDAL**.

   -or-

   - Click **Change**, locate a directory, select the appropriate file and click **Save**.
10. On the **Database Type** panel, select **MSSQL Server**. The **AWS RDS** option and **Microsoft Azure SQL** option are displayed.

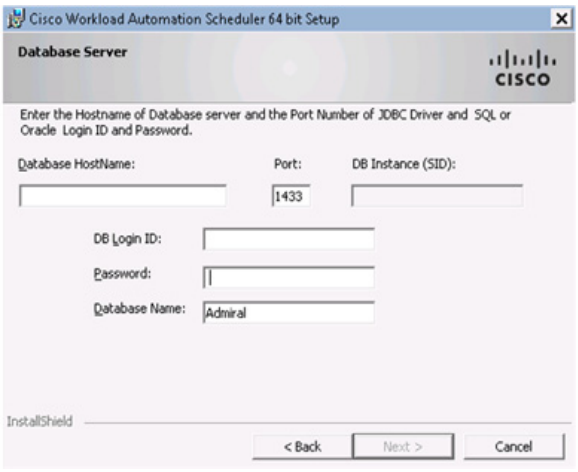
    Note: To install an Oracle database, follow the instructions in Using an Oracle Database, page 41.

Figure 3 Database Type Panel



11. Click **Next**. The CWA installer displays the **Database Server** panel.

Figure 4 Database Server Panel



12. On the **Database Server** panel, enter these values:
    - **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 for MSSQL is 1433.
- **DB Instance (SID)**–Ignore for MSSQL (Oracle only).
- **DB Login ID**–Enter the login credentials for the database administrator.
- **Password**–Enter the password for the database administrator.
- **Database Name**–Enter the database name (MSSQL only). By default, the database name is **Admiral**.

13. Click **Next**. The **Active Directory/LDAP Authentication** panel displays.
14. Select the authentication type, 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.
15. For Active Directory, enter the following information:

    - **Host–** Enter the hostname or IP address for the Active Directory server.
    - **Port–**Enter the port number for the AD 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.

    Example of an AD Setting

    ```
    Security.Authentication=ActiveDirectory
    ActiveDirectory.Host=<ip address or your_hostname>
    ActiveDirectory.Port=389
    ActiveDirectory.UserSearchPrefix=DC=example,DC=com
    ActiveDirectory.GroupSearchPrefix=DC=example,DC-com
    ```

    -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 CWA Web Client user authentication is defined to use Oracle/Sun Directory Server with role-based access.
    - **Index–** Check this option if you have an index.
    - **GroupBindDN–** Enter the group account to query the LDAP server.

Note: If you want to authenticate users across multiple domains rather than installing the Master in each domain, follow the instructions in Enabling Multi-Domain Authentication, page 44

Example of an LDAP Setting

```
Security.Authentication=LDAP
LDAP.HostName=<ip_address or hostname>
LDAP.Port=389
LDAP.BindDN=ou=people,dc=example,dc=com
LDAP.UserObjectClass=inetOrgPerson
LDAP.UserBindDN=dc=example,dc=com
LDAP.GroupBindDN=dc=example,dc=com
```

16. On the **Ready to Install the Program** panel, click **Install** to start the installation process. The **Installing Cisco Workload Automation - Master** panel displays.

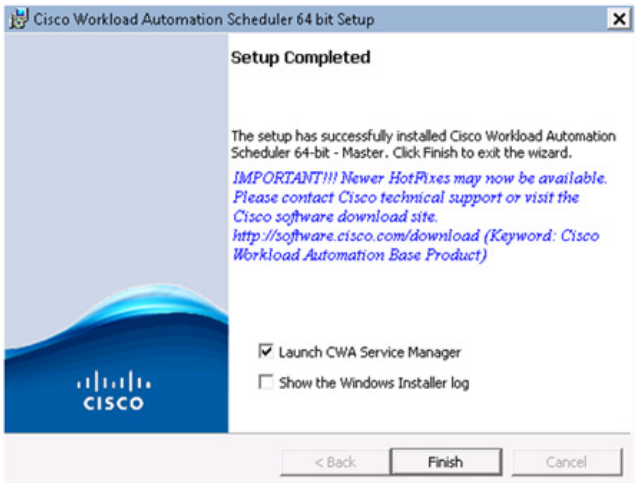
    The progress of your Master installation is displayed in the form of a progress bar.

    Regulatory: Do not click Cancel once the installation process begins copying files in the Setup Status panel. Canceling 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.

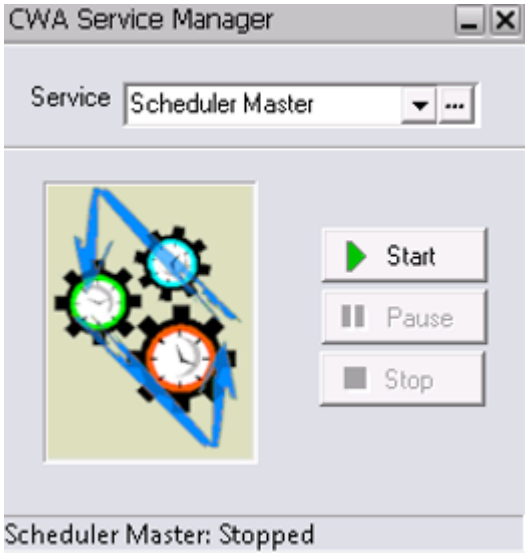
17. On the **Setup Completed** panel, select **Launch CWA Service Manager** and then click **Finish**. The **CWA Service Manager** window is displayed.

Figure 5 Setup Completed Panel



18. On the **CWA Service Manger** window, click **Start** to run the scheduler master.

Figure 6 CWA Service Manager



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:

1. Download the Cisco Workload Automation Base Product software for your environment from cisco.com.
2. Extract the files onto the target machine.
3. Navigate to the **\Scheduler\<your platform>** directory.
4. Run *setup.exe*.
5. On the **File Download Security Warning** panel, click **Run**.
6. On the **Internet Explorer-Security Warning** panel, click **Run**.
7. On the **Welcome** panel, click **Next**.
8. On the **Installation Type** panel, select **Master**, then click **Next**.
9. On the **CWA 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.
10. On the **Destination Folder** panel, select the directory where the CWA 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*.

11. On the **Database Type** panel, select **ORACLE Server**. Then, click **Next**.

    Note: If **Oracle Server** is selected, the **Microsoft Azure SQ**L option is not visible.

12. 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 for Oracle is 1521.
    - **DB Instance (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.

    Note: This information is available from the Oracle Database Administrator.

13. On the **Oracle Tablespace Datafiles** panel, specify the name and location of the Data, Index and Temp tablespaces so CWA can access the files, then click **Next**. By default, CWA 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.

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

    The **Installing CWA - Master** panel is displayed.

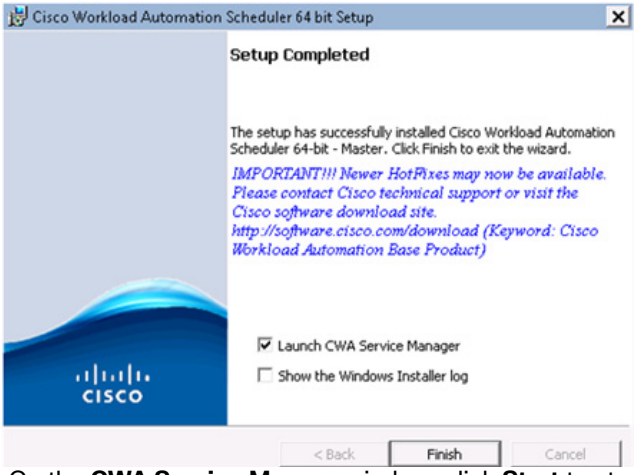
    The progress of your Master installation is displayed in the form of a progress bar.

    Regulatory: 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.

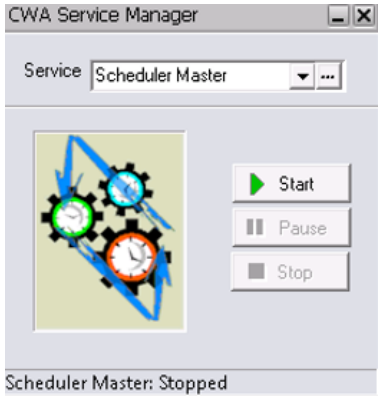
15. On the **Setup Completed** panel, select **Launch CWA Service Manager** and then click **Finish**. The **CWA Service Manager** window is displayed

Figure 7 Setup Completed Panel.



16. On the **CWA Service Manger** window, click **Start** to start the scheduler master.

Figure 8 CWA Service Manager



Verifying Master Connection

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

To verify the Master connection:

1. From the Windows Start menu on the Master machine, select **All Programs > Cisco Workload Automation > Scheduler > Service Control Manager** to display the CWA Service Manager.
2. From the Service list, select **Scheduler Master**. The Master status displays at the bottom of the dialog box.
3. Click **Start** to start the Master if it is not running.

Configuring the Master

This section covers these topics:

See Basic CWA Configuration, page 167 for more information about configuring your CWA system and the master.props file.

Configuring the Master for SNMP

If you want to use Simple Network Management Protocol (SNMP) to send traps in CWA, 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:

1. Stop the Master using the CWA Service Manager.
   a. From the Start menu on the Master machine, choose **Programs > Cisco Workload Automation > CWA Service Manager** to display the CWA 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”.)

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

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

   snmphost=<hostname of the SNMP server>

   snmpport=<port number used by the SNMP server>

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

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

6. Restart the Master from the CWA Service Manager.

Configuring the Nice Value for the Master Service

Usually the CWA 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 CWA 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.

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

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

For example, a CWA 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:

1. Log on the Master machine.

2. Navigate to the Master installation directory inside cmd.exe.

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
```

Enabling Multi-Domain Authentication

CWA allows for multiple-domain user authentication for the CWA Master. The purpose of this function is to allow users defined in different domains to be authenticated within one Master configuration to avoid installing one Master per domain.

To enable this multi-domain authentication:

1. Add the following new property value in *master.props*, located under *<MASTER_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 CWA user authentication.

This example defines two servers:

```
<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 example above, the authentication process will validate **TIDALSOFT** first and then **ITTIDAL**.

Installing an Oracle Database

See Using an Oracle Database, page 41 for Oracle database installation requirements.

Adding an Oracle Service as a Master Dependency

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

To add the Oracle service as a CWA Master dependency:

1. Log in as an **Administrator**.
2. From the Windows Start menu, choose **All Programs > Cisco Workload Automation > Scheduler > Service Control Manager > Scheduler Master**.
3. Stop the Master by clicking **Stop**.
4. Click **Configure**, then click **Dependencies**.
5. Select the service **OracleService <service name>** from the **Available Services** list and drag it to the Depends On tab.

6. Click **OK**, then click **OK** again.
7. Click **Start**.

The next time you reboot, the CWA 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 CWA 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 CWA 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 the Oracle database manually:

1. Open the Oracle SQL*Plus program.
2. Login as the SYSTEM user (or equivalent) and connect to the ADMIRAL TNS Name.
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.
4. Edit *orapopulate.sql* so it will create a valid initial super user account.
5. 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 CWA 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 CWA Master:

1. Stop all CWA components.
2. Exit all CWA Web Clients by choosing **File > Exit** from the menu for each CWA Web Client that is running.
3. Stop the Master:
   a. From the Windows Start menu, choose **Programs > Cisco Workload Automation > CWA Service Manager.**
   b. From the Service list, choose **Scheduler Master**.
   c. Click **Stop**; the light turns green when the Master has stopped.

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

Uninstallation Procedure

The CWA Master is uninstalled from the Windows Control Panel.

To uninstall the CWA Master:

1. From the Windows Start menu, choose **Control Panel**, then double-click **Add** or **Remove Programs**.
2. Scroll down the list of programs installed on the machine to the Cisco Workload Automation program.
3. Click the **Cisco Workload Automation <platform> - Master** program to highlight it.
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.
5. Click **OK** to uninstall. The Preparing Setup panel displays showing a progress bar. When the progress bar reaches 100%, a CWA 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.

   Regulatory: 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.
6. Click **OK** to finish.
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.
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 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.

Prerequisites for Master Installation with Restored Azure SQL Database

Once the Master MSSQL database is successfully restored to Azure SQL database, the database user is orphaned. To resolve this user issue, we need to follow the below steps:

Master DB connection execution

1. Execute the below query, if login “tidal” is not available.

```
CREATE LOGIN tidal WITH PASSWORD = 'Control@1234';
```

2. Execute the below query, if the login “tidal” exists.

```
Alter LOGIN tidal WITH PASSWORD = 'Control@1234';
```

3. Execute the below query, if the user account is not found in the system database.

```
CREATE USER tidal FOR LOGIN tidal WITH DEFAULT_SCHEMA = dbo;
```

4. Execute the following query:

```
ALTER ROLE loginmanager ADD MEMBER tidal;
```

User-created DB connection execution

1. Execute the below query to delete the user “tidal”, if the “tidal” user exists in the Admiral database.

```
DROP user [tidal];
```

2. Finally, execute the below queries:

```
CREATE USER tidal FOR LOGIN tidal WITH DEFAULT_SCHEMA = dbo;
exec sp_addrolemember 'db_owner', 'tidal';
ALTER DATABASE Admiral SET ANSI_NULL_DEFAULT ON;
```

Prerequisites for Master Installation with Restored AWS RDS MS SQL Database

It is assumed that Master is installed with the Database Admiral and User Tidal. Once the Master MSSQL database is successfully restored to AWS RDS MS SQL database, follow the below steps:

1. Execute the following query:

```
use Admiral
go
```

2. Execute the below query only if login ‘Tidal’ is not available:

```
CREATE LOGIN tidal WITH PASSWORD = 'tidal97', CHECK_POLICY = OFF
```

3. Execute the below query, only if the user ‘Tidal’ is not available in the Admiral database:

```
CREATE USER tidal FOR LOGIN tidal WITH DEFAULT_SCHEMA = dbo
go
```

4. Execute the below queries:

```
exec sp_defaultdb  @loginame='tidal', @defdb='Admiral'
go

exec sp_addrolemember 'db_owner', 'tidal'
go

exec sp_addsrvrolemember 'tidal', 'setupadmin'
go

exec sp_addsrvrolemember 'tidal', 'processadmin'
go
```

4

Installing the CWA Master for Unix

You can run CWA on Unix by installing the Unix versions of the Master software. The current Unix version of the CWA Master only works with an Oracle database.

Note that there are two methods to install the Unix version of the CWA Master:

- Installation Program (see Installing the Unix Master, page 52.)
- Manually – From the command line as described in Installing the Unix Master from the Command Line, page 55. 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, page 43 for information on modifying the main Master properties.

This chapter covers:

Installation Prerequisites

The following requirements must be met prior to installing the Unix Master:

- One of the Unix operating systems and corresponding JVM as listed in CWA System Requirements, page 13.
- 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 GB of RAM (The use of any CWA adapters requires an additional 1 GB.) and dual 500 MHz processors dedicated to CWA 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 CWA 6.3.2.

Note: Only one Master can be installed on a machine. CWA cannot operate correctly if two Masters are installed on the same machine.

Installing the Unix Master

To install the Unix Master:

1. Download the Cisco Workload Automation Base Product software for your environment from cisco.com.
2. Extract the files.
3. Copy *install.sh* to the target machine.
4. Change the permissions on the copied *install.bin* file to make the file executable by entering:

   ```
   chmod 755 install.sh
   ```

5. After copying the file to the directory, begin the installation program by entering:

   ```
   sh ./install.sh
   ```

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

6. After reading the introductory text that explains how to cancel the installation or modify a previous entry on a previous screen, click **Next**.
7. 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.
8. 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.

9. 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. See Installing Fault Tolerance, page 101 for more information.

10. Click **Next**. The **Select Admiral Database Creation Option** panel displays.
11. Select **Automatic** or **Manual**.

    CWA 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.

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

    CWA 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 specified database user will create the 'tidal' schema and its three tablespaces.

13. Click **Next**. The **JDBC Driver Information** panel displays.

14. 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.

15. Click **Next**. The **Test JDBC Connection** panel displays.

16. 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.

17. Click **Next**. The **Admiral Tablespace Installation** panel displays.

18. Specify the location for the Oracle tablespace directories to be created.

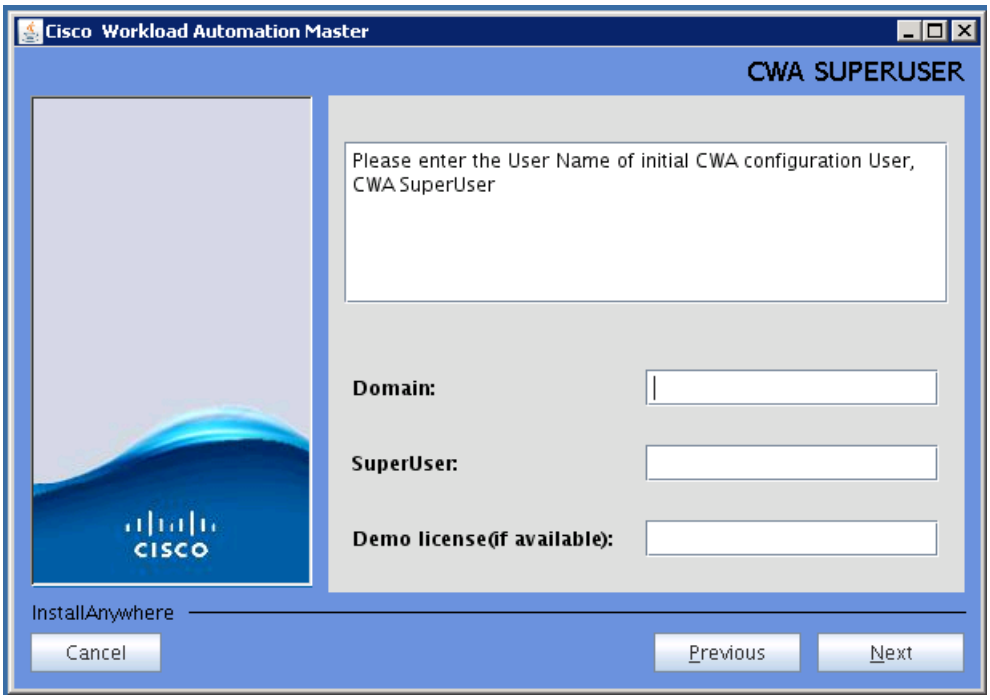
    - To use any location other than the default location, enter the directory paths to the ADMIRAL_DATA, ADMIRAL_INDEX and ADMIRAL_TEMP tablespaces. Do not change the actual datafile names. Change only the directory paths.
    - If your database is on a Windows platform, be sure to use Windows pathname 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*).

19. Click **Next**. The **Master Host Name** panel displays.

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

21. Click **Next**. The **CWA SUPERUSER** panel displays.

Figure 1 CWA SUPERUSER panel



- Enter the domain name of the initial CWA configuration Super User.
- Enter the name of the initial CWA configuration Super User.
- If you have a Demo license, enter the license number.

22. Click **Next**. The **Get Authentication Method** panel displays.
23. Select **AD** for Active Directory or **LDAP**.
24. For Active Directory, enter this information:
    - **Host–** Enter the hostname or IP address for the Active Directory server.
    - **Port–**Enter the port number for the AD 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.
25. 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 CWA Web Client user authentication is defined to use Oracle/Sun Directory Server with role-based access.

- **Index–** Check this option if you have an index.
- **GroupBindDN–** Enter the group account to query the LDAP server.

Note: If you want to authenticate users across multiple domains rather than installing the Master in each domain, follow the instructions in Enabling Multi-Domain Authentication, page 44

26. Click **Next**. The **Pre-Installation Summary** panel displays.

    This screen summarizes the information entered during the installation procedure.

27. Review the information to ensure it is correct.

28. 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.

29. Review the database report for any error notices.

30. 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.

31. 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 Unix Master 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:

1. Download the Cisco Workload Automation Base Product software for your environment from cisco.com.
2. Extract the files.
3. Copy *install.sh* to the target machine.

4. Change the permissions on the *install.sh* file in the directory to make the file executable:

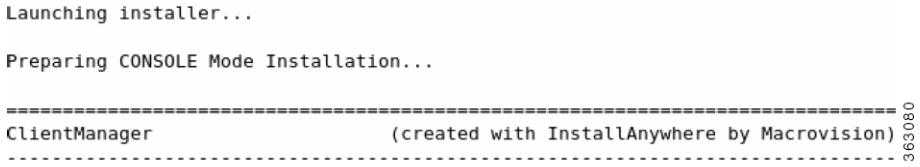
   ```
   chmod 755 install.sh
   ```

5. Open a command prompt window and enter:

   ```
   # sh ./install.sh -i console
   ```

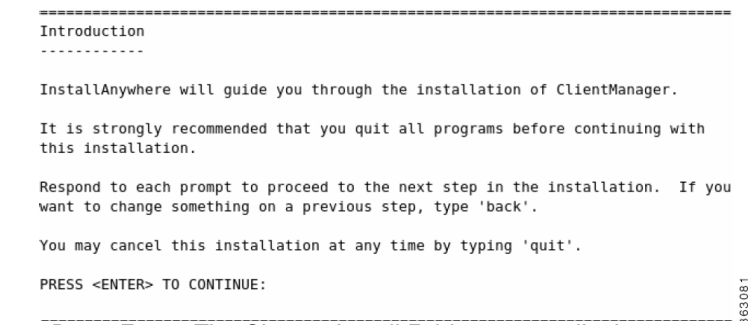
6. Press **Enter**. The following screen displays as the installation program begins.

Figure 2 Launching Installer Screen



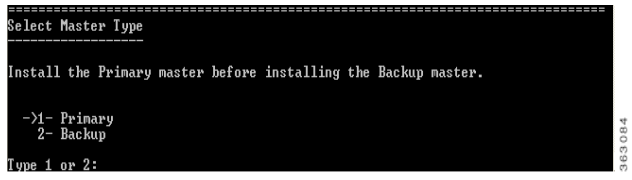
The initial installation screen is followed with the Introduction screen that provides instruction for proceeding with the installation program.

Figure 3 Introduction Screen



7. Press **Enter**. The Choose Install Folder screen displays.
8. Enter the directory path where the Master files should be installed. It is recommended that you use the default directory path when installing.
9. Press **Enter**. The Select Master Type screen displays.

Figure 4 Select Master Type Screen



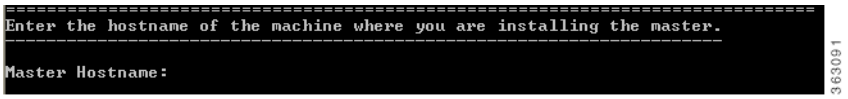
10. Select whether you are installing a primary or Backup Master.

    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 Installing Fault Tolerance, page 101 for more information on installing fault tolerance.)

11. Press **Enter**. The JDBC Driver screen displays.
12. 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).
13. Press **Enter**. The Master Hostname screen displays.



14. 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.

15. Press **Enter**. The SNMP Information screen displays.

    If you want to use the email function in CWA, 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**.

16. 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.
17. Press **Enter**. The CWA SUPERUSER screen displays.

18. Enter the domain name of the initial CWA configuration SuperUser, then press **Enter**.
19. Enter the name of the initial CWA configuration SuperUser, then press **Enter**. The Pre-Installation Summary screen displays.
20. Review the accuracy of the information.
21. 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.

22. Press **Enter** to exit the installer.
23. 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:

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

3. Enter the information you received from Technical Services in the appropriate brackets in the *connectdb.sql* script.
4. Save the script.
5. Locate the *orapopulate.sql* script within the *sql* directory.
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 CWA database should now be installed.

