Cisco Unified Workforce Optimization

Workforce Management Installation Guide 8.2
October 31, 2007

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

Workforce Management Installation Guide

Contents

Contents

Contents

Contents

Overview

1

Introduction

The Workforce Management (WFM) InstallShield Wizard guides you through the WFM installation. The installation includes two sets of components:

- Process components, including the WFM services
- Transaction components, including BIRT, Omnis, and Apache Tomcat

NOTE: Both sets of components must be installed on the same server.

After you have successfully installed WFM into a properly-configured Cisco Unified Workforce Optimization (WFO) environment, the basic functionality of WFM is ready to configure for your use. Users access WFM through a web browser.

For information about configuring WFM, see the following document:

- *Workforce Management Administrator User Guide for Cisco Unified Workforce Optimization*

Features of Workforce Management

WFM is an industry-leading software solution for multi-site staff forecasting and scheduling.

Call center managers can use WFM to complete the following tasks.

- Develop a schedule forecast (by day or period)
- Manage special events
- Prepare schedules (summary and individual)
- Manage day-to-day schedule-related activities (Intraday)
- Approve time-off requests and shift changes
- Generate productivity, performance and historical reports
- Create agent report cards
- Develop schedules for multiple sites
- Manage scheduling for offices in different time zones
- Manage key performance indicators
- Manage real-time adherence
- Monitor and adjust the current schedule for a team from a dashboard

Agents can also use WFM to access the system to see their own schedules and performance indicators.

Workforce Management Services

Workforce Management Capture Service

The Workforce Management Capture Service watches for historical call data reports created by the Workforce Management OOC (Odysoft ODBC Collector) Service. When the Workforce Management Capture Service detects a new report, it sends a compilation request to the Workforce Management Compile Service.

Workforce Management Compile Service

The Workforce Management Compile Service listens for compilation requests from the Workforce Management Capture Service. The Workforce Management Compile Service can compile historical data for agents, services or teams by day, week, month, or year, for use in forecasting and scheduling.

Workforce Management OOC Service

Every 30 minutes, the Workforce Management OOC Service collects all of the call data for the preceding 30 minutes from the Cisco Unified Contact Center Express (Unified CCX) database using the Open Database Connectivity (ODBC) interface. The Workforce Management OOC Service then writes the call data into historical reports.

High availability (HA) configurations can use multiple data sources. The Workforce Management OOC Service always connects to the first node, however, and fails over to the second node only if the first connection fails.

Workforce Management Request Service

The Workforce Management Request Service listens for user requests to generate forecasts and schedules.

Workforce Management RTE Service

The Workforce Management RTE (Real Time Engine) Service uses the Advanced Contact Management Interface (ACMI) protocol to get real-time information on agent states from the Unified CCX server. WFM displays agent state information in the Supervisor Adherence dashboard.

Workforce Management Sync Service

The Workforce Management Sync Service connects to the Unified CCX node using the ACMI-based synchronization process. The Workforce Management Sync Service retrieves and processes configuration data, such as contact service queue (CSQ) configurations, team configurations, and agent configurations.

Tomcat Service

The Tomcat Service enables desktop clients to access WFM.

What's New in This Version

WFM 8.2 includes the following new features.

- Support for Windows Vista with Internet Explorer 7.0 for clients
- Email/Chat scheduling (not through an exception)
- Enhanced usability by making ACD populated fields read-only
- Simplification of the Call Forecast Calculation screen
- Support for Microsoft SQL Server 2005 independent location-like storage

WFM Documentation

The following documents contain additional information about WFM:

- *Workforce Management Administrator User Guide for Cisco Unified Workforce Optimization*
- *Workforce Management Agent User Guide for Cisco Unified Workforce Optimization*
- *Workforce Management Service Information Manual for Cisco Unified Workforce Optimization*
- *Workforce Management Release Notes for Cisco Unified Workforce Optimization*

Port Usage

A WFM environment consists of one WFM server and two or more remote devices, including the Unified CCX server and one or more client PCs.

The following list shows the software running on each of these devices.

- WFM server
  - WFM services
  - WFM application
  - WFM instance of SQL Server
  - Apache Tomcat
- Unified CCX server
  - Unified CCX
  - Unified CCX instance of SQL Server
  - CTI server (part of the RmCm subsystem)
- Client PC
  - Internet Explorer 6.0 or 7.0

Table 1 lists the TCP and UDP ports used by WFM and its components on the WFM server.

NOTE: For more information about Apache Tomcat port usage, go to http://tomcat.apache.org/tomcat-5.5-doc/index.html.

Table 1. WFM Port Usage on WFM Server

Server application protocol	Destination port (listening)	Client application protocol
WFM instance of SQL Server	TCP 1433 TCP 1434	WFM Capture Service WFM Compile Service WFM RTE Service WFM Request Service WFM Sync Service Apache Tomcat
WFM RTE Service	TCP 30001 (configurable)	ACMI Service (GED-188)
WFM Sync Service	TCP 59011	*unused*
Apache Tomcat	TCP 8087 TCP 8017 TCP 8007	HTTP AJP 1.3 Shutdown port

Table 2 lists the TCP and UDP ports used by WFM and its components on remote devices in the WFM environment, including the Unified CCX server and one or more client PCs.

Table 2. WFM Port Usage on Remote Devices

Server application protocol	Destination port (listening)	Client application protocol
CTI server*	TCP 42027 (configurable)	ACMI Service
Unified CCX instance of SQL Server	TCP 1433 TCP 1434	WFM Sync Service
WFM RTE Service	TCP 42027 (configurable)	Unified CCX instance of SQL Server
Apache Tomcat	TCP 8087 TCP 8017 TCP 8007	HTTP AJP 1.3 Shutdown port

*You can set this port number in the System Parameters window of the Unified CCX Administration web page. The parameter name for the port number is RmCm TCP Port. For more information, see *Managing System Parameters*, *Cisco Customer Response Solutions Administration Guide*.

System Requirements

2

Overview

This chapter describes the following requirements for WFM:

- System Requirements (page 16)
- System Capacity (page 20)
- Configuration Data (page 21)

System Requirements

The following tables list the minimum system requirements for the WFM server and clients.

System Environment

WFM has been verified in the following configurations:

Table 3. Verified configurations

ACD	PBX
Unified CCX 5.0	Cisco Unified CallManager (Unified CM) 5.1, 6.1
Unified CCX 6.0	Unified CM 4.3

Operating Environment

The WFM server requires the following operating system and hardware configuration.

Table 4. WFM server minimum configuration

Operating System	Hardware
Windows Server 2003 R2	• 3.4 GHz Dual Pentium 4 • 2 GB RAM • 146 GB hard disk space • Cisco Media Convergence Server (MCS) or equivalent* **NOTE:** Running WFM on a platform other than a Cisco MCS or exact equivalent is not supported by