7. Save the script.
8. Login as the SYSTEM user (or equivalent).
9. Run the *connectdb.sql* script to create a user called *tidal* and to create the database tablespaces. Run the following scripts as the CWA 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 CWA 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.

Command	Description
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:

1. Check the status of the Master to see if it is running, by entering:

```
./tesm status
```

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
   ```

3. Once the Master is stopped, use the Unix file manager to locate the uninstaller folder called *UninstallerData*.
4. From the *UninstallerData* folder, run *Uninstall_UnixMaster*. The Uninstall Master panel displays.
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.

6. Click **Done** to exit.

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.

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:

1. Check the status of the Master to verify that it is not running by entering:

   ```
   ./tesm status
   ```

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
   ```

3. Once the Master is stopped, return to the Master directory.

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

5

Installing the Client Manager

This chapter describes the prerequisites and installation procedures for installing the Client Manager on Windows and Unix machines.

Two main components of the CWA architecture are the Master and Client Manager. The Client Manager allows CWA to achieve higher performance and scalability needs. Its purpose is to service requests from user-initiated activities, such as through the CWA Web Client, CWA Transporter and from other external sources that utilize the Command Line Interface (CLI) or published CWA Web services. Client Manager allows the CWA 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: Until TES 6.2, the Client Manager cache database could be deployed on Derby, MSSQL 2005, 2008 R2, or 2012 or Oracle 10g, 11g, 11g R2, or 12c. From TES 6.2 and later, you must deploy a stand-alone cache database using MSSQL or Oracle. TES 6.2.1 SP3 and later support MSSQL 2008 R2, 2012, and 2014 or Oracle 11g, 11gR2 or Oracle 12c. See the *CWA Compatibility Guide* for specific database version support for all platforms and versions.
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. See Installing a CWA Cache Database, page 64.

This chapter covers:

Installation Prerequisites

For platform support and minimum system requirements for the Client Manager, see Installation Prerequisites, page 63 in this guide. 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 CWA Windows/Unix Master.

- Apply all patches supplied in the latest hotfix.
- Be sure that you have installed JDK version 1.8 on the Client Manager machine.
- Obtain machine names, host names, port numbers and IP addresses before beginning the installation.
- Ensure that each computer used for CWA can communicate with the other machines on the network. If you cannot ping to and from each component machine, CWA cannot function properly. Network conditions affect the operation of CWA.
- 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.
- If the MSSQL DB server is **Azure SQL database**, install the Microsoft SQL Server Native Client 11.0 in the Client Manager environment.
- Contact Support if you have any questions.

Installing a CWA Cache Database

You must deploy a stand-alone CWA Cache which is named “TESCache” on one of these database platforms: MSSQL 2008, 2012 or Oracle 11gR2. See the *Cisco Workload Automation Compatibility Guide* for specific version support for each CWA release. 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.

The instructions for installing an MSSQL or Oracle cache database are described in these sections:

- Installing an MSSQL Cache Database, page 64
- Installing an Oracle Cache Database, page 65

Installing an MSSQL Cache Database

To install an MSSQL cache database:

1. Locate the *createcachedb-mssql.sql* script. The datafile sizes should match those from the Master database.
2. Edit the script for datafile locations and user password. The default password is " tidalcloud888" .
3. Save the script.
4. Execute the script in MSSQL server to create the new database.
5. Locate the plugin *<ClientManagerInstallDir>/config/<cache>.dsp* configuration file. For example, *C:\program files\TIDAL\ClientManager\config\tes-6.2.dsp*.
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
```

7. Copy the MSSQL JDBC driver, *sqljdbc4.jar*, into *<ClientManagerInstallDir>/lib*.
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.

Installing an Oracle Cache Database

To install an Oracle cache database:

1. Locate the createcachedb-oracle.sql script in *<ClientManagerInstallDir>/cache/<cache>/cachesql.zip*.
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”.
3. Save the script. The user (schema) name must be TES. This cannot be changed.
4. Execute the script as Oracle SYSTEM user (or equivalent).
5. Locate the plugin ***<****ClientManagerInstallDir>/config/<cache>.dsp* configuration file. For example, *C:\program files\TIDAL\ClientManager\config\tes-6.2.dsp*.
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
   ```

7. Copy the Oracle JDBC driver, *ojdbc6.jar*, into *<ClientManagerInstallDir>/lib*.
8. Restart the Client Manager.

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.

Installing Client Manager for Windows

To install Client Manager:

1. Copy the appropriate installation files to the target machine.
2. Navigate to the **\Client Manager\<your platform>** directory.
3. Double-click *setup.exe*. The **Security Warning** dialog box displays.
4. Click **Run**. The **Preparing to Install...** dialog box displays followed by the Welcome dialog box.
5. Click **Next**. The **Destination Folder** panel displays.
6. Select the directory where the CWA files will reside.

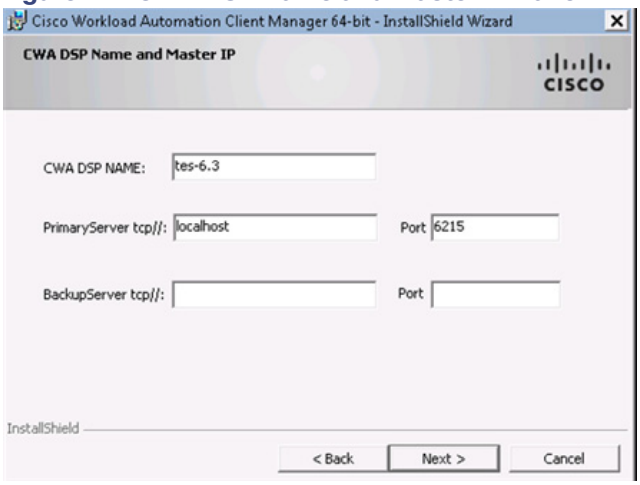
- Accept the default location **C:\Program Files\Tidal\ClientManager.**

-or-

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

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

Figure 1 CWA DSP Name and Master IP Panel



8. Enter these values:

   CWA DSP NAME—Enter the name of your Data Source Plug-in. This value can be anything you want it to be. The default is `tes-6.3`.

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

   PrimaryServer tcp//—Enter the host name or IP address for your Primary Master. The default port is **6215**.

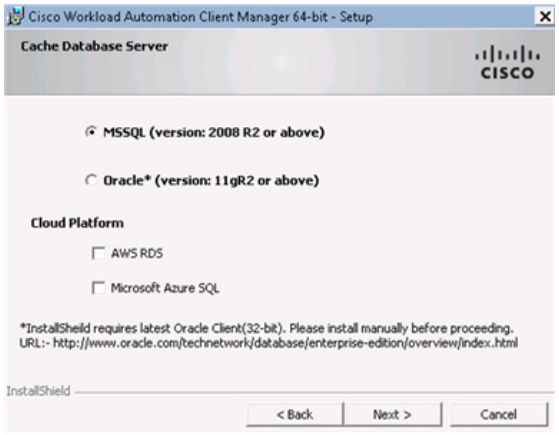
   BackupServer tcp//—If using Fault Tolerance, enter the IP address for your Backup Master.

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

10. Choose **MSSQL (2008 R2 or above)** or **Oracle* (version:11gR2 or above)**. If **MSSQL (2008 R2 or above)** is selected, the AWS RDS option and Microsoft Azure SQL option are displayed.

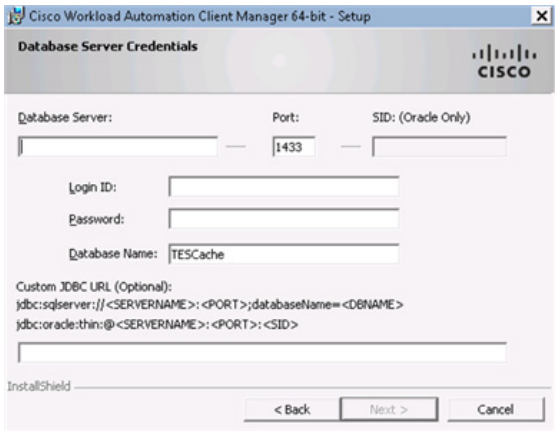
    Note: If **Oracle*(Version:11 gR2 or above)** is selected, the **Microsoft Azure SQL** option is not visible.

Figure 2 Cache Database Server Panel



11. Click **Next**. The **Database Server Credentials** panel displays.

Figure 3 Database Server Credentials Panel



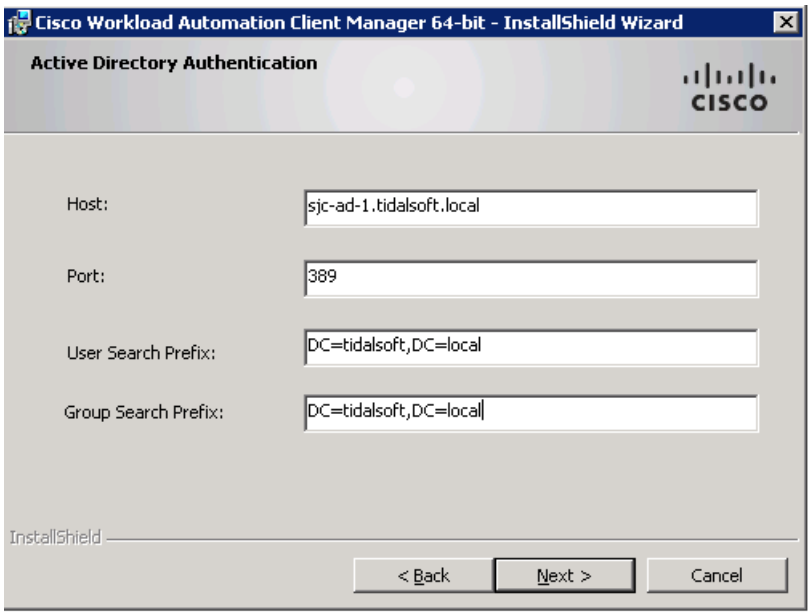
12. Enter the login credentials and database name, and click **Next**. The **Active Directory/LDAP Authentication** panel displays. By default, the **Database Name** is **TESCache**.

13. Select Active Directory or LDAP, 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.

Figure 4 Active Directory Authentication Panel



14. For Active Directory, enter the following information:

    - **Host** – Enter the hostname or IP address for the Active Directory server.
    - **Port** – Enter the port number for the AD 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.

    Example of an AD Setting

    ```
    Security.Authentication=ActiveDirectory
    ActiveDirectory.Host=<ip address or your_hostname>
    ActiveDirectory.Port=389
    ActiveDirectory.UserSearchPrefix=DC=example,DC=com
    ActiveDirectory.GroupSearchPrefix=DC=example,DC-com
    ```

15. 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.
    - **Index**– Check this option if you have an index.
    - **GroupBindDN** – Enter the group account to query the LDAP server.

    Example of an LDAP Setting

    ```
    Security.Authentication=LDAP
    LDAP.HostName=<ip_address or hostname>
    ```

```
LDAP.Port=389
LDAP.BindDN=ou=people,dc=example,dc=com
LDAP.UserObjectClass=inetOrgPerson
LDAP.UserBindDN=dc=example,dc=com
LDAP.GroupBindDN=dc=example,dc=com
```

Note: If you want to authenticate users across multiple domains rather than installing Client Manager in each domain, follow the instructions in Enabling Multi-Domain Authentication, page 69

16. Click **Next**. The **Ready to Install the Program** panel displays.
17. 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.** The **Installing Cisco Workload Automation 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.
18. The **Setup Completed** panel displays.
19. 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 6.3.2 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.

Enabling Multi-Domain Authentication

CWA allows for multiple-domain user authentication for Client Manager. The purpose of this function is to allow users defined in different domains to be authenticated within one Client Manager configuration to avoid installing one Client Manager per domain.

To enable this multi-domain authentication:

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 CWA user authentication.

   This example defines two servers:

   ```
   <ext-user-auth>
   <user-auth>
   <name>CWA1</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>CWA2</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 example above, the authentication process will validate **CWA1** first and then **CWA2**.

Verifying Successful Installation

You should verify that all of the required 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: Jobs and other object definitions can be viewed or modified after the Primary Sync is completed and the Client Manager is initialized.

Installing Client Manager for Unix

To install Client Manager for Unix:

1. Copy *install.sh* to the target machine.
2. Change the permissions on the copied *install.sh* file to make the file executable by entering:

   ```
   chmod 755 install.sh
   ```

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

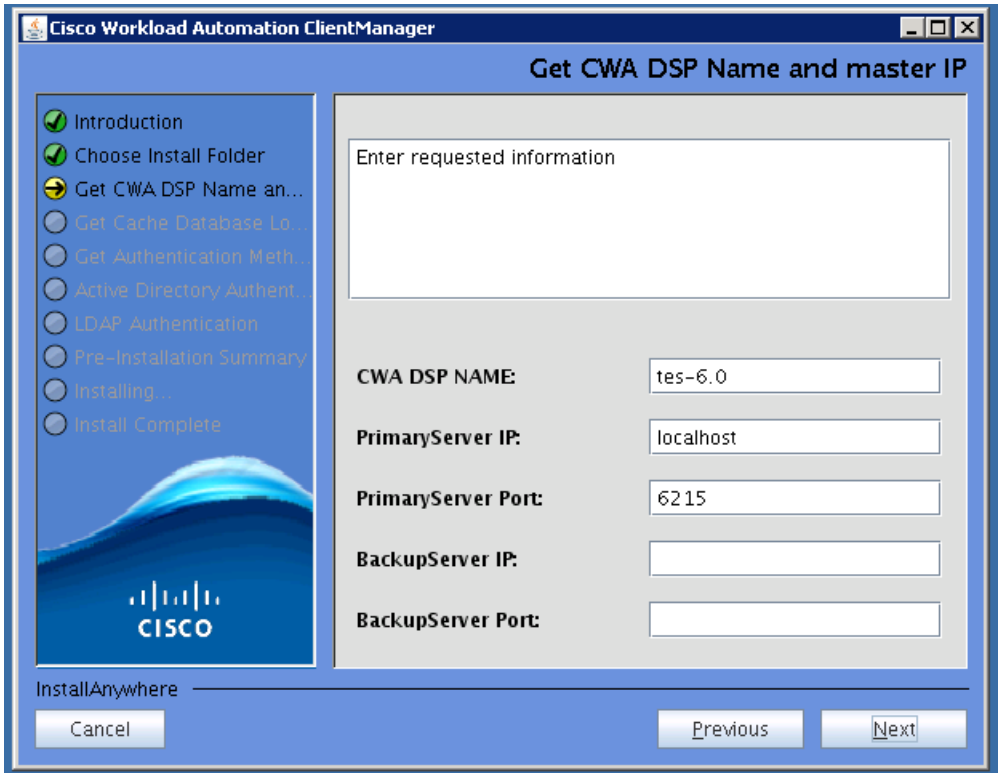
   ```
   sh ./install.sh
   ```

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

   The **Introduction** panel follows.

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 Install Folder** panel displays.
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.
6. Click **Next**. The **Get CWA DSP Name and Master IP** panel displays.

Figure 5 CWA DSP Name and Master IP Panel



- **CWA DSP NAME**—Enter the name of your Data Source Plug-in. This value can be anything you want it to be. The default is `tes-6.0`.

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

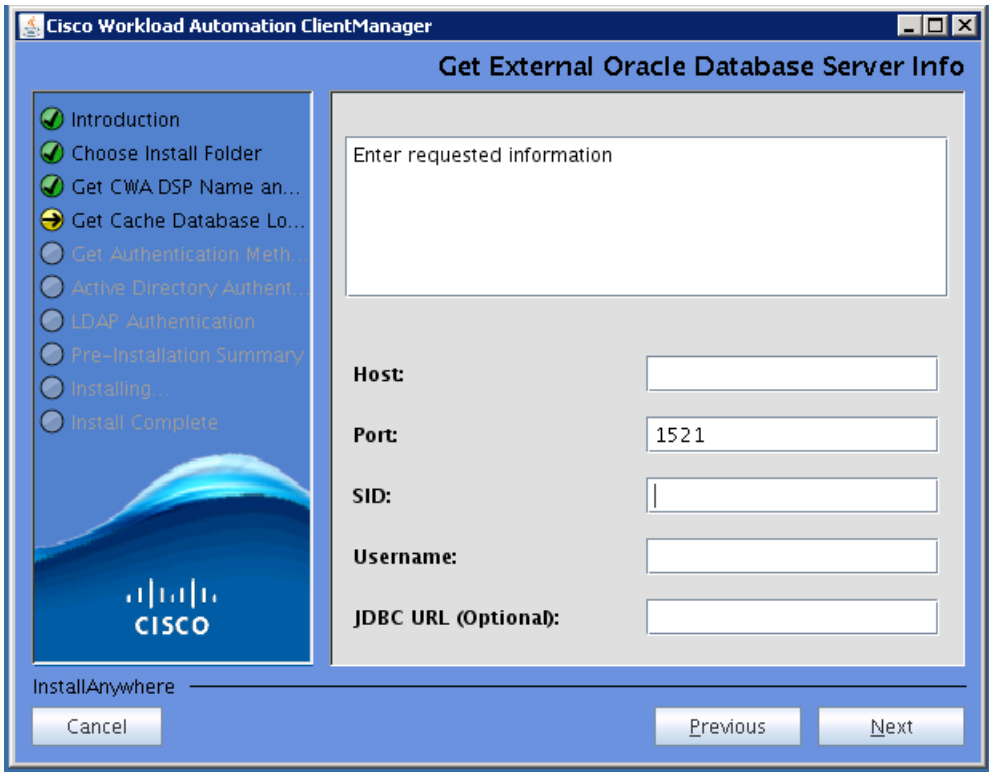
- **Primary Server IP**—Enter the host name or IP address for your Primary Master.
- **Primary Server Port**—Enter the port id for the primary server. The default port is **6215**.
- **Backup Server IP**— If using Fault Tolerance, enter the IP address for your Backup Master.
- **Backup Server Port**—Enter the port id for the backup server.

7. Click **Next**. The **Get Cache Database Location** panel displays.

   The only option, **Oracle database (version 11R2 and above)**, is selected by default.

8. Click **Next**. The **Get External Oracle Database Server Info** panel displays.

Figure 6 Get External Oracle Database Server Info Panel



9. Enter this information:
   - **Host**–Enter the hostname of the database server.
   - **Port**–Enter the port number of the database. The default port for Oracle is 1521.
   - **SID**–Enter the Oracle System ID.

   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.
   - **Username**– Enter the user name for the database administrator.
   - **JDBC URL (Optional)**– Enter the JDBC URL.
10. Click **Next**. The **Enter Oracle DB Server User Password** panel displays.
11. Enter the Oracle user password.
12. Click **Next**. The **Select New or Existing Cache Database** panel displays.
13. Select one of these options:
   - Create new CacheDB (Default)
   - Overwrite (Replace) current CacheDB (recommended)
   - Skip (use existing) CacheDB (not recommended)
14. Click **Next**. The **Get Authentication Method** panel displays.
15. Select **AD** for Active Director or Click **Next**. , 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.

Note: See also, Enabling Multi-Domain Authentication, page 69.

16. For Active Directory, enter the following information:
    - **Host** – Enter the hostname or IP address for the Active Directory server.
    - **Port** – Enter the port number for the AD 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.

    -or-

17. 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.
    - **GroupBindDN** – Enter the group account to query the LDAP server.
18. Click **Next**. The **Pre-Installation Summary** panel displays.

    This screen summarizes the information entered during the installation procedure.
19. 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 Client Manager** panel displays.

    The status of your installation is displayed with a progress bar. The **Install Complete** panel displays.
20. 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, the number of threads, and other variables, this can take some time.

Installing Client Manager from a Command Line

To install Client Manager from a command line:

1. Copy *install.sh* to the target machine.
2. Change the permissions on the copied *install.sh* file to make the file executable by entering:

```
chmod 755 install.sh
```

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

   ```
   sh ./install.sh -i console
   ```

   The following screen displays as the installation program begins.

   When the installation program starts, the Introduction screen displays.

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.

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

6. Verify the path you entered, then press **Enter**. The Get CWA 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.

7. Enter the name of your Data Source Plug-in, then press **Enter**.

8. Enter the host name or IP address for your Primary Master, then press **Enter**.

9. Enter the port number for the Primary Master, then press **Enter**.

10. Enter the host name or IP address for your Backup Master, then press **Enter**.

11. Enter the port number for the Backup Master, then press **Enter**.

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

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

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 CWA Web Client user authentication is defined to use Oracle/Sun Directory Server with role-based access.

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

    Once installation is complete, the Installation Complete screen displays.
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.

Configuring the Index Tablespace for Oracle Databases

When using an Oracle cache database with the Client Manager, the index tablespace might need to be configured. In CWA 6.2 and beyond, the index tablespace in the tes-6.0.dsp file is a configurable option. This file should have the following property:

```
DataCache.Oracle.IndexTableSpace=TESCACHE_INDEX_<oracle_sid>
```

where oracle_sid is the Oracle system identifier.

For example:

```
DataCache.Oracle.IndexTableSpace=TESCACHE_INDEX_ORCL
```

Note: If this definition is commented out, you must uncomment it.

Once this is set, clear the cache and restart Client Manager.

Starting and Stopping Client Manager

Starting and Stopping the Windows Client Manager

To start Client Manager:

1. From the Windows Start menu on the Master machine, choose **All Programs > Cisco Workload Automation > Scheduler > Service Control Manager** to display the **CWA Service Manager**.
2. From the Service list, choose **Client Manager**. The Client Manager status displays at the bottom of the dialog box.
3. Click **Start** to start the Client Manager.

To stop Client Manager:

1. From the Windows Start menu on the Master machine, choose **All Programs > Cisco Workload Automation > Scheduler > Service Control Manager** to display the **CWA Service Manager**.
2. From the Service list, select **Client Manager**. The Client Manager status displays at the bottom of the dialog box.

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

Starting and Stopping the Unix Client Manager

To start Client Manager:

1. Open a command prompt window.
2. Enter:

   ```
   ./cm start
   ```

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

To stop Client Manager:

1. Open a command prompt window.
2. Enter:

   ```
   ./cm stop
   ```
3. Press **Enter**.

Uninstalling Client Manager

Uninstalling the Windows Client Manager

The CWA Master is uninstalled from the Windows Control Panel.

To uninstall Client Manager:

1. From the Windows Start menu, choose **Control Panel**, then double-click **Add or Remove Programs**.
2. Scroll down the list of programs installed on the machine to the Client Manager program.
3. Click the Client Manager program to highlight it.
4. Click **Remove** to start the uninstallation process. A confirmation message displays.
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.

   Regulatory: 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.
6. Click **OK** to finish.
7. Repeat to remove other components.
8. Once you complete uninstalling components, reboot the machine to clear the registry..

   Regulatory: 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:

1. Open a command prompt window.
2. Enter:

```
# sh ./Uninstall_UnixClientManager
```

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

1. Open a command prompt window.
2. Enter:

```
# sh ./Uninstall_ClientManager -i console
```

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

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.

Configuring SSL

This section describes the various ways you can configure SSL for CWA:

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 Workload Automation products installed and connected to one another:

- Master
- Client Manager
- 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:

1. Shut down the Client Manager.
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.

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>
-->
```

4. Save the file and start the Client Manager.

5. Open a web browser on the Client Manager host system and enter the URL of CWA Web Client 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 SSL using your own certificate:

1. Obtain the 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

2. Configure the SSL connector with the server key and certificate:

In this section, you 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, page 78.

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

f. (Optional) Obfuscate the passwords before storing them in the file so their secrecy is secured. See Obfuscating Passwords for SSL, page 81.

g. (Optional) 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.

h. Save the file and start the Client Manager.

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

Open a Web browser and enter the URL of CWA Web Client 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 Active Directory

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

To configure SSL for Active Directory:

1. Shut down the Client Manager.
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*.

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
   ```

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
   ```

5. (Optional) Obfuscate the passwords before storing them in the file so their secrecy is secured. See Obfuscating Passwords for SSL, page 81.
6. Restart the Client Manager.

Obfuscating Passwords for SSL

When configuring SSL, you can obfuscate the passwords before storing them in the file so their secrecy is secured.

To obfuscate passwords

1. First, open a command shell window and change directory to the **lib** directory under Client Manager's installation directory.
2. Issue this command:

   java -cp jetty-util-9.1.5.v20140505.jar org.eclipse.jetty.util.security.Password <your_password>

   where **<your_password>** is the password to be obfuscated. This output of this command is something like:

   ```
   OBF:<password_string>
   MD5:<password_string>
   CRYPT:<password_string>
   ```

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

Connecting to an SSL-Enabled Active Directory or Open LDAP Environment

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

1. Stop the Client Manager.
2. Request a copy of the CA Certificate for Client access.
3. For the 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 an Open LDAP server, copy a DER encoded CA Certificate from the Open LDAP Client to the Client Manager machine. For example, *certnew.cer*.
4. 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
```

5. 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
   ```

6. (Optional) Obfuscate the passwords before storing them in the file so their secrecy is secured. See Obfuscating Passwords for SSL, page 81.

7. 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

Kerberos Authentication Support for Web Client

This section provides the prerequisites and configuration details for Kerberos authentication.

Prerequisites

To perform Kerberos authentication

- All Machines required for Kerberos setup should be in the same domain, for example, CWAKERBEROS.COM.
- Kerberos setup for CM requires minimum of four boxes in the same domain with administrator rights:
  - Active Directory Box with domain controller (for example, named as CWAKDC).
  - Client Manager Box (for example, named as CWAAPP).
  - Master Box (for example named as CWAMASTER).
  - Client Browser Box (for example named as CWACLI).
- Ensure that the all boxes are reachable from each other through the following commands:

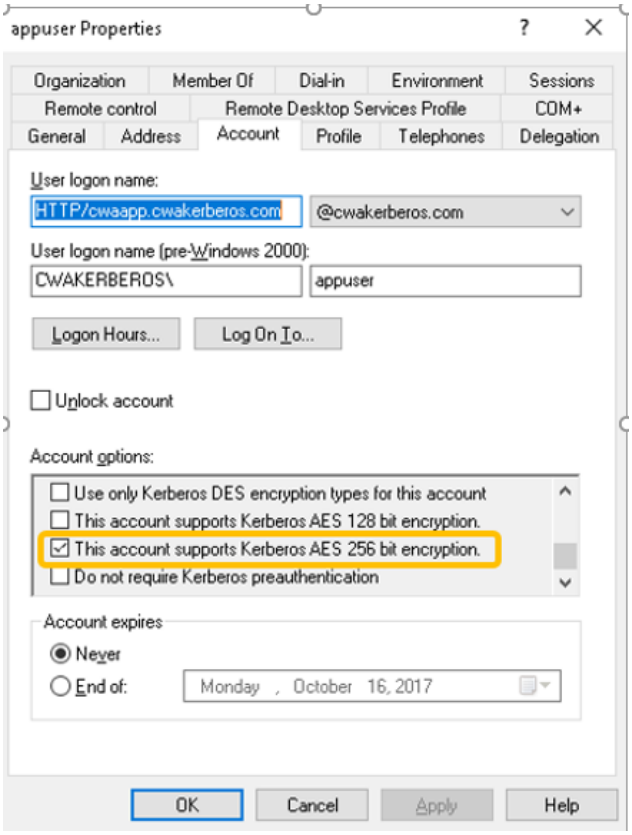
  ```
  ping <hostname> or <IP address>
  nslookup <hostname> or <IP address>
  ```

- Create required users on the AD. A specific user is required to start the client manager service. For example, appuser.
- Configure the users to support AES 256 encryption. For more information, see Configuring Users

Configuring Users

After the creation of user accounts, navigate to **Account** tab and choose **This account supports Kerberos AES 256 bit encryption** as Account option.

Figure 7 Properties with Account Details



Creating Service Principal Name/Key Tab File And Updating JCE jars to JDK

To create service prinicipal name/key tab file and updating JCE jars

- Open a command prompt in AD box.

  Create SPN for the client manager box user who starts the client manager service. This SPN creation is a mapping between the client manager box user and service running on the client manager box.

- Enter the following command to ensure that there are no SPNs registered for that user:

  ```
  setspn -l <client manager user>
  ```

  For example, setspn -l appuser

  ```
  c:\Users\Administrator>setspn -1 browseruser
  Registered ServicePrinicpalNames for CN=browseruser, OU=dev, DC=cwakerberos, DC=com
  ```

- To add the SPN user, enter the following command:

```
setspn  -s <service name> <client manager user>
```

For e.g., setspn -s HTTP/cwaapp.cwakerberos.com appuser

- To add all possibilities for the service, add the following:

```
setspn -s HTTP/cwaapp appuser
```

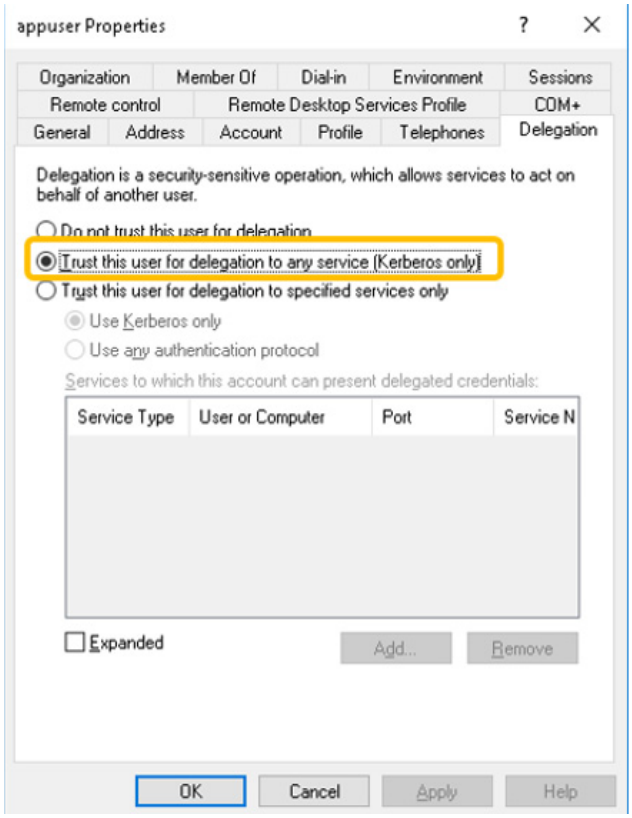
- To ensure registration for all, enter the below command:

```
c:\Users\Administrator>setspn -1 appuser
Registered ServicePrincipalNames for CN=appuser, CN=Users, DC=cwakerberos, DC=com;
HTTP/cwaapp.cwakerberos.com
HTTP/cwapp
```

- Navigate to the AD box and users section to choose the client manager user (appuser).
- Select **Delegation** tab and choose **Trust this user for delegation to any service (Kerberos only)**.

  Note: This **Delegation** Tab is enabled only when the user is registered for any service principal.

Figure 8 Properties with Delegation Details



- Create the Key tab file which is the authorization token for client manager user (appuser).
- On the command prompt, enter the following command:

```
ktpass -out <keytab location> -princ <SPN>@<realm name> -mapUser <domain\client manager user name>
-mapOp set -pass <password> -crypto <crypto> -pType KRB5_NT_PRINCIPAL

For example,
```

```
ktpass -out c:\temp\appuser.keytab -princ HTTP/cwaapp.cwakerberos.com@CWAKERBEROS.COM -mapUser
cwakerberos\appuser -mapOp set -pass control@123 -crypto AES256-SHA1 -pType KRB5_NT_PRINCIPAL
```

- Copy the key tab file from AD box to the client manager box.
- Add JCE jars to JDK (or JRE) to support unlimited strength cryptographic functions by following the below steps:
  - Download the **JCE Unlimited Strength Jurisdiction Policy Files jce_policy-8.zip** (for Java 8) from http://www.oracle.com/technetwork/java/javase/downloads/index.html. The zip file contain two jar files : local_policy.jar, US_export_policy.jar a README.txt and a COPYRIGHT.html file.
  - Apply the .jar files into the actual JDK that is being run.

  Note: There are two directories namely JDK and JRE directory (For example JDK1.8 and JRE1.8)
  - Copy the two .jar files from the zip file, and replace the ones in the JDK distribution of the JRE. For example, **/jdk1.8.0_37/jre/lib/security/** and **/jre1.8.0_37/lib/security/** directories

Configuring Client Manager for Kerberos

To configure the client manager

- Ensure that the Kerberos Setup for client manager have the below artifacts. For Windows, the below artifacts are available in the config folder of the client manager for configuration.
  - spnego.conf file
  - krb5.ini file
  - spnego.properties file
- For Unix, ensure that you create, configure and place the above files in the config folder of the client manager.

  The contents of the spnego.conf is given below:

```
com.sun.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required
principal="HTTP/cwaapp.cwakerberos.com@CWAKERBEROS.COM" <SPN with realm>
keyTab="c:/temp/appuser.keytab" <location of the key tab file>
useKeyTab=true
storeKey=true
debug=true
isInitiator=false;
};
com.sun.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
principal="HTTP/cwaapp.cwakerberos.com@CWAKERBEROS.COM" <SPN with realm>
useKeyTab=true
keyTab="c:/temp/appuser.keytab" <location of the key tab file>
storeKey=true
debug=true
isInitiator=false;
};
```

  The contents of the krb5.ini described below:

```
[libdefaults]
default_realm = CWAKERBEROS.COM <domain name>
default_keytab_name = c:/temp/appuser.keytab <key tab file location>
```

```
permitted_enctypes = aes128-cts aes256-cts arcfour-hmac-md5
default_tgs_enctypes = aes128-cts aes256-cts arcfour-hmac-md5
default_tkt_enctypes = aes128-cts aes256-cts arcfour-hmac-md5

[realms]
CWAKERBEROS.COM = {
kdc = 172.21.243.238 <IP address of the AD box>
admin_server = 172.21.243.238
default_domain = CWAKERBEROS.COM
}

[domain_realm]
cwakerberos.com= CWAKERBEROS.COM
.cwakerberos.com = CWAKERBEROS.COM

[appdefaults]
autologin = true
forwardable = true
```

The contents of the spnego.properties described below:

```
targetName = HTTP/cwaapp.cwakerberos.com@CWAKERBEROS.COM
```

- Edit the **clientmgr.props**, and provide the following configuration. It is recommended that you use forward slash '/' as the file separator. If you use Windows style file separator '\', you must escape each by a backslash '\'.
  - Flag to set Kerberos mode. If set to false, the client manager works in Basic authentication mode through AD/LDAP

```
Security.isKerberos=true
```

  - Domain name

```
Security.Kerberos.domainRealm=CWAKERBEROS.COM
```

  - Location of the krb5.ini file. The customer can provide their own path in which the files are located.

```
Security.Kerberos.krbPath=C:\\Program Files\\Tidal\\Client Manager\\config\\krb5.ini
```

  - Location of the spnego.conf file. The customer can provide their own path in which the files are located.

```
Security.Kerberos.loginConfPath= C:\\Program Files\\Tidal\\Client Manager\\config\\spnego.conf
```

  - Location of the spnego.properties file. The customer can provide their own path in which the files are located.

```
Security.Kerberos.spengoTargetPath= C:\\Program Files\\Tidal\\Client
Manager\\config\\spnego.properties
```

  - Logging flags

```
Security.Kerberos.spengoDebug=all
Security.Kerberos.krbDebug=true
```

  - Domain name

```
Security.Kerberos.krbRealm=CWAKERBEROS.COM
```

  - AD box hostname

```
Security.Kerberos.KDCHostName=cwakdc.cwakerberos.com
```

Configuring Browsers for Kerberos Authentication

To configure the browsers for Kerberos authentication

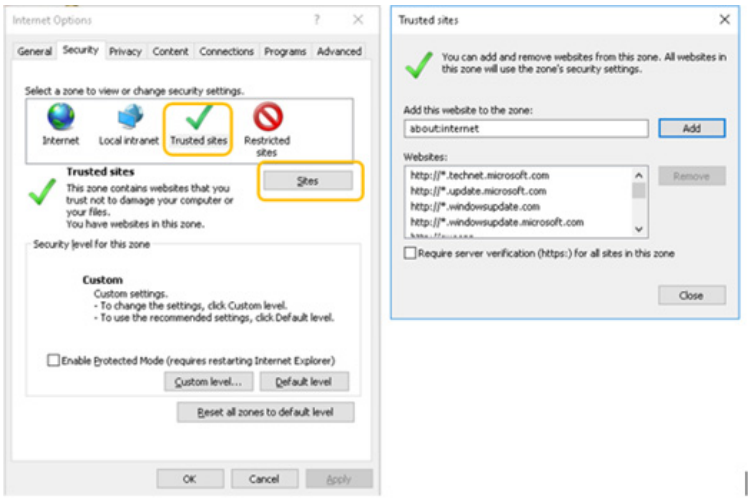
1. **IE**

   - Navigate to **Tools** > **Options** > **Security > Local Intranet** > **Sites** (all should be selected) Windows Server version does not have this option.
   - Navigate to **Tools** > **Options** > **Security**> **Local Intranet** > **Sites**> **Advanced** (add URL to server (http:// and/or https:// use the hostname). Windows Server version does not have this option.

     For example, http://cwaapp.cwakerberos.com:8080/client
     https://cwaapp.cwakerberos.com:8080/client
   - Go to **Tools** > **Options** > **Security** > **Trusted Sites** > **Sites** (add this website to the zone (http:// and/or https:// use the hostname)

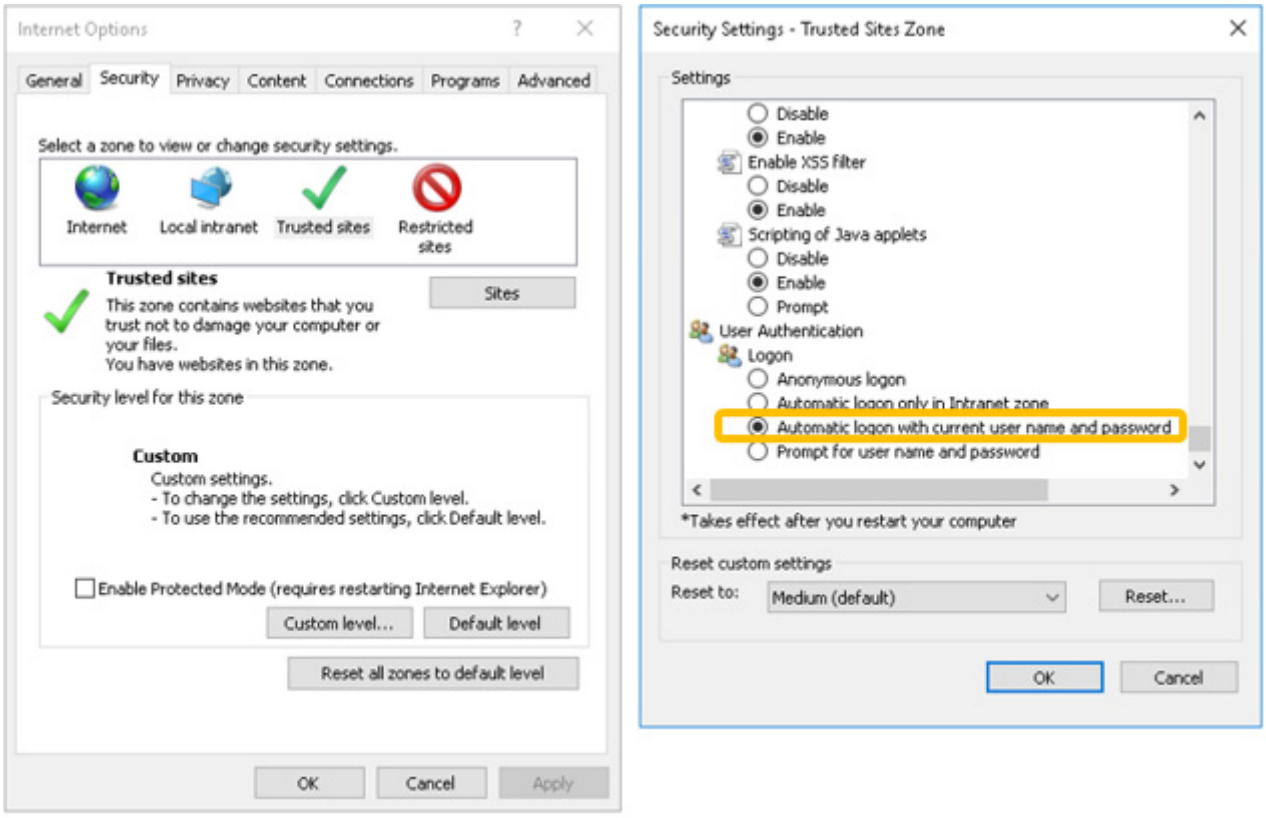
     For example
     http://cwaapp.cwakerberos.com:8080/client
     https://cwaapp.cwakerberos.com:8080/client

Figure 9 Internet Options and Trusted Sites



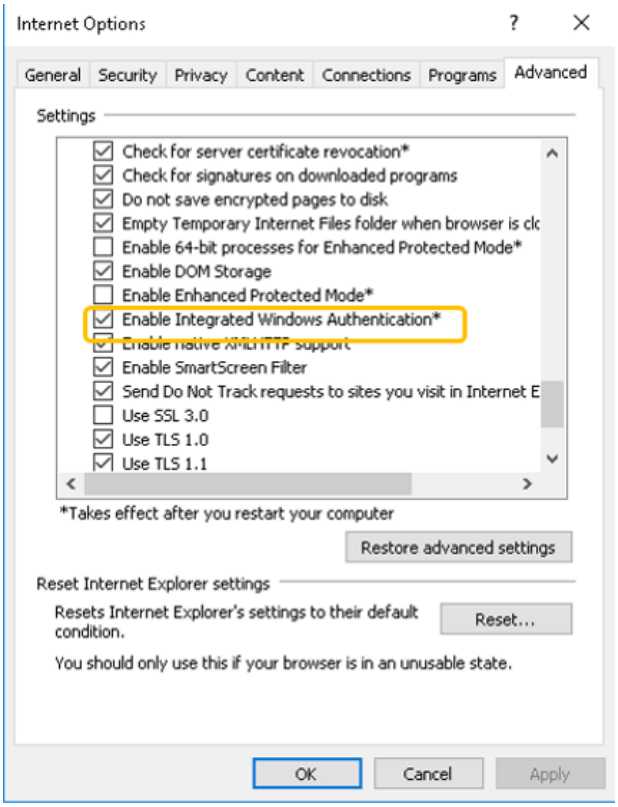
   - Navigate to **Tools** > **Options** > **Security** > **Trusted Sites**, and click **Custom level**. Under **Security Settings**, choose **User Authentication** and select **Automatic login with current user and password**.

Figure 10 Internet Options with Security Settings



– Go to **Tools** > **Options** > **Advanced**.

Figure 11 Internet Options with Advanced Settings



- Select **Enable Integrated Windows Authentication** option
- Close IE. Then, launch IE and browse the CM URL.

2. **Firefox**
   - Browse to about:config and agree to the warnings
   - Search for network settings
   - Set network.negotiate-auth.delegation-uris to http://,https://
   - Set network.negotiate-auth.trusted-uris to http://,https:/
   - Browse the CM URL
   - Launch the CM URL

Note: Ensure that the login is done without prompting for the credentials.

6

Installing a CWA Java Client

Cisco Workload Automation offers a desktop-like client experience with a light-weight Java Client which can be installed as a standalone application or can be launched from a browser connected directly to the CWA Master. Installers are provided for Windows and Unix operating systems.

This chapter covers:

Installation Prerequisites

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

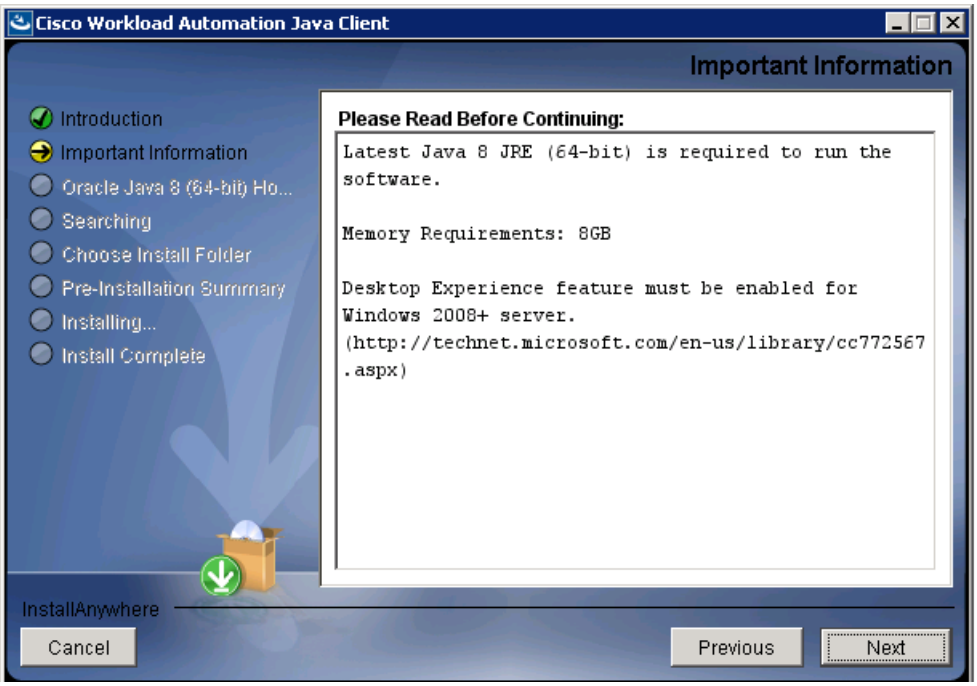
- Java 8 update 40 or higher (64-bit)
- Hardware specifications:
  - Memory: 8GB to 16GB
  - CPU (64-bit): 2.2+ GHz Quad Core
- Software specifications:
  - Only JavaFx2 certified systems are supported. See:

    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:

1. If necessary, download and extract the latest CWA software.
2. Navigate to the \TESClient\<your platform> directory.
3. Run the *install.exe* file. The installation wizard displays.
4. At the Introduction screen, click **Next.**
5. The installer displays the Important Information screen which contains important Java Client requirements:



6. Read the information and click **Next**.
7. At the Oracle Java 8 (64-bit) Home screen, choose the path to the Java 8 folder.

   Note: You may have installed multiple Java virtual machines. Ensure that you choose version 8 specifically.
8. At the Choose Install Folder screen, select the location where you want the Java Client to be installed.
9. The Pre-Installation Summary screen shows the items that will be installed. Click **Install**. The installation progress is shown in the next screen.
10. The Install Complete screen summarizes the results of the installation. Click **Done**.
11. Confirm that a new CWA Java Client shortcut is created.

Installing the Java Client for Unix

To install the Java Client for Unix:

1. Run the *install.sh* file. The installation wizard displays.

2. At the Introduction screen, click **Next.**
3. At the Important Information screen, read the information and click **Next**.
4. At the Oracle Java 8 (64-bit) Home screen, choose the path to the Java 8 folder.

   Note: You may have installed multiple Java virtual machines. Ensure that you choose version 8 specifically.
5. At the Choose Install Folder screen, select the location where you want the Java Client to be installed.
6. The Pre-Installation Summary screen shows the items that will be installed. Click **Install**. The installation progress is shown in the next screen.
7. The Install Complete screen summarizes the results of the installation. Click **Done**.
8. You can now launch the software by executing the `tesclient.sh` command.

Running the CWA Java Client

You can run the CWA Java Client as an application on your system, as well as via a web browser:

- Running the Java Client as a System Application, page 93
- Running the Java Client Via a Web Browser, page 94

See Configuring the CWA Java Client, page 95 for information about monitoring and controlling Java Client access and performance.

Running the Java Client as a System Application

Prerequisites

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

- The Java Client Host machine must be in the DNS/NIS+ domain.
- The Java Client Host machine must be allowed to connect to port 6215 of the CWA Master.
- The CWA master.props file must have a valid AD/LDAP configuration.

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

1. Launch the Java Client that you have installed. The Login screen displays.
2. Enter the following details:
   - **Server**– The Master's hostname
   - **User**– AD/LDAP user name
   - **Password**–AD/LDAP password
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, CWA will run a web server at port 8080. The Java Client host must be allowed to access a configured port on CWA's host machine.
- On Windows, only Internet Explorer 64-bit (c:\Program Files\Internet Explorer\iexplorer.exe) is capable of running 64-bit Java 8. Only 64-bit Java 8 will support 8GB memory requirements.
- For all operating systems and browsers, you must enable Java content in the Java Control Panel.
- The supported browser versions are the same as that of the CWA Web Client.

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

To run the Java Client via a web browser:

1. Open a CWA-supported web browser and enter the following URL:

   `http://<master's hostname>:8080/tesclient`

   where *master's hostname* is the host name of CWA.

2. Click **Launch Enterprise Scheduler**.
3. Click **Run** to allow execution of the Java Client.

   The Java Client is launched.

If the version of the 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.

Configuring the CWA Java Client

As a thick client, the CWA Java Client can consume a considerable amount of resources of the CWA Master. You can monitor and control CWA Java Client usage by:

Limiting the Number of CWA Java Client Connections

You can control the number of users connected to the CWA Master via the CWA Java Client at any time. If the configured maximum number of CWA Java Client connections is exceeded, additional requests are denied.

Note: Configuring a maximum number of CWA Java Client connections does not limit the number of CWA Web Clients connecting through the Client Manager, nor does it limit the number of super admin users using the CWA Java Client.

To limit the number of CWA Java Client connections

1. Open the master.props file that resides in the *config* directory on the Master machine.
2. Add this configuration property to master.props:

   ```
   TESClient.ConnectionLimit=<max_number_of_connections>
   ```

   where `<max_number_of_connections>` is the maximum number of CWA Java Client connections allowed to the CWA Master.

Restricting User Access via the CWA Java Client

You can control which users can connect to the CWA Master via the CWA Java Client.

Note: You cannot deny access to a super admin user.

To restrict user access via a CWA Java Client connection

1. In the Navigator, choose Administration > Security Policies.
2. Choose the Workgroups, LDAP Groups, or Interactive User and choose Edit.
3. Check “Deny TES Client Access”.
4. Save the security policy.

Viewing Slow CWA Java Clients

CWA Java Clients that are slow in consuming messages from the CWA Master can cause a Master process to consume a huge amount of heap memory while trying to retain the pending messages.

You can view the CWA Java Clients connected to the CWA Master at any time along with the information on whether any of the Java Clients is slow in communicating with the Master. If a Java Client connection is slow, a super admin user can terminate that connection.

Note: This feature is available only on the CWA Java Client.

To view slow CWA Java Client connections

1. Log on to the CWA Client.
2. From the Navigator, choose **Master Status**.
3. Click the **Connections** tab.

The **Queued Messages** column indicates the queued messages for each connection. A fast client should ideally show close to "0" queued messages or show a decreasing amount of queued messages over time.

Configuring the Monitoring of Slow CWA Java Client Connections

You can enable monitoring of the CWA Java Client connections to the CWA Master and be alerted when a slow connection is detected.

To configure the frequency of checking for slow CWA Java Client connections

1. Open the master.props file that resides in the *config* directory on the Master machine.
2. Add this configuration property to master.props:

   ```
   Client.SlowConnectionCheckInterval=<time_in_seconds>
   ```

   where `<time_in_seconds>` is how often CWA Java Client connections will be checked. To make sure that the monitoring process is not overly intrusive on the operations of the CWA Master, set to 60 seconds or more.

   When a slow CWA Java Client is detected, the system event "Client Connection Slow" is triggered. A CWA Client connection is considered to be slow if the client has received less than 95 percent of the messages from the CWA Master over the duration of the client session. You can optionally change this tolerance threshold as described in the next step.

3. (Optional) You can change the tolerance threshold for what is considered to be a slow connection using the following configuration property in master.props to any value other than 95 (such as 99 – meaning 99 percent):

   ```
   Client.SlowConnectionThreshold=95
   ```

4. (Optional) You can set up an action event when a slow connection is encountered. For example you could associate an Email Action to the "Client Connection Slow" System Event to get email notifications. See the "Events" chapter in the *Cisco Workloade Automation User Guide* for how to do this.

Controlling the Java Client Access

CWA provides a "whitelisting" mechanism for allowing Java Client access to the Master based on the Java Client's subnet mask, IP address, and/or user ID. This lets you restrict Master access by Java Clients that are unauthorized or that are on a slow network. For example, you might want to safeguard the Master from running out of memory due to a Java Client with a slow downloading speed which can cause a backlog in the Master memory.

Java Client Access Configuration Parameters

To support the Java Client whitelisting feature, CWA provides three parameters that control which Java Client IP addresses and users are allowed to access the Master. These parameters are specified in the master.props file:

- **TESClient.SubnetMaskList–**Specifies the list of one or more subnet mask(s) which comprises the Java Client IP addresses that are allowed to access the Master.

  - Multiple subnet masks must be comma-separated.
  - IPV6 is not supported.

  Example:

  ```
  TESClient.SubnetMaskList=171.37.102.224/28,173.37.154.96/28, 172.21.45.70/26
  ```

- **TESClient.IPAddressList**–Specifies the list of one or more Java Client IP addresses that are allowed to access the Master.
  - Multiple IP addresses must be comma-separated.
  - IP address ranges can be specified with a hyphen and multiple ranges should be comma-separated.
  - Both IPV4 and IPV6 are supported.

  Example value:

  ```
  172.21.45.70-172.21.47.145, 172.25.5.51
  ```

- **TESClient.UserIdList**–Specifies the Java Client users who are excluded from the whitelisting feature and are allowed to access the Master. That is, the TESClient.UserIdList lets you provide exceptions for some users if Java Client IP address is not in the allowed subnet mask list or the IP addresses list.
  - Separate multiple user names with a comma.

  Example:

  ```
  TESClient.UserIdList=tidalsoft\\sbrights, tidalsoft\\qatest
  ```

See Configuring the Master Parameters (master.props), page 168 for the details about entering these and other configuration parameters.

Note: After configuring the parameters, restart the Master for them to take effect.

Enabling Java Client Access

You enable Java Client whitelisting by setting the parameters described in Java Client Access Configuration Parameters, page 96 in master.props. The TESClient.SubnetMaskList and/or the TESClient.IPAddressList parameter must be specified to enable the IP address validation.

Java Client Validation Rules

When Java Client whitelisting is enabled, the Master validates each Java Client at login time using these rules:

- If all three parameters described in Java Client Access Configuration Parameters, page 96 are specified, the Master validates the Java Client in the order of TESClient.SubnetMaskList, TESClient.IPAddressList, and finally with TESClient.UserIdList.
- If neither TESClient.SubnetMaskList or TESClient.IPAddressList is configured, TESClient.UserIdList is ignored.
- If the Java Client IP address is not in the subnet mask list, the Master checks whether the IP address is in the allowed IP addresses list or range. If both validations fail, the Master checks whether the Java Client login user is in the configured user ids list. If all validations fail, user is not allowed to login with the Java Client and an error message is displayed. Otherwise, if any validation passes, the existing user authorization code takes effect.
- When either the TESClient.SubnetMaskList or the TESClient.IPAddressList parameter is configured, if TESClient.UserIdList is not configured, the IP address validation is done based on TESClient.SubnetMaskList or TESClient.IPAddressList only.

- If the hostname of a particular Java Client has more than one type of IP address (IPV4 and IPV6), the Master validates all hostnames against the allowed IP address list configured in the TESClient.IPAddressList parameter.

Possible Errors with Java Client Whitelisting

With Java Client whitelisting enabled, errors are displayed when IP address validation fails to help you understand and troubleshoot what occurred. The IP address (IPV4 and/or IPV6) are included in the error message so that you can provide this information to your Administrator while reporting this issue. All errors related to IP address validation are audited.

Two error types might be displayed:

- **Error Message Type-1:** When the **TESClient.IPAddressList** in master.props is configured with both IPV4 and IPV6 addresses, if Java Client hostname has both IPV4 and IPV6 and the IP address validation fails, an error message like this is displayed:

- **Error Message Type-2:** When **TESClient.IPAddressList** in master.props is configured with both IPV4 and IPv6 addresses and one of these things occurs:
  - The Java Client hostname has only IPV4.
  - The Java Client machine has both IPV4 and IPV6 address types but the **TESClient.IPAddressList** is configured only with IPV4.

  ...then an error message like this is displayed if IP validation fails:

Note: The latest Java Client is compatible with older Masters. However, IP address validation is bypassed in this case.

Managing Java Clients with Slow Connections

A Java Client with a slow connection, too little RAM, or other conditions can cause the Master to back up messages or consume high memory and even crash. You can configure a number of options in the master.props file to get warnings when a Java Client gets close to memory or queue size limits and terminate Java clients that exceed memory or queue size limits.

The typical reasons that a Java Client can cause problems with the Master are:

- The Java Client connects to the Master over a slow network.

- The Java Client has been allocated low JVM heap memory or an incorrect JVM parameter is defined in the CWA_client.bat file.
- The Java Client runs on a machine with insufficient RAM which may lead to paging to disk.
- There are many active Java Clients simultaneously, the Master can experience out-of-memory issues.

The configuration parameters provided to help manage these conditions are described in the table below.

Parameter	Description	Unit	Permitted Values
Client.SlowConnectionCheckInterval	The time interval at which the Master periodically checks for slow CWA Java Client connections.	Seconds	Integer (starts with 1)
CLIENT.RESOURCE_POLLING_INTERVAL	The polling interval the Java Client uses to check the queue size and memory usage of the Java Client.	Seconds	Integer (starts with 1)
CLIENT.WARNING_LIMIT_QUEUE_SIZE	The queue size limit at which a warning message is displayed if this value is exceeded.	Queue size	Integer (starts with 1)
CLIENT.TERMINATION_LIMIT_QUEUE_SIZE	The queue size limit at which the Java Client is terminated by the Master if this value is exceeded.	Queue size	Integer (starts with 1)
CLIENT.WARNING_LIMIT_MEMORY_UTILIZATION	The (% of Used Heap Memory to Total Heap Memory) or the (% Used RAM to Total RAM) at which a warning message is displayed if this value is exceeded.	Percentage	Numeric (0.1 to 100)
CLIENT.TERMINATION_LIMIT_MEMORY_UTILIZATION	The (% of Used Heap Memory to Total Heap Memory) or the (% Used RAM to Total RAM) at which the Java Client is terminated by the Master if this value is exceeded.	Percentage	Numeric (0.1 to 100)

For slow Java Clients due to slow network conditions, you should specify these parameters with values greater than zero:

- Client.SlowConnectionCheckInterval
- CLIENT.RESOURCE_POLLING_INTERVAL
- CLIENT.WARNING_LIMIT_QUEUE_SIZE
- CLIENT.TERMINATION_LIMIT_QUEUE_SIZE

For slow Java Clients with low memory issues, you should specify these parameters with values greater than zero:

- CLIENT.WARNING_LIMIT_MEMORY_UTILIZATION
- CLIENT.TERMINATION_LIMIT_MEMORY_UTILIZATION
- CLIENT.RESOURCE_POLLING_INTERVAL

Uninstalling the CWA Java Client

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

For UNIX systems, use **`install.sh -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).

7

Installing Fault Tolerance

The basic principle of fault tolerance is to keep your production schedule running continuously despite machine failures. If the machine managing your production schedule fails, fault tolerance ensures that another machine is available to assume control over the production schedule.

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.

This chapter covers:

Overview of Fault Tolerance

This section describes fault tolerance components, configuration, operational modes, and network configuration.

Fault Tolerance Components

Fault tolerance consists of the following main components:

- Client Manager – The Client Manager services requests from user initiated activities, such as through the CWA 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 CWA 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. *CWA* does *not* provide fault tolerance for the database.

Fault Tolerance Configuration

Fault tolerance has two configuration modes: auto mode and fixed mode.

Auto mode

Auto mode is the default way of configuring fault tolerance. 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, Fault Tolerance Operational Modes, page 102.

Fixed Mode

In fixed mode, if the Primary Master fails, the Backup Master assumes control just as with auto mode. However, in fixed 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.

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, page 116.

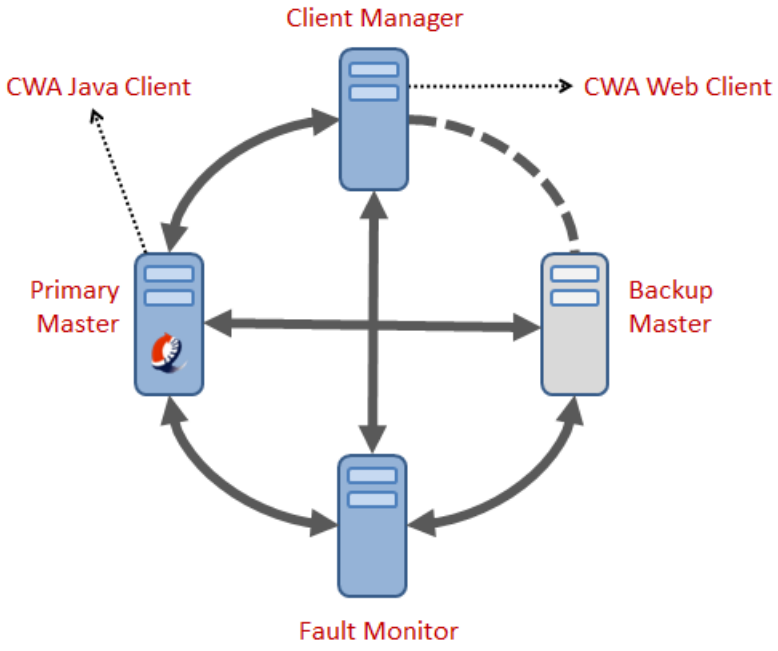
In the Unix installation procedure after providing a directory location for the installation files, a screen asks if you wish to install a Primary Master or Backup Master. You should install the Primary Master first. Complete the Primary Master installation and then repeat the Master installation on 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 CWA Master for Unix, page 51.

Fault Tolerance Operational Modes

Whenever the Primary Master is running while the Backup Master remains available to assume control, the system is in normal 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 in backup mode.

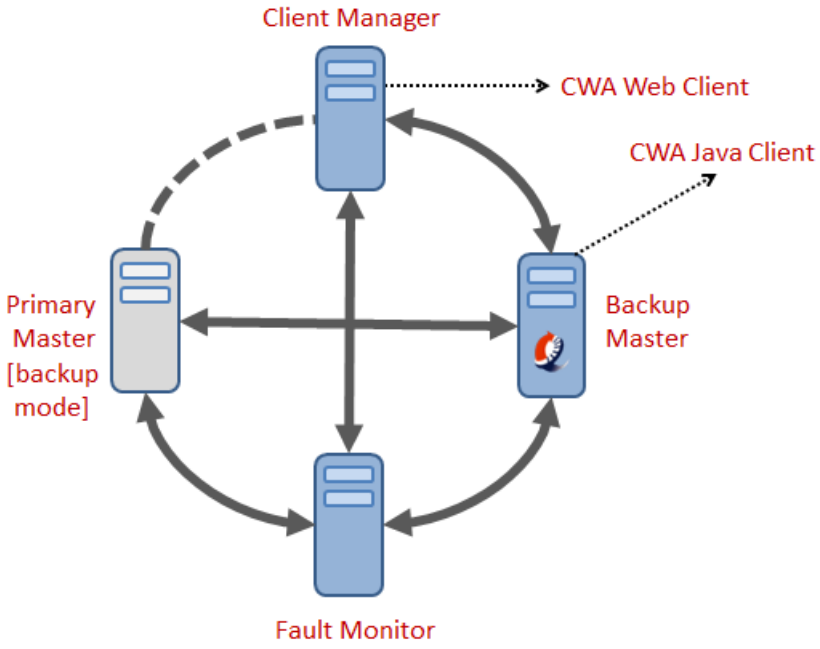
Normal (Standby) Mode

The diagram below shows normal operation, or the standby mode. The Backup Master remains in the background until required though maintaining constant communication with both the Primary Master and the Fault Monitor.



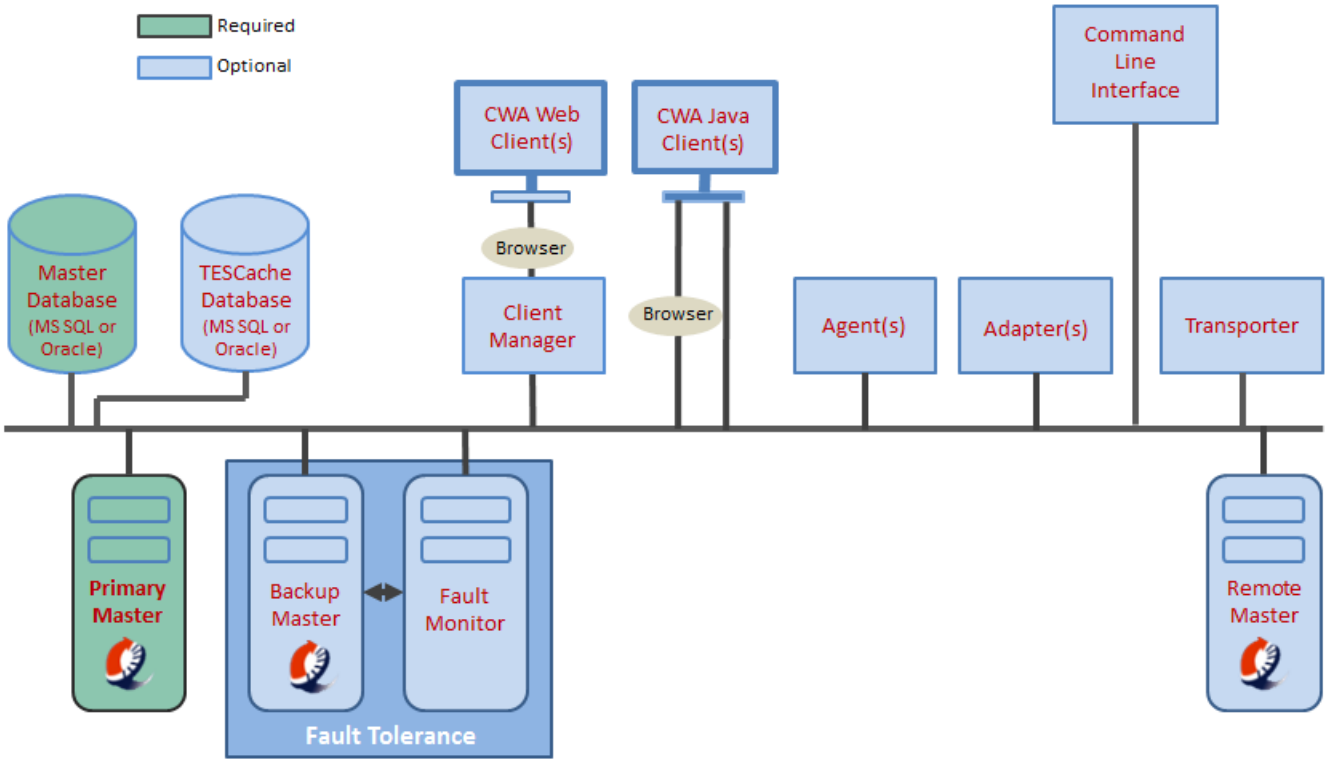
Backup Mode

The following diagram 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.



Fault Tolerance 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. The following diagram shows the network connections and the communication ports.



Installation Prerequisites

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 CWA System Requirements, page 13 in this guide for the system requirements for the Fault Monitor.

The information in this section applies to both Windows and Unix installations.

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

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.

Regulatory: 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.

Pre-Installation Requirements

Make sure that following conditions are 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 to serve as the Primary Master, the Backup Master, and the Fault Monitor. All three machines must be in the same domain.
- The Primary Master must be installed, licensed and operational.
- A 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.
- The Primary Master, Backup Master, and the Fault Monitor must have the same operating system (including patches).
- The Primary Master and the Backup Master must have the same database connectivity and hardware configuration. Their software and configuration should mirror the each other.
- Make sure that the primary and Backup Master machines can 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.
- 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 same version of JVM must be installed on the Primary Master, Backup Master and Fault Monitor machines.
- Obtain license files for your CWA fault tolerance components from the Cisco representative.
- Compile an installation check list as described in Installation Check List, page 106.

Installation Check List

Prior to installing fault tolerance, collect the following information about the machine components that is needed during the installation.

Primary Master:

Computer Name_____

Host Name_____

Backup Master:

Computer Name_____

Host Name_____

Fault Monitor:

Computer Name_____

Host Name_____

Client Manager:

Computer Name_____

Host Name_____

Admiral Database:

Computer Name_____

Host Name_____

TES Cache Database:

Computer Name_____

Host Name_____

Domain User Account_____

Fault Monitor:

Computer Name_____

Host Name_____

Port Numbers:

Fault monitor to Master (default=6703)_____

Master to Master (default=6704)_____

Fault monitor to client (default=6705)_____

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 CWA while the second Master is referred to as the Backup Master. This Backup Master, like the Primary Master, is controlled from the Service Manager. 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 **Master Status** pane in the CWA Web Client.

The fault tolerance setup consists of steps which must be performed in order. The procedures for each step are covered in these sections:

- Installing the Backup Master, page 107
- Installing the Fault Monitor on Windows, page 108
- Controlling the Fault Monitor, page 109

Note: Make sure that you have met the conditions in Pre-Installation Requirements, page 106 before starting installation.

Installing the Backup Master

To install the Backup Master:

1. Run the CWA *setup.exe*.
2. On the Internet Explorer-Security Warning dialog box, click **Run**.
3. On the Welcome panel, click **Next**.

4. On the Installation Type panel, select **Backup Master**, then click **Next**.
5. On the Destination Folder panel, select the directory where the CWA files will reside.
   - Click the **Change** button to search for a directory.

   -or-

   - Accept the default location C:\Program Files\TIDAL.
6. Click **Next**. The Database Type panel displays.
7. Select the type of database being used and click **Next**. The Database Server panel displays.
8. Enter the hostname of the Primary Master database, the port number of the JDBC driver, and if using Oracle, the SID used by the Primary Master.
9. Click **Next**. The Ready to Install the Program panel displays.
10. Click **Install**. The Installshield Wizard Complete panel displays.
11. Click **Finish** to close the wizard.

Installing the Fault Monitor on Windows

Regulatory: The Fault Monitor must be installed on a separate machine from the primary and Backup Masters.

To install the Fault Monitor on Windows:

1. Run the CWA *setup.exe*.
2. On the Internet Explorer–Security Warning dialog box, click **Run**.
3. On the Welcome panel, click **Next**.
4. On the Installation Type panel, select **FaultMonitor**, then click **Next**.

   The **Destination Folder** panel displays.
5. Select the directory where the CWA files will reside:
   - Click the **Change** button to search for a directory.

   -or-

   - Accept the default location *C:\Program Files*.
6. Click **Next**. The Enter requested data panel displays.
7. Enter the following:
   - FM Port –The port number on which the Primary Master and Backup Master connects to the Fault Monitor (by default, 6703).
   - Client Port – The port number on which the Client Manager connects to the Fault Monitor (by default, 6705).
8. Click **Next**. The Ready to Install the Program panel displays.
9. 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.
10. Click **Finish** to complete Fault Monitor installation and return to the CWA installation dialog box.

Controlling the Fault Monitor

You can monitor the Fault Monitor from the CWA 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 CWA 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:

1. From the Windows Start menu, and choose **Programs > Cisco Workload Automation > CWA Service Manager** to display the CWA Service Manager.
2. From the Service list, choose **SchedulerFaultMon**.
3. Click **Start**.

Stopping the Fault Monitor

To stop the Fault Monitor, use the following command:

1. From the Windows Start menu, and choose **Programs > Cisco Workload Automation > CWA Service Manager** to display the CWA Service Manager.
2. From the Service list, choose **SchedulerFaultMon**.
3. Click **Stop**.

Checking the Fault Monitor Status

To check the operation status of the Fault Monitor, use the following command:

1. On the Fault Monitor machine, click the Windows Start button and choose **Programs > Cisco Workload Automation > CWA Service Manager** to display the CWA Service Manager.
2. From the Service list, select **Fault Monitor**. At the bottom of the CWA Service Manager, the status of the selected service displays.

Installing Fault Tolerance for Unix

Installing fault tolerance on a network means adding another Master to shadow an existing Master. The first Master becomes the Primary Master in CWA while the second Master is referred to as the Backup Master. A network component that monitors the operation of the two Masters called the Fault Monitor is installed on a third machine.

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 CWA Web Client. For more information, refer to the Fault Monitor Interface, page 115.

The fault tolerance setup consists of steps which must be performed in order. The procedures for each step are covered in these sections:

- Installing the Backup Master, page 110

Note: Make sure that you have met the conditions in Pre-Installation Requirements, page 106 before starting installation.

Installing the Backup Master

Instructions for installing the Backup Master are the same instructions provided in Installing the CWA Master for Unix in this guide. 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.

Installing the Fault Monitor on Unix

Regulatory: 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 on Unix:

1. Copy *install.sh* to the target machine.
2. Change the permissions on the *install.sh* file in the directory to make the file executable:

   ```
   chmod 755 install.sh
   ```

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

   ```
   sh ./install.sh
   ```

   The **Introduction** panel displays.

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.
5. Accept the default location, **/opt**, where the CWA Fault Monitor files will reside.

   Note: You must use the default location shown above for the Fault Monitor files.

6. Click **Next**. The **Port Numbers** panel displays.
7. Enter the port number of the Fault Monitor Master Port and the Client Manager, then click **Next**. The **Pre-Installation Summary** panel displays the destination location selected for the Fault Monitor files.
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.

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

Verifying Successful Installation of the Fault Monitor

To 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 CWA 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 CWA 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
```

Configuring Fault Tolerance

Fault tolerance in CWA is configured on the Fault Tolerance tab in the System Configuration dialog box of the CWA Web Client. Messages about fault tolerance are displayed in both the Fault Monitor console and the CWA 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. Obtain the license code from the licensing manager at Cisco. Registering the license for Fault Tolerance is performed from the CWA Web Client or Java Client as described in Licensing Procedures, page 165.

Failover Configuration

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

Enabling Fault Tolerance

To enable fault tolerance:

1. Before enabling fault tolerance, stop the Backup Master.

   a. From the Windows Start menu, choose **Programs > Cisco Workload Automation > Scheduler > Master > Service Control Manager** to display the CWA 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.

2. In the CWA Web Client, choose **System Configuration** from the Activities main menu to display the System Configuration dialog box.
3. Select the Fault Tolerance tab.
4. Click the Enable Failover option to add the check mark and enable fault tolerance operation.
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:

1. Verify that Failover is enabled. See Enabling Fault Tolerance, page 111.
2. Close all Clients.
3. Stop the Client Manager, Masters, Primary and Backup, if running, via the Service Control Manager (Windows) or the command line (Unix).
4. Verify that the Fault Monitor is running.
5. Start the Primary Master and verify that it is running via the Service Control Manager (Windows) or the command line (Unix).
6. Start the Backup Master and verify it is running via the Service Control Manager (Windows) or the command line (Unix).
7. Start the Client Manager via the Service Control Manager (Windows) or the command line (Unix).
8. Log into the application via the CWA Web Client and choose **Operations > Master Status**.
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, page 112 for more information on the options used to configure fault tolerance.

Verifying Fault Tolerance Operation

To verify fault tolerance operation:

1. Launch the CWA Web Client and from the Navigator pane, select **Operations > Fault Monitor** to display the Fault Monitor pane.
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:

1. Locate the *master.props* file in the **config** directory where you installed the Fault Monitor files on the Fault Monitor machine.
2. Open the *master.props* file in a text editor.
3. On a separate line in the file, enter:

   ```
   ToleranceTime=<number of minutes>
   ```

   where <number of minutes> is replaced with the number of minutes to pass without contact with the Primary Master before failover to the Backup Master.
4. Stop the Fault Monitor.
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 CWA 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 CWA Web Client. If you change the port number in one place, you must manually change the port number in the other place.
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:

1. On the Fault Monitor machine, locate *config* > *master.props*.
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.
3. Start the Client Manager.
4. Change the port number to a port number not in use by any other application.
5. Stop the Fault Monitor.
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 CWA 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 CWA in Fault Tolerant Mode

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

To stop CWA in Fault Tolerant mode:

1. Stop all fault tolerance components from the Navigator pane of the CWA Web Client by selecting **Operations > Fault Monitor** to display the Fault Monitor pane.
2. Right-click the Fault Monitor pane and from the displayed context menu, choose **Stop All**.

Starting CWA 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 CWA in Fault Tolerant mode:

1. On the Fault Monitor machine, verify that the Fault Monitor is running.
2. Start the Primary Master.
3. Start the Backup Master.
4. Launch the CWA 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.

1. From the Fault Monitor machine, verify that the Fault Monitor is running.
2. If the Primary Master is not running, start it.
3. Stop the Backup Master.
4. The Primary Master will leave standby mode and assume control.
5. Start the Backup Master.
6. Launch the CWA 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.

8

Installing Agents

An agent is a separate installation component of Cisco Workload Automation 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 including Windows, Unix, z/OS, MPE/iX, and OpenVMS environments. Check with your sales representative for the current list of the types of agents available.

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.

This chapter describes how to install and configure agents:

See these standalone guides for installation, configuration, and usage for these Agents:

- *Cisco Workload Automation HP OMU Agent Guide*
- *Cisco Workload Automation MPE/iX Agent Guide*
- *Cisco Workload Automation OpenVMS Agent Guide*
- *Cisco Workload Automation z/OS Agent and Gateway Adapter Guide*

About Agents

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

In the basic CWA 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 CWA 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.

Platform Support for Agents

CWA provides agents for Windows, Unix, z/OS, MPE/iX, and OpenVMS environments. The platform support for agents is documented in *Cisco Workload Automation Product Compatibility Guide* which is provided with the CWA documentation on cisco.com at:

http://www.cisco.com/c/en/us/support/cloud-systems-management/tidal-enterprise-scheduler/products-documentation-roadmaps-list.htm

Agent-specific documentation is provided for these agents:

- MPE/iX
- OpenVMS
- z/OS

Go to this link:

http://www.cisco.com/c/en/us/td/docs/net_mgmt/datacenter_mgmt/Tidal_Enterprise_Scheduler/6-2-3/documentation/overview/Cisco_TES_6-2-1_SP3_Documentation_Overview.html

to access to all agent and adapter documentation.

Regulatory: 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.

Rights for Installing and Running Agents

The rights need to install and run agents are summarized in this table:

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 and Configuring Windows Agents

This section describes how to install, configure, and run an agent on Windows in these topics:

- Windows Server 2012 .NET Requirement, page 121
- Installing an Agent on Windows, page 121

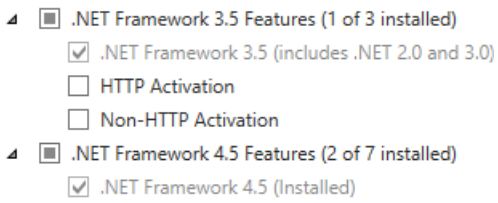
Windows Server 2012 .NET Requirement

The Windows Agent installation requires .NET 2.0. With Windows Server 2012, .NET 4.5 is installed by default. .NET 2.0 is an optional component that must be explicitly configured as part of .NET 3.5. Follow the steps below to install the required .NET 2.0 for the Windows Agent.

Note: On the Windows Server 2012, .NET is installed by default as a Windows feature and it does not show up as an option in the Control Panel Add/Remove programs user interface.

To configure .NET 3.5 (including .NET 2.0) for the Windows Agent:

1. Open the Add Roles and Features Wizard.
2. Select both " .NET Framework 3.5 Features" and " .NET Framework 3.5 (includes .NET 2.0 and 3.0)" as shown here:



3. Apply your changes.

Installing an Agent on Windows

To install an agent:

1. Download and extract the **Cisco Workload Automation Agent for Windows** software.
2. Double-click the *Agent_windows_TIDAL Agent.msi* file. The Security Warning dialog box displays.
3. Click **Run**. The Status panel displays.

   The **Welcome to the CWA Agent Setup** 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.
4. Click **Next**. The **Destination Folder** panel displays.
5. Select the directory where the CWA files will reside:
   - Click **Change** and select the appropriate file.

   -or-

   - Accept the default location at *C:\Program Files (x86)\TIDAL*.

6. Click **Next**. The **Agent Port Number** panel displays.
7. Enter the port number that the agent will listen on. The default port is **5912**.
8. Click **Next**. The **Ready to Install the Program** panel displays.
9. 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.
10. Click **Finish**.

Verifying the Installation

To verify installation:

1. From the Windows Start menu, choose **All Programs > Cisco Workload Automation > CWA Service Manager** to display the CWA Service Manager.
2. From the Services list, choose **AGENT_1**.

   If the CWA 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.

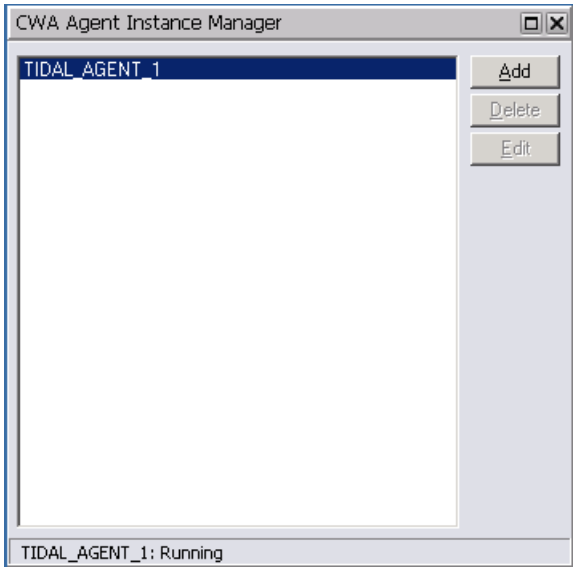
Configuring Agents on Windows

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

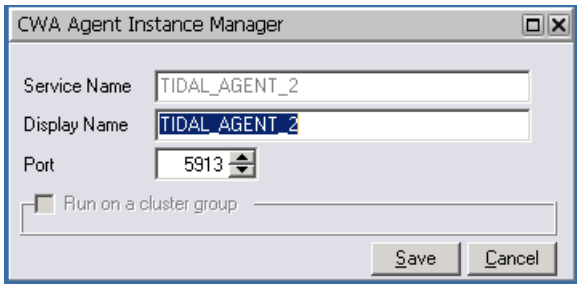
Adding Agent Instances

To add an instance:

1. From the Windows Start menu, choose **Programs > Cisco Workload Automation > Agent > Instance Manager** to display the Instance Manager.



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



3. Enter the following:

   - **Service Name** – The name of the agent service. The name in this field is automatically generated and cannot be edited.
   - **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. By default, the TIDAL_AGENT_1 port is 5912. When you add additional agents, the port increments by 1 by default.
   - **Run on a cluster group** – Enabled if this agent instance is on a node that is configured for a cluster with an existing agent service. If the node is not part of a cluster, this option is unavailable. See Configuring the Windows Agent for a Cluster, page 131.

4. Click **Save**.

Note: To connect to the agent you just added, see Defining an Agent Connection, page 144.

Editing Agent Instances

You can modify the port number and the name of the instance that is displayed but the service name cannot be changed.

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

To edit an instance:

1. Stop the agent.
   a. From the Windows Start menu, choose **All Programs > Cisco Workload Automation > CWA Service Manager** to display the CWA Service Manager.
   b. From the Services list, choose **TIDAL_AGENT_<#>**.
   c. Click **Stop**.
2. From the Windows Start menu, choose **Programs > Cisco Workload Automation > Agent > Instance Manager** to display the Instance Manager.
3. Select the instance.
4. Click **Edit**. The Edit dialog box displays.
5. Make the necessary edits, then click **Save**. The Information dialog box displays.
6. Click **OK**.
7. Re-start the agent.
   a. From the Windows Start menu, choose **All Programs > Cisco Workload Automation > CWA Service Manager** to display the CWA Service Manager.
   b. From the Services list, choose **TIDAL_AGENT_<#>**.
   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:

1. Stop the agent.
   a. From the Windows Start menu, choose **All Programs > Cisco Workload Automation > CWA Service Manager** to display the CWA Service Manager.
   b. From the Services list, choose **TIDAL_AGENT_<#>**.
   c. Click **Stop**.
2. Fromthe Windows Start menu, choose **Programs > Cisco Workload Automation > Agent > Instance Manager** to display the Instance Manager.
3. Select the instance.
4. Click **Delete**. A confirmation message displays.
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 Unix Agents Using the Command Line, page 143.

Note: To delete an agent through the client, see Defining an Agent Connection, page 144.

Configuring an Agent 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 CWA Services Manager as discussed in Verifying the Installation, page 122.

To configure an agent for Windows:

1. From the Windows Start menu, choose **Settings > Control Panel**.
2. Double-click **Administrative Tools**.
3. Double-click **Services**.
4. Double-click the agent you just installed.
5. On the **General** tab of the AGENT Properties dialog box, click **Stop** to stop the service.
6. On the **Log On** tab, select **This Account**.
7. Enter the requested information in the User Name/Domain Name and Password fields, then click **OK**.
8. Right-click the agent and choose **Start**.

   -or-

   On the **General** tab, click **Start** to restart the agent.
9. Close the Services and Administrative Tools dialog boxes.
10. Go to the client and follow the procedure detailed in Configuring an Agent for Windows, page 125 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 (x86)\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.

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

Cisco Workload Automation 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 on Windows

To start or stop an agent:

1. From the Windows Start menu, choose **All Programs > Cisco Workload Automation > CWA Service Manager** to display the CWA Service Manager.
2. From the Services list, choose the name of the agent.
3. Click **Start** to start the agent.

   -or-

   Click **Stop** to stop the agent.

Checking Agent Status

To check the status of an agent:

1. From the Windows Start menu, choose **All Programs > Cisco Workload Automation > CWA Service Manager** to display the CWA Service Manager.
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:

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**.
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\...
3. Right-click the TIDAL_AGENT_1 key and choose **New > String Value** from the resulting menu.
4. Name the new key that is created on the right pane, JobLaunchMode.
5. Right-click the new JobLaunchMode key and select the Modify option from the context menu to display the Edit String dialog box.
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:

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**.
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\...
3. Right-click the TIDAL_AGENT_1 key, then choose **New > String Value** from the resulting menu.
4. Name the new key that is created on the right pane, JobUseDefDesktop.
5. Right-click the new **JobUseDefDesktop** key and choose **Modify** from the context menu to display the Edit String dialog box.
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:

1. From the Windows Start menu, choose **All Programs > Cisco Workload Automation > CWA Service Manager** to display the CWA Service Manager.
2. Click the ellipsis button to display the Service Configuration dialog box.
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
```

4. Click **OK**.
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 Steps 4 and 5 below.

To create a self-signed host certificate and configure it to a port:

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**.
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.
3. Start Microsoft Management Console (mmc) and copy the certifcate "local" located in *Personal > Certificates* into *Trusted Root Certification Authorities > Certificates*.
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.

5. Click **OK**.

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 CWA.

Prerequisites

Before installing the 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 *Cisco Workload Automation Compatibility Guide*.
- 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 Windows Agent 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:

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.

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.

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.

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 and Configuring Windows Agents, page 120. 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.

5. From the Windows Start menu, choose **Programs > Cisco Workload Automation > Agent > Instance Manager** to display the Agent Instance Manager.

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, 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.

7. Select the **Run on a cluster group** option to expand the screen to display the cluster configuration fields.

8. In the **Cluster Group field**, select which cluster group that this agent instance belongs to.

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.

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.

11. In the Cluster Nodes field, select which node this agent instance is on. When the fields are completed, click the **Save** button.

12. Go to each node and repeat this procedure for each agent instance.

13. When each agent instance on each node is configured properly, start each clustered agent instance from its active node using the CWA Service Control Manager. Starting the agent instance in the Service Control Manager automatically starts the agent resource in the Windows Cluster Administrator.

Uninstalling Agents on Windows

To uninstall the agent, you must use the **Add/Remove Programs** utility in the Windows Control Panel.

To uninstall an agent:

1. Close the CWA client to begin the uninstallation process.
2. From the Windows Start menu, choose **Settings>Control Panel**, then double-click **Add or Remove Programs**.
3. Scroll down the list of programs installed on the machine to the CWA program.
4. Click the CWA program to highlight it.
5. Click **Remove** to start the uninstallation process.
6. When prompted to confirm that you want to uninstall the program, click **OK**.
7. Click **Finish** to end the uninstallation process.
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 CWA 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 and Configuring Unix Agents

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

In the basic CWA 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 CWA 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.

Installing a Unix Agent from the Command Line

Before installing the CWA 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:

Note: While the installer must be run as the root user, the user who has to run the agent service must have read access to the directory in which the agent has to be installed into (/opt, by default).

1. Download the **Cisco Workload Automation Agent for Linux/Unix** software.
2. Login as root.
3. Copy the *install.sh* and *install.tar* files to your temp directory.

   Note: Do not unpack the install.tar file. The file will automatically unpack during the installation process
4. Change the permissions on the *install.sh* file in the directory to make the file executable:

```
chmod 554 install.sh install.tar
```

5. Begin the installation by entering:

   ```
   ./install.sh
   ```

   An introduction screen displays as the installation program begins.

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.

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.

8. Press **Enter**. The Select the Location screen displays.

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.

10. Type **1** to select the Add Instance option, then press **Enter.** The Select the Location for the Agent Files screen displays.

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)

12. Press **Enter**. A confirmation summary screen displays the information that you entered.

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 on Unix

You can configure Unix agents (add and delete agent instances) using the **Agent Configuration Menu**.

Note: While the installer must be run as the root user, the user who has to run the agent service must have read access to the directory in which the agent has to be installed into (/opt, by default).

To display this menu:

1. Log on as agent owner on the agent machine.

2. Go to the *bin* directory by entering:

   ```
   cd /opt/TIDAL/Agent/bin
   ```

3. Type in the following:

```
./tagent config
```

The **Agent Configuration Menu** displays.

Adding Agent Instances

To add an instance:

1. In the Agent Configuration Menu enter **1 a**nd press **Enter**.
2. Enter the name of the agent, its port number and the directory path to the Java binaries and then press **Enter**.
3. Enter **Y** and press **Enter**. An agent instance is added.
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:

1. Stop the agent.
2. In the Agent Configuration Menu enter **3** and press **Enter**. The Select Agent Instance to Delete panel displays.
3. Type the number of the instance to delete.
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

Cisco Workload Automation 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 on Unix

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.

Checking Agent Status

To check the agent status on Unix:

1. Run this command:

   ```
   ./tagent <agent name> status
   ```

Preventing Unauthorized Use of a Unix 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 a Unix agent:

1. Login as the owner of the agent.
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.
3. Change the *Users.cfg* file permissions to limit access to just the agent owner, by entering:

   ```
   chmod 700 Users.cfg
   ```
4. In the *Users.cfg* file, enter:

   ```
   EXCLUDE
   ```
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.

6. To ensure that the changes take effect, stop and restart the agent.

   -or-

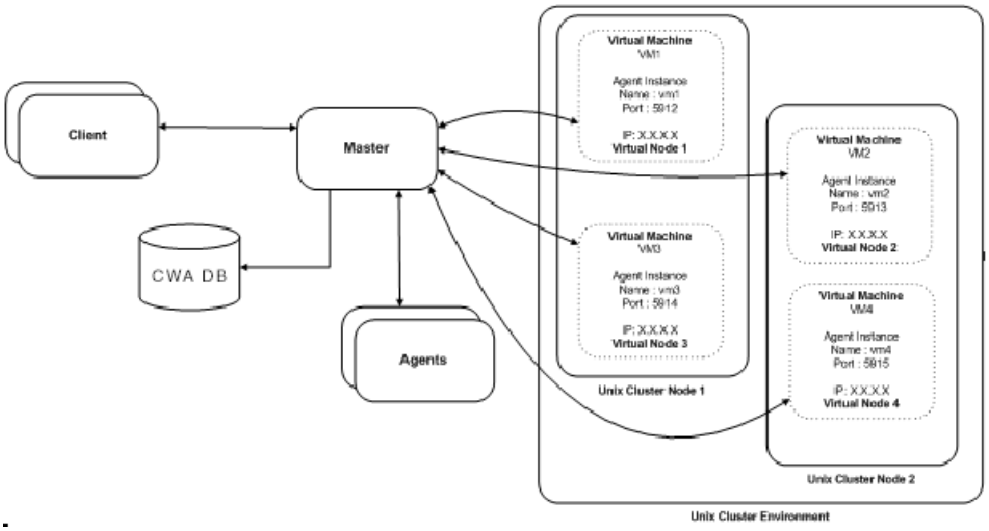
   Disconnect and reconnect the client connection to the agent.

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.

Configuring a Cluster to Run the Unix Agent

The Agent for Unix can run in a Unix cluster environment.

The following diagram illustrates how Cisco Workload Automation is configured in an environment with Unix cluster:



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 Master to maintain the agent connection when the cluster management software moves the virtual machine to another participating node.

Prerequisites

To configure the CWA 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 CWA agent must be met on each of the individual nodes.
- The installation and configuration of CWA 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 CWA 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:

1. FTP the agent installation files to one of the participating nodes in the cluster.
2. Login as root to the same physical node where the agent installation files were copied.
3. Change to the directory where the agent installation files were copied.
4. Follow the normal Agent installation procedure that is described in the Installing and Configuring Windows Agents, page 120 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:

1. Identify each of the Virtual Machines that require an agent instance associated with it.
2. Login to a cluster node as the agent owner.
3. Change to the agent *bin* directory and run the t**agent –config** command to begin the agent configuration.
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.

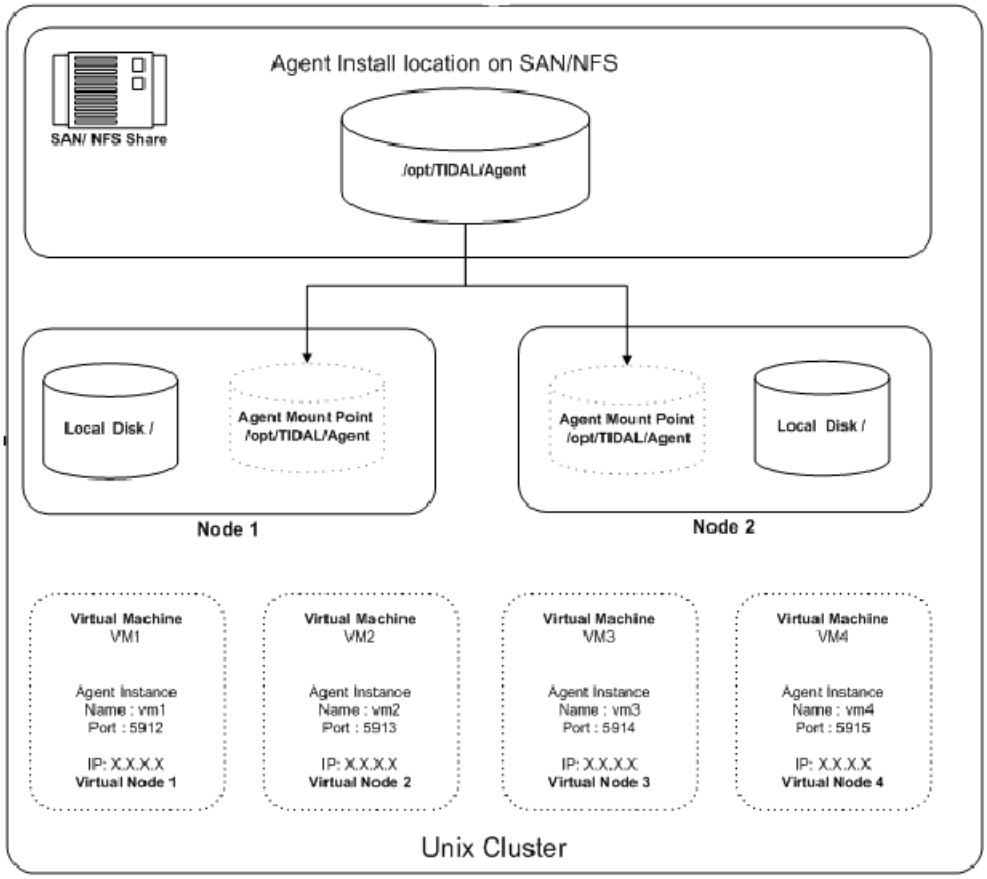
Configure CWA to Connect to Agent Instances on a Virtual Machine

Configuring the connection to the Agent instances in the CWA 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.

Unix Cluster



Uninstalling Unix Agents Using the Command Line

The uninstallation procedure will not be successful if the agent is running. Stop the agent before removing the CWA Agent for Unix.

To uninstall:

1. Check the status of the agent to verify that it is not running by entering:

   ```
   ./tagent <agent name> status
   ```

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
   ```

3. Once the agent is stopped, return to the location where you installed the Unix agent. By default, this location is the */opt* directory.
4. At the command prompt, enter:

   ```
   cd /opt
   ```

5. Have your Unix administrator remove the agent directory and its contents

Connections and Agent Procedures in CWA

The procedures described in this section are performed in the CWA Console.

Defining an Agent Connection

To define a connection between the agent and the Master:

1. From the Navigator pane of the CWA client, choose **Administration > Connections**.

   The Connections pane displays.

2. Click the Add button on the CWA toolbar.

   -or-

   Right-click in the Connections pane and choose **Add Connection**, then choose the **Agent for Windows** or **Agent for Unix** option from the menu.

   The Connection Definition dialog box displays.

3. Enter a name for the agent you installed.

   Note: This name does not have to match the machine name or instance name.

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.

5. Select the Enabled option.
6. On the Connection tab, configure:

   - Machine Name – The name or IP address of the machine that the agent is installed on. This name must be a valid DNS name.
   - Master-to-Agent Communication Port – The agent's listener port number specified when installing the agent.

7. 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:

1. From the Connections pane, select the agent to delete.
2. Click the **Delete** button on the CWA 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:

1. From the Navigator pane, choose **Administration > Connections** to display the Connections pane.
2. Double-click the agent.

   -or-

   Select the agent and click the **Edit** button on the CWA toolbar.
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.
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:

1. From the Navigator pane, choose **Administration > Connections** to display the Connections pane with the licensed computers.
2. Double-click the agent to edit or select the agent and click the **Edit** button on the CWA toolbar to display the agent's connection definition.
3. Select the General tab if it is not showing.
4. In the Job Limit field on the General tab, change the job limit to the desired value.
5. Click **OK**

Changing the Name of the Computer Displayed in CWA

To change the name of the computer:

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.
2. In the Name field, change the computer's name. This name is used when referring to the computer on CWA panes and dialog boxes.
3. Click **OK**.

Changing the Machine Hostname of the Computer

To change the hostname of the computer:

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.
2. Select the Connection tab.
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.

Agent/Master Secure Connection

In order to provide strict control over which Cisco Workload Automation 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 CWA Masters to which a CWA Agent will create connections.

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 32-bit Windows

  ```
  C:\Program Files\TIDAL\Agent\TIDAL_AGENT_1
  ```

- For 64-bit Windows

  ```
  C:\Program Files(x86)\TIDAL\Agent\TIDAL_AGENT_1
  ```

- For Unix (Linux, z/OS)

  ```
  /opt/TIDAL/Agent/TidalAgent1
  ```

- 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.

Here 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 Agent Issues

When the Agent for Windows or 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 is operating before they can track down the source of the problem. Before contacting Technical Services about an agent issue, you should verify the agent version and turn on diagnostic logging to collect information about the way the agent is functioning. These are the first steps that Technical Services will have you do, if you have not done it before contacting them.

Troubleshooting a Unix Agent that Fails to Start

If your Unix agent fails to start or hangs on the following message:

```
TIDAL Agent for UNIX
Starting agent testagent on port 5912
Opening Connection......
```

...there might be no logs to troubleshoot. Typically, this problem is caused by an IP address mismatch. Follow the procedure below to check the IP address definitions.

To troubleshoot a Unix agent that fails to start or hangs

1. Check the IP of the agent server and how it is configured.
2. Run **ifconfig**.
3. Compare the system IP returned from **ifconfig** to the system's IP defined in the file **/etc/hosts**.
4. If there's a mismatch, you need to fix it so that the IP addresses match.

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:

1. From the Navigator pane of the client, choose **Administration > Connections** to display the Connections pane.
2. In the various connections listed in the pane, locate the agent with the problem.
3. Look in the Version column of that agent to see the version of the agent being used.

Configuring Diagnostics for a Windows Agent

To run diagnostics for the Windows agent:

1. Login to the agent console as an authorized user.
2. Using Service Manager, select the Agent that you wish to use diagnose.
3. Add the following string to the end of the **Path:** field.

   ```
   Debug=high
   ```

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.

Configuring Diagnostics for a 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.

To turn on diagnostic logging:

1. On the agent machine type the following command to stop the agent:

   ```
   ./tagent <agent name> stop
   ```

2. Go to the */bin* directory and locate the *tagent.ini* file for the desired agent.

3. Inside the *tagent.ini* file, under the port setting, type the following:

   ```
   ovb=Tidaldebug
   ```

4. Save the file and its changes.

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.

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
   ```

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.

Raising the Logging Levels for Windows and Unix Agents

To raise the logging level for a Windows Agent:

1. Open the CWA Service Manager on the agent machine.
2. Select the agent in the dropdown.
3. Click on the dots [...].
4. In the Service tab, change the path to include the DEBUG option to read " DEBUG=HIGH"
5. Click OK to save changes.
6. Restart the agent.

To raise the logging level for a Unix Agent:

1. Go to the agent machine and go to the directory where the agent is installed.
2. Go to " Bin/" and edit " tagent.ini" .
3. Under " [config]" put " ovb=tidaldebug" .
4. Restart the agent.

DataMover Job Support

Note: DataMover jobs are only supported on Unix/Linux agents.

By default, when the 3.2 agent is installed, it can run with Java 1.8 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. Both AS3 and HFS functionalities require Java 1.8.

There are new subdirectories in 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 1.8 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 Java 1.8 version.

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 1.8 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 1.8 or the default Java must be 1.8. 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.

Hortonworks Hadoop

Download the Hortonworks Hadoop client libraries and copy into the Agent/lib directory. See Installing the Hadoop Client Libraries, page 152 for how to obtain and install the libraries.

Cloudera Hadoop

Download the Cloudera Hadoop client libraries and copy into the Agent/lib directory. See Installing the Hadoop Client Libraries, page 152 for how to obtain and install the libraries.

MapR Hadoop

In order to use DataMover for MapR Hadoop, the MapR Client must be installed on the machine running the CWA agent. The CWA 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, page 151 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.

Installing the Hadoop Client Libraries

Hadoop client libraries are required for processing the Hadoop-related DataMover, Hive, MapReduce, and Sqoop jobs. As of CWA 6.3.2, Hadoop libraries are not included with CWA. Instead, we provide a Maven script (POM.xml) to install the required libraries.

If you do not already have Maven, you must download and install it. Obtain the POM.xml file from the folder/directory named "Hadoop" in the CD and run the file script to download the required Hadoop client libraries. Instructions for obtaining Maven and downloading the Hadoop libraries are included in these sections:

- Installing Maven, page 152
- Downloading the Hadoop Client Library, page 152

Note: The instructions here are for Windows.

Installing Maven

If you do not have Maven installed, follow the instructions below.

Maven Prerequisites

- JDK must be installed.
- The JAVA_HOME environment variable must be set and point to your JDK.

To download and install Maven:

1. Download maven 3 or above from https://maven.apache.org/download.cgi.
2. Unzip apache-maven-<3 or above>-bin.zip.
3. Add the bin directory of the created directory (for example, apache-maven-3.3.9) to the PATH environment variable
4. Confirm a successful Maven installation by running the **mvn -v** command in a new shell. The result should look similar to this:

```
C:\Users\subrchan\Desktop>mvn -v
Apache Maven 3.3.9 (bb52d8502b132ec0a5a3f4c09453c07478323dc5; 2015-11-10T22:11:47+05:30)
Maven home: C:\vinoth\software\apache-maven-3.3.9-bin\apache-maven-3.3.9
Java version: 1.7.0_79, vendor: Oracle Corporation
Java home: C:\Program Files\Java\jdk1.7.0_79\jre
Default locale: en_US, platform encoding: Cp1252
OS name: "windows 7", version: "6.1", arch: "amd64", family: "windows"
```

Downloading the Hadoop Client Library

With Maven installed, you can now download the Hadoop client library. Maven scripts (POM.xml) are provided for the following distributions of Hadoop:

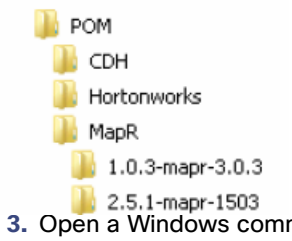
Hadoop Distribution Type	Versions
Cloudera	CDH5
Hortonworks	HDP 2.4.x
MapR	5.1.0

Note: The *Cisco Workload Automation Compatibility Guide* contains the most current version information.

To download and install the Hadoop client library

1. Download the POM.zip file. This file is provided in the /Hadoop directory in the CWA 6.3.2 distribution package.
2. Unzip the POM.zip.

   The POM xml files needed by Maven are saved in the directory structure shown here:



3. Open a Windows command prompt and navigate to the directory for the Hadoop distribution in which you are interested. For example, navigate to the CDH directory if you want to download Hadoop client libraries for Cloudera.
4. Edit the POM.xml file to mention exact versions of MapR, Hadoop, Hive, and Sqoop that you are using. For example, for Cloudera the required properties could be edited as shown below:

   ```
   <properties>
   <Hadoop.version>2.6.0-cdh5.6.0</Hadoop.version>
   <Hive.version>1.1.0-cdh5.7.0</Hive.version>
   <Sqoop.version>1.4.6-cdh5.6.0</Sqoop.version>
   </properties>
   ```

   For MapR it is also necessary to mention the version of MapR used, as shown in the following example:

   ```
   <properties>
   <Hadoop.version>2.7.0-mapr-1602</Hadoop.version>
   <Hive.version>1.2.0-mapr-1605</Hive.version>
   <Sqoop.version>1.4.6-mapr-1601</Sqoop.version>
   <Mapr.version>5.1.0-mapr</Mapr.version>
   </properties>
   ```

5. From the directory containing the Hadoop distribution you want, execute this command:

   ```
   mvn dependency:copy-dependencies -DoutputDirectory=<directory to which you want to download the
   jars>
   ```

   For example, running the following command from the CDH directory:

   ```
   mvn dependency:copy-dependencies -DoutputDirectory=C:\CDHlib
   ```

   would insert the Cloudera Hadoop client libraries to the “C:\CDHlib” directory.

9

Installing Adapters

Generally, the adapters are installed as part of the base Master installation. This chapter lists the supported CWA adapters, describes how to license them, and provides CWA configuration information in:

Supported Adapters

Here is a list of adapters that are supported for CWA 6.3.2. Note that a few adapters that were previously available have been discontinued. See the *Cisco Workload Automation Compatibility Guide* for exact versions.

Note: See online Help in the CWA Client for documentation about using the adapters.

In addition, all documentation for each adapter (configuration and usage) is provided in adapter-specific PDF documents for your convenience. These are available on cisco.com.

- Amazon EC2
- Amazon S3
- BusinessObjects
- BusinessObjects BI Platform
- BusinessObjects Data Service
- Cognos
- Email
- Hive
- HP OMU
- Informatica
- JDBC
- JD Edwards
- JMS
- MapReduce

- SAP
- Sqoop
- SSH
- UCS Manager
- VMware
- Web Service
- z/OS

Licensing an Adapter

Each Cisco Workload Automation connection to an adapter server must be licensed. You cannot create a connection to an adapter until you apply the adapter license file. If you purchase the adapter after the original installation of Cisco Workload Automation, you will receive a new license file authorizing the use of the adapter. All licenses are controlled by the Master server.

You use the same procedure to license an adapter as you do to apply a permanent license as described in Applying a Permanent License, page 166.

General Adapter Configuration in CWA

The **service.props** file is used to configure adapter behavior. **service.props** is located in the \config directory located under the Adapter's GUID directory, You can create both the directory and file if it does not yet exist.

The table below lists many of the parameters that can be specified in service.props. Some properties apply to all adapters (shaded in the table) and some properties are adapter-specific as indicated by the **Applicable Adapter(s)** column. The properties are listed in alphabetical order.

Property	Applicable Adapter(s)	Default	What It Controls
BYPASS_SEC_VALIDATION	Oracle Apps	N	If set to Y, the secondary user validation is bypassed. If not, secondary user validation is performed.
CLASSPATH	All	<none>	(Optional) – The path to the JDBC driver. If the default CLASSPATH used when the Adapter process is started does not include an appropriate JDBC driver jar required to connect to the PowerCenter Repository Database, you will need to specify this *service.props* configuration
CONN_SYNC	All	N	Setting this flag to Y allows synchronous connections without overloading the RDOnly Thread. If set to N, the adapter might stop trying to reconnect after an outage or downtime.
DISCONN_ON_LOSTCONN	Informatica	N	Setting this flag to Y avoids an unnecessary logout call to the Informatica server when the connection is lost. This logout call usually hangs.

Property	Applicable Adapter(s)	Default	What It Controls
EnableDynamicPollingInterval	All	N	Use to avoid frequent polling on long-running jobs. When set to Y in service.props of a particular adapter, these properties are enabled: MinDynamicPollInterval–Minimum value should be 5 seconds. MaxDynamicPollIntervalInMin–Maximum value should be 5 minutes. PercentOfEstDuration–Default value is 5.
IGNORE_CODES	Informatica	<none>	This parameter can be set in service.props, job configuration and connection configuration parameters. The order of precedence is service.props (applicable for all jobs running in all connections), job level (only for that particular job), and connection (applicable for all jobs in the connection). This parameter is used to specify Informatica-specific error codes, separated by commas (,), that you want to ignore while running a job.
IGNORESUBREQ	Oracle Apps	N	Y or N. Setting this flag to Y stops huge job xml file transfers back and forth between the adapter and the AdapterHost during polls when a single request set has multiple sub-requests of more than 100. The default value is N or empty.
kerbrealm	MapReduce	<none>	If the Hadoop cluster is Kerberos secured, use this value to specify the Kerberos Realm. For example, **`kerbrealm=TIDALSOFT.LOCAL`**
kerbkdc	MapReduce	<none>	If the Hadoop cluster is Kerberos secured, use this value to specify the KDC Server. For example, **`kerbkdc=172.25.6.112`**
Keystore	BusinessObjects, BusinessObjects BI, BusinessObjects DS, Cognos, JD Edwards, Oracle Applications, UCS Manager, VMware, Web Service	<none>	Specify `Keystore=c:\\<adapter_certificate_directory>\\<your_trusted_keystore>.keystore` when importing certificates into a Java keystore.

Property	Applicable Adapter(s)	Default	What It Controls
LAUNCH_DELAY (in milliseconds)	Informatica	<none>	This parameter can be set in service.props, job configuration and connection configuration parameters. The order of precedence is service.props (applicable for all jobs running in all connections), job level (only for that particular job), and connection (applicable for all jobs in the connection). If a non-zero value is set for this parameter, then the jobs are delayed for the specified number of milliseconds before being submitted to Informatica.
LoginConfig	BusinessObjects BI Platform, BusinessObjects Data Services	<none>	Specifies the location of the login configuration if using WinAD or LDAP authentication. For example: LoginConfig=c:\\windows\\bscLogin.conf where "`c:\\windows\\bscLogin.conf`" is the location of the login configuration information. Note the use of \\ if this is a Windows location.
MaxLogFiles	Informatica, JDBC	50	(Optional) – Number of logs to retain. Defaults to 50 if not specified.
OUTPUT_ASYNC_LOGOUT	Informatica	N	Setting this flag to Y avoids jobs getting stuck in Gathering Output status.
OUTPUT_SYNC	All	Y	Enables concurrent output gathering on a connection. To enable this feature, set the value to N in service.props of this adapter.
POLL_SYNC	All	Y	Enables concurrent polling on connections of the same type. This is helpful when there is a heavily load on one connection of an adapter. The heavily loaded connection will not affect the other adapter connection. To enable this feature, set the value to N in the service.props of this adapter.
QUERY_TIMEOUT	Oracle Apps	N	Y or N. If set to Y, the timeout value defined using the parameter QUERY_TIMEOUT_VALUE is applied to the SQL queries. Default value is N or empty.
QUERY_TIMEOUT_VALUE	Oracle Apps	unset	The time period in seconds that SQL queries wait before timeout. If 0 or not set, there is no timeout.
READPCHAINLOG	SAP	Y	Used to control the log gathering in SAP Process Chain jobs. This property depends on the Summary Only check box of the job definition Options tab.
SCANFOR_SESSIONSTATS	Informatica	Y	Y or N – Set this parameter to N to turn off the default behavior of Informatica jobs collecting the session statistics during the job run.
SCANFOR_SESSIONSTATS_AFTER_WF_ENDS	Informatica	N	Y or N – Set this parameter to Y to turn off the gathering of session statistics during each poll for the status of Informatica jobs.
TDLINFA_LOCALE	Informatica	<none>	Points to the Load Manager Library locale directory. See "Configuring the Informatica Adapter" in the *Informatica Adapter Guide* for how to set this for Windows and Unix environments.

Property	Applicable Adapter(s)	Default	What It Controls
TDLJDBC_LIBPATH	JDBC (Windows only, optional)	<none>	An alternate path to the JDBC library files. The library file path should have been configured given system environment variables. This option is available in case you wish to use an alternate set of libraries and may be helpful for trouble-shooting purposes.
TDLJDBC_LOCALE	JDBC	<none>	The path to the JDBC locale files.
TDLINFA_REQUESTTIMEOUT	Informatica	<none>	(Optional) – The number of seconds before an API request times out. The default is 120 seconds, if not specified.
TRANSACTION_LOG_BATCH_SIZE	MS SQL	5000	Set this parameter if more than 5000 lines need to be read from the transaction table.
version_pre898	JD Edwards	N	If running on a JD Edwards server version that is less than 8.9.8, set version_pre898=Y.

10
Versions

This chapter describes how to determining your version and apply new service packs and hot fixes:

Upgrading from Java 7 to Java 8

Customers upgrading from Java 7 to Java 8 must update the JAVA_HOME parameter in the following files:

- On the Master, update the master.props file in the Master/Config folder. Restart the Master.
- On the Client Manager, update the clientmgr.props file in the Client Manager/Config folder. Restart the Client Manager.
- On the Agent, update the JAVA_HOME environment variable. Restart the Agent.
- On the Transporter, update the transporter.props file in the Transporter/Config folder. Restart the Transporter.

Customers must have Java 7 to run the CWA Java Client if they run other CWA Components on Java 8. The lib path and bin path in tesclient.bat must point to Java 7.

Upgrading from Java 7 to Java 8

11

CWA Licensing

Before you can run CWA, you need to run through the licensing procedure. This applies whether you are just trying out the software, or have already decided to implement CWA.

This chapter provides details about licensing the Cisco Workload Automation (CWA) version 6.3.2.

CWA License Types

CWA provides two basic license types to fit your needs.

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

License Type	Description
Demo License	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.
Permanent License	If you have purchased CWA, your sales representative can give you a Permanent license. This license is customized to match your planned installation and includes a Master license and licenses for anything else you have purchased such as agents, Fault Monitor, and so on. 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. Agents can be licensed as “floating” in which case your license allows <x> number of agents to work at once, where <x> is the number of agents you purchased. Floating agent licenses can be for any supported operating system. You can also purchase licenses for specific agents. The specifically-licensed non-floating agents are displayed on the Licensed Agents tab as described in Licensed Agents Tab, page 164.

Extensions and components that add extra functionality to CWA might require separate licenses. For example, Fault Monitor, the Windows and Unix Agents, and the Command Line Interface program (SACmd) all require individual licenses. For more information and current availability, contact your sales representative.

You can license CWA with a Demo license during installation. The installer prompts you for a demo code, and if you give it a code, then it will create the demo.lic file for you. When your Demo license expires, or if you did not enter it during installation, you can manually license CWA as described in Licensing Procedures, page 165.

Registered License Dialog

Registering the license for CWA is done from the CWA Web Client or the CWA Java Client.

You can verify your purchased licenses in the Registered License dialog displayed by selecting **Activities > Registered License** in the CWA Web or Java 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 CWA 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 CWA 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 CWA (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: Only non-floating agents are displayed on the Licensed Agents tab. If your license has a floating agent provision, you can define your own agents, but the Licensed Agents tab displays 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. CWA 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 Cisco before the agent connection can be re-established.

Regulatory: Restart the Client Manager after a new license has been loaded.

Licensing Procedures

You might have entered the demo license code when you installed the Master. However, you might need to reapply the demo license, you have purchased and want to apply a permanent CWA license, or perhaps you have purchased additional product licenses.

Carefully follow the instructions below to make sure that your license is applied correctly:

- Applying a Demo License, page 165
- Applying a Permanent License, page 166

Applying a Demo License

To license CWA with a Demo license:

1. Select **Queues**> **System Queue**, and set the value to 0. This will stop all jobs from launching. Wait until all running jobs have completed.
2. 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.

   Windows:

   a. Click **Start** and select **Programs>Cisco Workload Automation>Scheduler>Master>Service Control Manager**.

   b. Select **Scheduler Master** in the Service list and click **Stop**.

   Unix:

   Enter **tesm stop**.
3. Take a backup and then remove all old license files (e.g. *.lic and *.lic_old) from the **<master installation directory>\config** directory.

   By default, based on your platform, this directory is:

   Windows:

   ```
   C:\Program File\TIDAL\Scheduler\Master\config
   ```

   Unix:

   ```
   /opt/TIDAL/Scheduler/Master/config
   ```
4. Create a new file called **demo.lic** in the **<master installation directory>\config** directory.
5. Type or paste the contents of the license file into the new **demo.lic** file.
6. Save the file in the **<master installation directory>\config** directory.
7. Restart the Master:

   Windows:

   – Click Start in the Service Control Manager.

   Unix:

   – Enter **tesm start**.

The Master reads and applies the demo code when it starts.

Applying a Permanent License

To license CWA with a Permanent license:

1. Select **Queues**> **System Queue**, and set the value to 0. This will stop all jobs from launching. Wait until all running jobs have completed.
2. Stop the Master:

   Windows:

   a. Click **Start** and select **`Programs>Cisco Workload Automation>Scheduler>Master>Service Control Manager`**.

   b. Select **Scheduler Master** in the Service list and click **Stop**.

   Unix:

   Enter **tesm stop**.
3. Take a backup and then remove all old license files (e.g. *.lic and *.lic_old) from the **`<master installation directory>\config\`** directory.

   By default, based on your platform, this directory is:

   Windows:

   ```
   C:\Program Files\TIDAL\Scheduler\Master\config
   ```

   Unix:

   ```
   /opt/TIDAL/Scheduler/Master/config
   ```
4. Create a new file called **master.lic** in the **`<master installation directory>\config\`** directory.
5. Type or paste the contents of the license file into the new **master.lic** file.
6. Save the file in the **`<master installation directory>\config\`** directory.
7. Restart the Master:

   Windows:

   – Click Start in the Service Control Manager.

   Unix:

   – Enter **tesm start**.

The Master reads and applies the master code when it starts.

12

Basic CWA Configuration

Before you run CWA, 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 CWA's many strengths is its flexible architecture.

During installation of CWA, 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 CWA functions that are available to you. By default, this account is considered the CWA Administrator/Super User and has the ability to perform all functions.

Basic configuration is complete when you have finished adding users (see the next chapter, Defining Users, page 177). Advanced configuration options include creating and editing security policies, setting logging options and creating queues and agent lists. The *Cisco Workload Automation User Guide* contains detailed information about using and configuring CWA.

You can configure most properties of the Master using the System Configuration dialog box in the CWA Web Client. Other major Master parameters are managed through the *master.props* file on the Master machine as described in this chapter:

Note: Ensure that the regional settings used by the CWA 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.

Configuring the CWA System

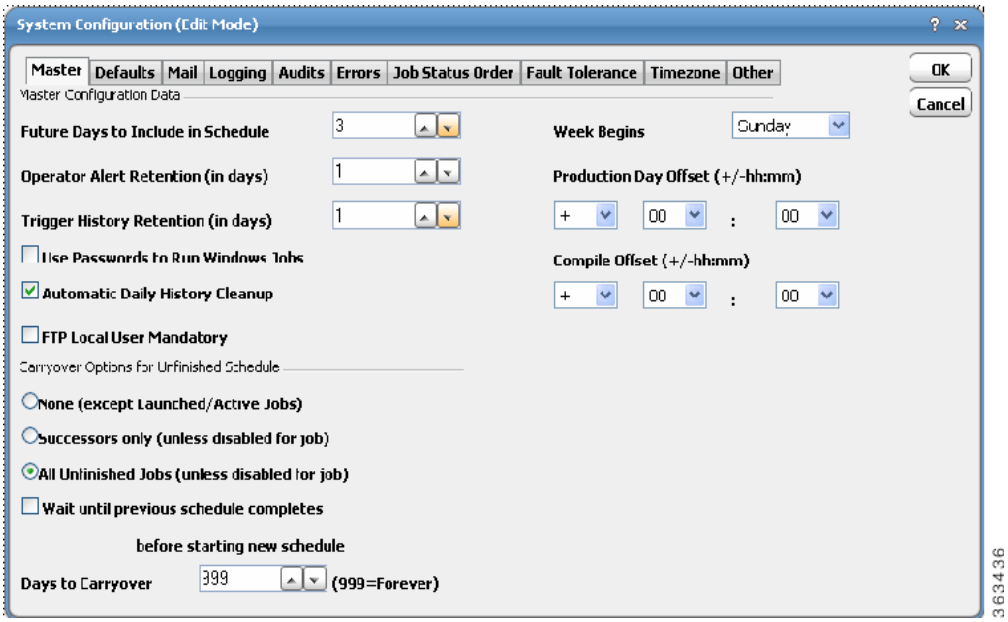
Before using CWA, configure the Master operation parameters, job defaults, mail system connections (if you are using email), and job status sort order.

To configure the CWA system:

1. Launch the CWA Web Client.

   Go to http://<servername>:8080/client and log on using install Super User's network credentials.

2. From the Activities menu, choose **System Configuration**. The System Configuration dialog box displays.



Refer to the “Getting Started” chapter in the *Cisco Workload Automation User Guide* for more information on the options in the System Configuration dialog box.

Configuring the Master Parameters (master.props)

You can change the properties of the Master that were set during installation as 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. See the “Parameters” chapter in the *Cisco Workload Automation User Guide* for more information about system parameters.

The *master.props* file on the Master looks like this 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;${TIDAL_HOME}\lib\ojdbc14.j
ar;${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.

The table in master.props properties, page 169 contains a subset of the properties that are managed in the *master.props* file are listed below in alphabetical order.

master.props properties

Note: This not a complete list.

Property	Default	What it controls
ActiveDirectory.Host	company.com	The Active Directory server URL.
ActiveDirectory.Port	389	The Active Directory server port.
ActiveDirectory.GroupSearchPrefix	OU=Group1,DC=company,DC=com	The prefix of the AD node containing group records. The Client Manager will scan these records when determining the groups to which a user belongs.
ActiveDirectory.UserSearchPrefix	OU=Group1,DC=company,DC=com	The prefix of AD node containing user records. The Client Manager will scan these records when authenticating a user.
AdapterHostHeartbeat	16	Specifies the interval (in seconds) that the adapter host environment checks with the Master.
AdapterHostMaxMemory	256	Maximum size of Adapter host heap space in MBs.
AdapterHostMinMemory	64	Starting size of Adapter Host heap space in MBs.
AdapterHostResendMsgInt	60	Specifies the interval (in seconds) that the adapter host waits for a confirmation from the master that a message was received before resending the message again.
AdapterHostServerPort	6950	Port number used by the adapter host server.
AdapterHostServicePort	6980	Port number used by the adapter host service.
AgentHeartBeatInt	20	Seconds between heartbeats. Minimum is 15 seconds. Agent's equivalent is HB=<milliseconds> (might be in tagent.ini).
AgentHeartbeatFailureCount	6	Number of missed heartbeats allowed before declaring the connection bad. Minimum value is 3.
AgentManagerLog	SEVERE	Sets the level of detail for recording messages from agents to the Agent Manager log.
AgentPort	5591	Port number used by the master to communicate with the agent.
AgentResendMsgInt	600	Seconds after which an unasked message is resent to the Master. Minimum is 180 seconds. Agent's .prp equivalent is RS=<milliseconds>.
AgentResendTimeTickInt	60	Seconds to wait before syncing time with the master. Minimum is 20 seconds. Agent's .prp equivalent is TT=<milliseconds>.
AgentTZCompileInt	1200	Agent time shift amount (in seconds) that causes the master to recompile. -1 disables the recompile.
APClient	<AlarmPoint client name>	Specifies the name of the AlarmPoint client.
APParams	<AlarmPoint parameters>	Specifies parameters for notification from the AlarmPoint server.
APstartDir	3	The directory path to the AlarmPoint agent file. If using UNIX the following format is used: /opt/TIDAL/invoqsystems/APAgent If using Windows, the following format is used: d:\\APAgent
classpath		The path to the packages used in the program.

Property	Default	What it controls
ClientManagerLog	SEVERE	Sets the level of detail for recording messages about CWA activity to the Client Manager log.
CLIENT.RESOURCE_POLLING_INTERVAL		The polling interval the Java Client uses to check the queue size and memory usage of the Java Client. Specify an integer value in seconds.
Client.SlowConnectionCheckInterval		The time interval in seconds at which the Master periodically checks for slow CWA Java Client connections.
Client.SlowConnectionThreshold	95	The slowness threshold which is defined as the percentage of messages that a CWA Java Client should have received to be considered fast enough and thus above the slowness threshold.
CLIENT.TERMINATION_LIMIT_MEMORY_UTILIZATION		The (% of Used Heap Memory to Total Heap Memory) or the (% Used RAM to Total RAM) at which the Java Client is terminated by the Master if this value is exceeded. Specify as a percentage. Permitted values are 0.1 to 100.
CLIENT.TERMINATION_LIMIT_QUEUE_SIZE		The queue size limit at which the Java Client is terminated by the Master if this value is exceeded. Specify the queue size limit as an integer.
CLIENT.WARNING_LIMIT_MEMORY_UTILIZATION		The (% of Used Heap Memory to Total Heap Memory) or the (% Used RAM to Total RAM) at which a warning message is displayed if this value is exceeded. Specify as a percentage. Permitted values are 0.1 to 100.
CLIENT.WARNING_LIMIT_QUEUE_SIZE		The queue size limit at which a warning message is displayed if this value is exceeded. Specify the queue size limit as an integer.
CMDMasterPort	6600	Number of the port that the command line program uses to connect to the Master machine.
CommThreads	8	Number of communication threads at one time.
CommunicationLog	SEVERE	Sets the level of detail for recording messages about defined connections and sockets to the Communications log.
CompilerLog	SEVERE	Sets the level of detail for recording messages about the status of compiling production schedules to the Compiler log.
CONNECTINTERVAL	30	The maximum length of time (in seconds) that should be spent attempting to re-establish connection if the SAP connection is lost.
CONNINFOPOLL	10	Interval of seconds between polls to the SAP application server to determine the connection load (available job slots).
DatabaseConnections	20	Number of connections from the master to the database allowed at once (does not affect cursor count).
DatabaseLog	SEVERE	Sets the level of detail for recording database messages to the Database log.
DatabaseReconnectAttempts	10	Number of times the master will attempt to reconnect with the admiral database if disconnected.
DefaultLog	0	Sets the level of detail for recording general messages to the default log.

Property	Default	What it controls
DirectoryMonitorInt	10	Specifies the time interval (in seconds) for an agent to check directories for files (file events).
EncryptAgent	Y	By default, the Master sends data to the agent in encrypted form, without need to specify this parameter. N disables encryption but you must restart Master service.
ENCRYP_AGENT_PROP	N	Enables encryption of the agent communications.
EventManagerLog	SEVERE	Sets the level of detail for recording event-related messages to the Event Manager log.
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 Tolerance log.
FileMonitorInt	2	Specifies the time interval (in seconds) for an agent to check for files.
FMMasterPort	6703	Number of the port used by the master to connect to the fault monitor.
FT_OPERATION	AUTO	Specifies how fault tolerance is configured. AUTO—The Primary Master and Backup Master are interchangeable; either can be active. If one fails and the other takes over, when the failed Master comes back online, it remains in standby mode. FIXED—The Primary Master role is fixed. If it fails, the Backup Master takes over only until the Primary Master comes back online. 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. If a failover occurs, the Primary Master cannot be restarted until the Backup Master is stopped.
GWStartedTaskExclude	None	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	None	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.
JAVA_HOME		The path to the Java home directory.
JdbcDriver	<directory path>	Database connection driver.
JdbcURL	<directory path>	Database connect string.
JDBGL	1	Sets the debugging level for the z/OS Gateway adapter.
JOBINTERCEPTINT	10	Interval of seconds between checking the SAP intercepted jobs queue.
JVMARGS		Property that sets the JVM argument (Windows only).

Property	Default	What it controls
JobManagerLog	SEVERE	Sets the level of detail for recording messages about job status to the Job Manager log.
LogDirectory	<../log>	Location to write log files. Default=${TIDAL_HOME}/log.
LOGPKT	N	Enables the logging of network traffic between CWA and the z/OS Gateway adapter.
masterID	<master instance name>	Specifies the name of the master instance to the OpenView adapter. This is the same as the primary master alias.
MaxLogFiles	100	The size of the Master*.log file before it rolls over.
MessagePoolSize	0	Message pool size
MessageThreads	8	Number of messages threads at one time. Minimum value is 3. Maximum value is 12.
opcmsgPath	<directory path>	The path to the opcmsg.exe file installed on the master by HP OpenView to communicate with the OpenView Operations Message Browser.
OraAppsDBConnection	5	Specifies the maximum number of connections opened to the Oracle Applications database.
ORADEBUG	OFF	Enables debugging for the Oracle Applications adapter.
OUTPUT_SCAN_CASE_INSENSITIVE	N	When searching job output for designated text strings, converts CWA scanning to case-insensitive. By default, the scanning of job output is case-sensitive. If the job output is large, setting this value may adversely affect memory and system performance.
PSCheckServer	Y	Turns on/off checking of the Process CWA's heartbeat.
PSDBConnection	5	Specifies the maximum number of connections opened to the PeopleSoft database.
PSFinalStatusWait	0 (no status check)	Specifies an interval of time (in seconds) before doing a secondary status check after detecting a "completed" status. This is an additional buffer of time to accommodate those occasions when PeopleTools switches final status shortly after the job completes. This value can be subtracted from the **PSWaitOutput** value if both parameters are used to delay output after completion. If this parameter is greater than 20 seconds, set the **PSWaitOutput** to 0.
PSRunServerOption	Any	The default server the adapter should use to submit process requests when running PeopleTools version 8.45 and later. There are four options: 1–Any (default) 2–Specific 3–Specific OS 4–Primary
PSTimeout	3 x the heartbeat stipulated in process server (180 seconds)	The interval in seconds without a heartbeat before considering a connection to the PeopleSoft server lost.
PSUseRunStatus	N	When running API aware processes in PeopleSoft and this parameter is set to Y, then ignore the **PRCSRTNCODE** value and use the **RUNSTATUS** to determine the status.
PSWaitOutput	30	Number of seconds to wait for PeopleSoft job output.

Property	Default	What it controls
QueueManagerLog	SEVERE	Sets the level of detail for recording messages about queue activity to the Queue Manager log.
SaveReplacedTokens	N	Specifies if the resolved value of tokens should be saved to the database. The default setting is to not save the resolved value (N). Useful if using passwords as a variable value and you do not want the passwords to be visible to other users.
SAPLAUNCHTRIES	3	Number of attempts to try launching an SAP job before going to Error status.
SAPOUTPUTTHREADS	5	Number of concurrent output threads per SAP connection. Due to the potential length of job output, output has its own thread and opens its own connection to retrieve the output and closes the connection as soon as the output completes. This parameter prevents the output requests from exceeding the connections licensed by SAP.
SAPOUTPUTTRIES	5	Number of attempts to connect to the output server for SAP job output.
SAPSERVERTIME	D	The default is to regularly poll the SAP server for the time. If N is specified, this time check polling of the SAP server is disabled. O specifies the old timecheck call.
SAPTIMEOUT	120	Number of seconds before the Remote Function Call (RFC) times out.
SAPTIMEZONE	N	If Y is specified, CWA will use the time zone where the SAP system resides when scheduling SAP jobs. This time difference is displayed in the Time Zone column of the Connections window. To use this parameter, enable “GET_SYSTEM_TIMEZONE” in the SAP system for remote access.
SchedulerLog	OFF	Sets the level of detail for recording system level messages about the master to the master log.
Security.Authoentication	ActiveDirectory	
Security.Authentication.Ext.File	user-auth.xml	
snmphost	2	Name of the machine where the SNMP software was installed.
snmpport	5	Number of the port used by the SNMP software.
SMTP.legacyConfig	N	Denotes that the Master supports SSL and Authentication. If the property is set to ‘Y’, the Master behaves similar to 6.3.1 release, where it just uses the SMTP Server, port (25) and return address, and ignores the newly added fields in the **System Configuration** dialog, namely, **Use SSL/TLS**, **Authentication Required**, and so on.
TESClient.ConnectionLimit		Maximum number of CWA Java Clients that can connect to a CWA Master at any one time. Note that this does not affect or limit the number of CWA Web Client connections (via the Client Manager) nor the number of super admin users using the CWA Client.

Property	Default	What it controls
TESClient.IPAddressList	<none>	The Java Client IP addresses that are allowed to access the Master. Separate multiple IP addresses with a comma. IP address ranges can be specified with a hyphen and multiple ranges should be comma-separated. Both IPV4 and IPV6 are supported. Example value: 172.21.45.70-172.21.47.145, 172.25.5.51
TESClient.SubnetMaskList	<none>	One or more subnet masks for Java Client IP addresses that are allowed to access the Master. Separate multiple subnet masks with a comma. IPV6 is not supported. Example: TESClient.SubnetMaskList=171.37.102.224/28,173.37.154.96/28, 172.21.45.70/26
TESClient.UserIdList	<none>	The Java Client users who are allowed to access the Master. Separate multiple user names with a comma. Example: TESClient.UserIdList=tidalsoft\\sbrights, tidalsoft\\qatest
ToleranceTime	3	The maximum time allowed for heartbeats lost between FM and PM/BM before FM decides connection to PM/BM is lost. This is assuming the connection is not lost yet. If the connection is lost already (i.e. physical disconnect, PM/BM shutdown, socket timeout, etc) then the FM will failover immediately. Thus ToleranceTime does not apply in the case when the master is shutdown. The FM will failover immediately since PM connection is lost. Note the rules for failover: the PM must lose connection to both the FM and the BM to cause a failover. For example, if the PM loses connection to the FM but not the BM, a failover will not occur, because the BM will reject the FM's failover as it can still talk with the PM.
TRACE	0 (Off)	A value of 1 turns on the trace function in SAP to collect diagnostic data into a file with an extension of .trc.
WebServer.Port	8080	Note that this is different from WebServerPort.
WebServerPort	9999	Turns on a webserver that can be used to analyze the contents of the memory here: http://<mastername>:9999/data.

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 CWA 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 CWA 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*.

13

Defining Users

During installation of CWA, 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 CWA functions that are available. This account is considered a CWA 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 Workload Automation User Guide* contains detailed information about using and configuring CWA.

This chapter covers:

User Configuration Interface

The first time that you run CWA, you have Super User capability which gives you full access to all CWA functions.

User Definition Dialog Box

The User Definition dialog box allows you add and configure accounts for CWA users.

Security Tab

This tab contains the following elements:

Element	Description
Super User	Select this option to give the user access to all available CWA 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 CWA 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 CWA 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. CWA 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 CWA users. If the users do not display, you do not have the appropriate rights to view users.

Adding a User

To add a user:

1. From the Navigator pane, choose **Administration > Interactive Users** to display all CWA users.
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.
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.
4. Type the user's full name in the Full Name field. This name will be used in CWA reports and some dialog boxes.
5. Choose a domain name from the Domain list.
6. Select the Security tab.
7. Select the Security Policy for the user.

   If the user needs full access to all CWA functions, select the Super User option. Super User capability within CWA is unrestricted.
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.

9. Select the Agents tab and use the list on the Agents tab to authorize agents for this user.
10. Additionally, you can select All Agents to authorize all agents.
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.
12. To enter additional information, select the Description tab.
13. Click **OK**.

Editing a User Definition

To edit a user definition:

1. From the Navigator pane, choose **Administration > Interactive Users** to display all CWA users.
2. Double-click the user record to edit or select the user and click the **Delete** button on the CWA toolbar.

   -or-

   Right-click the user record and choose **Edit Interactive User** from the context menu. The User Definition dialog box displays.
3. Edit the user name if it does not match the Windows login name. Remember that the user name is case-sensitive.
4. Edit the full name if necessary.
5. Select the Security tab.
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.
7. Click the Super User option if you want the user to have access to all CWA functions.
8. To add or remove specific functions to a security policy, see Security Tab, page 177.
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.
10. Select the Agents tab and use the list on the Agents tab to change the authorized agent for this user.
11. Select the Notification tab to edit contact information for the user.
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 Cisco Workload Automation workgroups, see your *Cisco Workload Automation User Guide*.
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:

1. From the Navigator pane, choose **Administration > Interactive Users** to display the Users pane, showing all CWA users.
2. Select the user and click the **Delete** button on the CWA 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.
3. Click **OK**..

Viewing Runtime Users

To view Runtime users:

1. From the Navigator pane, choose **Administration > Runtime Users** to display all CWA runtime users.

If the CWA runtime users do not display, you do not have the appropriate rights to view users.

2. Double-click the user name. The User Definition dialog box displays showing user information.

Impersonating Another User

To impersonate another user:

1. From the Navigator pane, choose **Administration > Interactive Users** to display the User pane, showing all CWA users.

   If the CWA users do not appear, you do not have the appropriate rights to view users.
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.
3. Click **OK** in the confirmation dialog box.

To stop impersonating another user:

1. Choose **End Impersonate** from the Users context menu.

   -or-

   Choose **Activities > End Impersonate**.

14

Configuring SSL Messaging

This section discusses the procedure to configure SSL messaging on a CWA 6.3.2 system. CWA uses Java Messaging Service (JMS) to implement communications among its components.

This chapter discusses SSL configuration for its components in these sections:

Obtaining Server Keys and Certificates

You need a pair of server key and certificate for each of the following components:

- Client Manager
- Primary Master
- Java Client

If you plan to use a Remote Master, you need a pair of server key and certificate for it too.

If you are setting up a fault tolerant system, you 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) using one of these methods:

Generating Keys and Certificates

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.

Obtaining a 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
```

Exporting and Importing a Certificate

When SSL messaging is enabled, each of CWA 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 CWA server. It will indicate what other CWA server's certificates must be imported into CWA 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 SSL on the Primary Master:

1. Shut down the Primary Master.
2. Copy the key store for the Primary Master to the **config** directory in the Master's installation directory.
3. Create a trust store by importing Client Manager's certificate. Follow the instructions in Obtaining Server Keys and Certificates, page 183.

   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.
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.

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' means no. You can use this property switch between SSL and non SSL messaging modes.

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, page 190 for instructions.

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, page 188.

Configuring SSL on a Remote Master

In this section, you will enable SSL on a Remote Master with the key stores you obtained from earlier section.

To enable SSL on the Remote Master:

1. Shut down the Remote Master.
2. Copy the key store for the Remote Master to the *config* directory in the Master's installation directory.
3. Create a trust store by importing the certificates of Primary Master. Follow the instructions in Obtaining Server Keys and Certificates, page 183.

   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.

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.

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.

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, page 190 for instructions.

7. Save the property file.

If you setting up a fault tolerant system, continue on to Configuring SSL on the Backup Master, page 186. Otherwise, continue on to Configuring SSL on the Client Manager, page 188.

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 enable SSL on the Backup Master:

1. Shut down the Backup Master.
2. Copy the key store for the Backup Master to the **config** directory in the Master's installation directory.
3. Create a trust store by importing Client Manager's certificate. Follow the instructions in Obtaining Server Keys and Certificates, page 183e. 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.
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.
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' means no. You can use this property switch between SSL and non SSL messaging modes.

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, page 190 for instructions.

7. Save the property file.

8. Continue on to Configuring SSL on the Fault Monitor, page 187.

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 SSL on the Fault Monitor:

1. Shut down the Fault Monitor.

2. Copy the key store for the Fault Monitor to the **config** directory in its installation directory.

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.

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.

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.

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, page 190 for instructions.

7. Save the property file.
8. Continue on to Configuring SSL on the Client Manager, page 188.

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.

To enable SSL on the Client Manager:

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, page 183.

   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.
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.
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.
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, page 190 for instructions.

5. Save the property file.

Configuring SSL on the Java Client

In this section, you will enable SSL on the Java Client with the keystores you obtained from the earlier section.

Note: SSL is not supported on Web launch Java Client.

To enable SSL on the Java Client:

1. Logout the Java Client.
   a. Create a *config* directory in the Java Client's installation directory.
   b. Create a **ssl.props** file for each Master. The format of the **ssl.props** file is as follows:

   ```
   <Hostname or IP address>-ssl.props
   ```

   c. Create a separate folder for each Master under the *config* directory in the Java Client's installation directory.
   d. Create a trust store by importing Primary Master's certificate. Follow the instructions in Obtaining Server Keys and Certificates, page 183.

   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 folder created for the specific Master under the *config* directory in the Java Client's installation directory.
2. Use a text editor to open the property file *config/<Hostname or IP address>-ssl.props* located in the Java Client'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.
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.
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, page 190 for instructions.

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 SSL passwords for Client Manager:

1. Open a command shell window and change directory to the *lib* directory under Client Manager's installation directory.
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.
3. Copy the entire line of command output and paste it into the value field of that password in property file.
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 SSL passwords for Fault Monitor or any Master:

1. Open a command shell window and change directory to the **lib** directory under Cisco Workload Automation's installation directory.
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.
3. Copy the entire line of command output and paste it into the value field of that password in property file.
4. Repeat step 1 to 3 for each of the other passwords.

15

Upgrading Components

Overview

This chapter describes upgrade procedures for these components:

If you are using work groups, the runtime user validation must be configured after upgrading from CWA (TES) 5.3.1, 6.1.x, 6.2.1, 6.3, or 6.3.1 to 6.3.2. See this section:

Note: The CWA 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. See Configuring the Master Parameters (master.props), page 168 for more information.

Upgrade Prerequisites

- Always make a backup of your data before upgrading.
- Set your system queue to 0.

- Stop all CWA components (Masters, Client Manager, Fault Monitor, Clients, etc.)
- Be sure that your system meets the minimum hardware/software requirements for the latest version. The hardware/software requirements may have changed from the last version.
- Before upgrading to 6.3.2, ensure that the CWA user has the right in Oracle to create triggers and sequences.
- A warning message will appear in the newly upgraded scheduler.out file if a 6.X environment is running off of a 5.3.1 license. If you wish to absolve this warning, you can regenerate the license to reflect 6.X version. This should not affect functionality.
- It is recommended (but not required) to uninstall and reinstall the latest versions of your agents at this time.
- The 6.2 and later versions of CWA (TES) have several prerequisite software components that were not required in earlier versions. The complete list of prerequisites is available in the section, Installation Prerequisites, page 13. If any of the prerequisites are not completed before installation, the upgrade procedure will not be successful.

Note: Your shortcut icons may no longer work after an upgrade. If clicking a CWA icon on the desktop does not start the component after upgrading, you need to recreate your CWA shortcuts.

Note: Be sure to back up your database before proceeding with this upgrade.

Upgrading the Windows Master to 6.3.2

Follow the steps below to upgrade Windows CWA (TES) Master from 6.2.1, 6.3.0, and 6.3.1, to version 6.3.2.

If you have CWA (TES) versions older than 6.2.1, you must first upgrade to 6.3.0 and then you can upgrade to 6.3.2. For upgrading to 6.3.0 version, refer the *Cisco Workload Automation Installation Guide* for release 6.3.

Note: Be sure to backup 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 6.3.2, 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:

1. Complete all prerequisites in Upgrade Prerequisites, page 191.

   If your installation uses an Oracle database, your database administrator must add the following Oracle privileges to the CWA user account in Oracle before beginning the upgrade procedure or the upgrade will fail:

   - Create sequence
   - Create trigger

2. Ensure that the system queue has been set to **0** so no new jobs will launch.
3. If not already done, stop the Master service through the CWA Service Manager.

   a. Click **Start > All Programs > Cisco Workload Automation > CWA Service Manager**.

   The **CWA Service Manager** dialog displays.

   b. Select **Scheduler Master** from the **Service** list.

c. Click **Stop**.

4. Run the *setup.exe* file.
5. Click **Run**.

   The **Internet Explorer-Security Warning** dialog displays.
6. Click **Run**.

   The **Welcome** panel displays.
7. Click **Next**.

   The **Master Upgrade** panel displays that the setup has detected previous version of Scheduler Master on this computer.
8. To upgrade Scheduler Master and use the existing Admiral database, click **Next**.

   The **Install Wizard Complete** panel displays.
9. Click **Yes** to reboot the machine so the changes from the upgrade process can take effect.
10. Click **Finish**.

The database modifications are performed when the Master is first started after the installation.

Upgrading the Unix Master

Follow the procedures in these sections to upgrade your Unix Master:

- Upgrading the Unix Master to 6.3.2, page 193

If you are upgrading the Unix Master using the command line, see:

- Upgrading the Unix Master from the Command Line, page 195

Upgrading the Unix Master to 6.3.2

Note: Be sure to backup 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:

1. Complete all prerequisites in Upgrade Prerequisites, page 191.

   If your installation uses an Oracle database, your database administrator must add the following Oracle privileges to the CWA user account in Oracle before beginning the upgrade procedure or the upgrade will fail:

   – Create sequence

   – Create trigger
2. Ensure that the system queue has been set to `0` so that jobs will not launch. They will remain in the “Waiting on Resources” status until the system queue has been released.
3. From the command line of the Master machine, stop the Master:

```
./tesm stop
```

4. Copy *install.bin* to the target machine and change the permissions on the file:

   ```
   chmod 755 install.bin
   ```

5. Run the upgrade program that you copied to your machine:

   ```
   sh./install.bin
   ```

   The **Introduction** panel displays.

6. Click **Next**.

   The **Readme** panel displays.

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,

8. Click **Next**.

   The **Choose Install Folder** panel displays.

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.

10. Click **OK** to the confirmation message.

    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.

11. Click **Next**. The **Get Authentication Method** panel displays.

12. Select **AD** for Active Directory or **LDAP**.

13. Click **Next**. The **Pre-Installation Summary** panel displays.

14. Verify that the information is correct.

15. Click **Install**.

    During the upgrade process, a progress bar is displayed.

    When the upgrade is complete, the **Install Complete** screen displays.

16. Click **Done**.

17. Return to the location where you copied the *install.bin* file and delete the *install.sh* file.

    It is no longer needed and may cause problems during other upgrades in the future.

18. If upgrading from 6.x to 6.3.2, 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 u*pd.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.
```

19. Restart the Master.

```
./tesm start
```

The database modifications are performed when the Master is first started after the installation.

Upgrading the Unix Master 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:

1. Copy *install.sh* to the target machine.
2. Change the permissions on the *install.bin* file in the directory to make the file executable:

```
chmod 755 install.sh
```

3. Open a command prompt window and enter:

```
# sh ./install.sh -i console
```

4. Press **Enter**.

   The **Introduction** panel displays.

5. Click **Next**.

   The **Readme** panel displays.

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,

7. Click **Next**.

   The **Choose Install Folder** panel displays.

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.

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.

10. Click **Install**.

    During the upgrade process, a progress bar is displayed.

    When the upgrade is complete, the **Install Complete** screen displays.

11. Click **Done**.

12. Return to the location where you copied the *install.sh* file and delete the *install.sh* file.

    It is no longer needed and may cause problems during other upgrades in the future.

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.
    ```

14. Restart the Master.

    ```
    ./tesm start
    ```

The database modifications are performed when the Master is first started after the installation.

Upgrading the Windows Backup Master to 6.3.2

Follow the steps below to upgrade Windows CWA (TES) Backup Master from 6.2.1, 6.3.0, and 6.3.1, to version 6.3.2.

If you have CWA (TES) versions older than 6.2.1, you must first upgrade to 6.3.0 and then you can upgrade to 6.3.2. For upgrading to 6.3.0 version, refer the *Cisco Workload Automation Installation Guide* for release 6.3.

The upgrade program upgrades the Backup Master. 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 Backup Master to version 6.3.2, 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 Backup Master:

1. Complete all prerequisites in Upgrade Prerequisites, page 191.

   If your installation uses an Oracle database, your database administrator must add the following Oracle privileges to the CWA user account in Oracle before beginning the upgrade procedure or the upgrade will fail:

- Create sequence
- Create trigger

2. Ensure that the system queue has been set to **0** so no new jobs will launch.
3. If not already done, stop the Backup Master service through the CWA Service Manager.
   a. Click **Start > All Programs > Cisco Workload Automation > CWA Service Manager**.

   The **CWA Service Manager** dialog displays.

   b. Select **Scheduler Backup Master** from the **Service** list.
   c. Click **Stop**.
4. Run the *setup.exe* file.
5. Click **Run**.

   The **Internet Explorer–Security Warning** dialog displays.
6. Click **Run**.

   The **Welcome** panel displays.
7. Click **Next**.

   The **Master Upgrade** panel displays that the setup has detected previous version of Scheduler Backup Master on this computer.
8. To upgrade Scheduler Backup Master, click **Next**.

   The **Install Wizard Complete** panel displays.
9. Click **Yes** to reboot the machine so the changes from the upgrade process can take effect.
10. Click **Finish**.

Upgrading the Unix Backup Master

Follow the procedures in these sections to upgrade your Unix Backup Master:

- Upgrading the Unix Backup Master to 6.3.2, page 197

If you are upgrading the Unix Backup Master using the command line, see:

- Upgrading the Unix Backup Master from the Command Line, page 199

Upgrading the Unix Backup Master to 6.3.2

The upgrade program upgrades the Backup Master.

To upgrade to the latest version:

1. Complete all prerequisites in Upgrade Prerequisites, page 191.

   If your installation uses an Oracle database, your database administrator must add the following Oracle privileges to the CWA user account in Oracle before beginning the upgrade procedure or the upgrade will fail:

- Create sequence
- Create trigger

2. Ensure that the system queue has been set to `0` so that jobs will not launch. They will remain in the “Waiting on Resources” status until the system queue has been released.
3. From the command line of the Backup Master machine, stop the Backup Master:

   ```
   ./tesm stop
   ```

4. Copy *install.bin* to the target machine and change the permissions on the file:

   ```
   chmod 755 install.bin
   ```

5. Run the upgrade program that you copied to your machine:

   ```
   sh./install.bin
   ```

   The **Introduction** panel displays.

6. Click **Next**.

   The **Readme** panel displays.

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,

8. Click **Next**.

   The **Choose Install Folder** panel displays.

9. Enter the directory path to the **Backup Master** folder where the Backup Master files were installed during the original installation of the Backup Master.

   The Upgrade program cannot proceed without knowing where the Backup 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 **Backup Master** folder.

   A confirmation message verifies that the required Backup Master directories are in the specified location.

10. Click **OK** to the confirmation message.

    If the Upgrade program cannot find the Backup Master files at the specified location, an error message displays and the installation process is aborted as soon as you acknowledge the error message.

11. Click **Next**. The **Get Authentication Method** panel displays.
12. Select **AD** for Active Directory or **LDAP**.
13. Click **Next**. The **Pre-Installation Summary** panel displays.
14. Verify that the information is correct.
15. Click **Install**.

    During the upgrade process, a progress bar is displayed.

    When the upgrade is complete, the **Install Complete** screen displays.

16. Click **Done**.
17. Return to the location where you copied the *install.bin* file and delete the *install.sh* file.

    It is no longer needed and may cause problems during other upgrades in the future.
18. Restart the Backup Master.

    ```
    ./tesm start
    ```

Upgrading the Unix Backup Master from the Command Line

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

To install from the command line:

1. Copy *install.sh* to the target machine.
2. Change the permissions on the *install.bin* file in the directory to make the file executable:

    ```
    chmod 755 install.sh
    ```
3. Open a command prompt window and enter:

    ```
    # sh ./install.sh -i console
    ```
4. Press **Enter**.

    The **Introduction** panel displays.
5. Click **Next**.

    The **Readme** panel displays.
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,
7. Click **Next**.

    The **Choose Install Folder** panel displays.
8. Enter the directory path to the **Backup Master** folder where the Backup Master files were installed during the original installation of the Backup Master.

    The Upgrade program cannot proceed without knowing where the Backup 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 **Backup Master** folder.

    A confirmation message verifies that the required Backup Master directories are in the specified location.
9. Click **OK**.

    If the Upgrade program cannot find the Backup 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.
10. Click **Install**.

During the upgrade process, a progress bar is displayed.

When the upgrade is complete, the **Install Complete** screen displays.

11. Click **Done**.
12. Return to the location where you copied the *install.sh* file and delete the *install.sh* file.

    It is no longer needed and may cause problems during other upgrades in the future.
13. Restart the Backup Master.

```
./tesm start
```

Upgrading the Client Manager to 6.3.2

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:

1. Locate the *.dsp* and *.props* files in your CWA **config** directory, and then save them.
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**.
3. Uninstall the Client Manager. See Uninstalling Client Manager, page 76.
4. Reinstall the Client Manager. See Installing the Client Manager, page 63.
5. Return the *.dsp* and *.props* files that you saved in Step 1 to your Cisco Workload Automation **config** directory.
   a. After reinstalling the Client Manager, stop the Client Manager service through the CWA Service Manager. See Starting and Stopping Client Manager, page 75.
   b. Return the *.dsp* and *.props* files that you saved in Step 1 to your Cisco Workload Automation **config** directory. to overwrite the existing *.dsp* and *.props* files.
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**.

   Regulatory: DO NOT delete client.war.
7. Restart the Client Manager service through the CWA Service Manager. See Starting and Stopping Client Manager, page 75.

Upgrading the Existing Master Database with New CWA (TES) Master Installation

Note: Be sure to back up your database before proceeding with this upgrade.

To upgrade the existing Master database from 6.2.x, 6.3 or 6.3.1 to 6.3.2 by installing the new CWA (TES) Master:

1. Install the 6.3.2 CWA Master for Windows. For more information, see the Chapter 3, "Installing the CWA Master for Windows,".
2. During installation, enter the details of the existing database server in the Database Server panel.

   The **Detect Admiral Database** confirmation dialog box appears stating the existence of the Admiral Database and Tidal account, and whether to continue the installation using the existing database.
3. Click **Yes** to proceed.
4. Continue and complete the installation.
5. Start the CWA Master.

Note: To upgrade the Client Manager database with the new CWA Client Manger installation, run **clearcache.sql** in the external cache database to drop the tables and views so that the database can be rebuilt. The **clearcache.sql** script is located in the following path: **<*Client Manager Install Directory*>/cache/<*plugin name*>/cachesql.zip**.

Upgrading the Windows Agent

Follow the procedures in these sections for the upgrade from/to versions:

- Upgrading the Windows Agent from 1.x to 3.x, page 201
- Upgrading the Windows Agent from 2.x to 3.x, page 201

Note: Many prefer uninstalling and reinstalling the agent, but the upgrade steps are below if preferred.

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 CWA Agent for Windows, use the CWA Service Manager to stop the agent.

To upgrade the Agent:

1. Copy *Tidal Agent.msi* to the target machine, then run it.
2. In the **File Download** dialog, click **Run**.
3. In the **Security Warning** dialog, click **Run**.
4. In the **Welcome** dialog, click **Next**.

   The **Question** dialog displays.
5. Click **Yes** to confirm that you want to upgrade the existing agent.

   The **Wizard Complete** panel displays.
6. Click **Finish**.

Upgrading the Unix Agent

Follow the procedures in these sections for the upgrade from/to versions:

- Upgrading the Unix Agent from 1.x to 3.x, page 202
- Upgrading the Unix Agent from 2.x to 3.x, page 202

Note: Many prefer uninstalling and reinstalling the agent, but the upgrade steps are below if preferred.

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.

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.

To install the agent from the command line:

1. Login as root.
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.
3. Change the permissions on the two install files in the directory to make the file executable:

   ```
   chmod 755 install.sh install.tar
   ```
4. Begin the installation by entering:

   ```
   ./install.sh
   ```

   An introduction screen displays as the installation program begins.
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.
6. Enter the name of the user to own the agent and press **Enter**.
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.
8. Press **Enter**.

   The **Agent Configuration Menu** screen displays.
9. Type **`1`** to select the **Add Instance** option and press **Enter**.
10. Enter the agent name.

11. Enter the number of the port the agent should use.
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.
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 Fault Monitor for Windows

To upgrade the Fault Monitor for Windows:

1. Copy the installation package to the machine where the Fault Monitor is being installed. If no screen displays, locate the main.htm file in the installation root directory and open it.
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.
3. Follow the upgrade instructions as they appear throughout the upgrade procedure.
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 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 for Unix:

1. Make a backup of the faultmon directory.
2. From the Fault Monitor pane of the CWA Web Client, right-click and select the **Stop Fault Monitor** option in the context menu.
3. From the installation 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 at **<installation_directory_root>\Upgrade\FaultMon\<operating system>\install.bin**.
4. Run the upgrade program that you copied to your machine:

   ```
   sh./install.bin
   ```

   The **Introduction** panel displays.
5. Read the directions on how to proceed and click **Next**. The **Readme** panel displays.
6. Verify that the listed prerequisites 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.

7. Click Next. The **Choose Install Folder** panel displays.
8. Enter the directory path 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 Fault Monitor 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.
9. Click **OK** to the confirmation message, then click **Next**.

   The **Pre-Installation Summary** panel displays.
10. Validate the summary, then 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.
11. Click the **Done** button to complete the upgrade process.
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.

Configuring Runtime User Validation for Workgroups after Upgrading

If you are using CWA workgroups, the runtime user validation must be configured after upgrading from CWA (TES) 5.3.1, 6.1.x, or 6.2.1, 6.3, or 6.3.1 to 6.3.2.

This process involves selecting a configuration option and possibly running some queries to configure the Master database as described below.

To configure runtime user access for workgroups:

1. In the CWA Web or Java Client, select Workgroups from the navigation pane.
2. Select the workgroup you want to configure and open its definition.
3. Select the Runtime Users tab.
4. At the bottom of the pane, choose one of the following options and follow the configuration steps below:

- Runtime users associated with the workgroup only (default)

Selecting this option allows only the runtime users associated with the workgroup to be available for jobs owned by the workgroup. This is the default option for a new workgroup.

- Runtime users associated with the current logged on user and runtime users associated with the workgroup

Selecting this option allows the runtime users associated with the current logged-on user along with the runtime users associated with the workgroup to be available for jobs owned by the workgroup. This is on par with CWA (TES) 5.3.1 functionality. Customers who are migrating/migrated from 5.3.1 to 6.3.2 can either select this option without restarting the Master and Client Manager (or) they can follow the steps here:

a. Execute the following query in the Master database:

Oracle:

```
UPDATE WORKGRP SET WORKGRP_EXTERNID = 'U', WORKGRP_LSTCHGTM = SYSDATE
```

MSSQL:

```
UPDATE WORKGRP SET WORKGRP_EXTERNID = 'U', WORKGRP_LSTCHGTM = GETDATE()
```

b. Commit the changes.

c. Restart the Master and Client Manager.

- Every member's runtime users in the workgroup and runtime users associated with the workgroup (caution required)

Selecting this option allows the runtime users associated with every member in the workgroup along with the runtime users associated with the workgroup to be available for jobs owned by the workgroup. This is on par with CWA (TES) 6.1 functionality. Selecting this option allows a member in a workgroup without runtime users to use the runtime users associated with other members in the same workgroup. So please select this option cautiously. Customers who are migrating/migrated from 6.1 to 6.3.2 can either select this option without restarting the Master and Client Manager (or) they can follow the steps here:

a. Execute the following query in Master database:

Oracle:

```
UPDATE WORKGRP SET WORKGRP_EXTERNID = 'Y', WORKGRP_LSTCHGTM = SYSDATE
```

MSSQL:

```
UPDATE WORKGRP SET WORKGRP_EXTERNID = 'Y', WORKGRP_LSTCHGTM = GETDATE()
```

b. Commit the changes.

c. Restart Master and Client Manager.

Note: Jobs owned by super users while editing will get a " Read Only Access" pop up when they do not own the runtime user associated to this job.

16

Troubleshooting

Many problems with the installation and operation of the Cisco Workload Automation 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 CWA components.

Two CWA documents can be of great assistance as you troubleshoot your CWA system:

- *Cisco Workload Automation Essential Knowledge Guide*—Provides guidance for working with Cisco's Technical Assistance Center (TAC), key tips for logging and troubleshooting, basic configuration information, how to start and stop all components, and how to perform many of the basic processes.
- *Cisco Workload Automation Product Compatibility Guide*—Provides a complete list of supported platforms, hardware, and software with version information for each.

You can access these and other CWA documents at:

http://www.cisco.com/c/en/us/support/analytics-automation-software/workload-automation-6-3/model.html

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 CWA 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 CWA component, verify that the user doing the installation has access to COM objects and if necessary enable COM object access.

CWA Fails to Install a Copy of msvcr71.dll

Occasionally, CWA fails to install a copy of *msvcr71.dll* (Windows 2003) or *msvcr100.dll* (Windows 2008) 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.

Any attempt to start CWA without the .dll will fail, and the failure will occur so early in CWA's launching process that CWA will not write a log file. Most means of launching CWA (services control panel, CWA 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* or *msvcr100.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).

Verifying and Enabling COM Object Access (Windows Agents)

This is required for Windows agents if it's not already done.

To verify and enable COM object access:

1. From the Windows Start menu, choose **Run**. The Run dialog displays.
2. In the Open field, enter **DCOMCNFG** and click **OK**. The Component Services dialog displays.
3. Choose **Component Services > Computers.**
4. Right-click **My Computer** and choose **Properties** from the resulting menu. The My Computer Properties dialog displays.
5. Select the **COM Security** tab.
6. In the **Launch and Activation Permissions** section, click **Edit Default**. The Launch and Activation Permission dialog displays.
7. In the **Group or user names** section, highlight your user account and verify that your account has Allow Launch access.
8. If the account has a Deny value, select **Allow**.
9. Click **OK**.
10. If the user is not listed, click **Add** and add the user ensuring the user has Allow Launch access.
11. Click **OK**.

OCSEXIT Jobs

If you find that jobs created using the OCSEXIT variable, that run on Windows agents, and that consistently end in Completed Abnormally, you may need to update your system path.

To update your system path:

1. Right-click **My Computer** and choose **Properties** from the resulting menu. The System Properties window displays.
2. Select the Advanced tab and click **Environment Variables**. The Environment Variables dialog displays.
3. Append **%systemroot%\system32** to your system's Path variable.
4. Click **OK**.

Changing the System Clock

Before changing the system clock, please shut down any CWA components installed on that machine. If you change the system time while a CWA component on that machine is active, you might experience connectivity problems.

Oracle Database Issues

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 CWA Master is still running, the CWA 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.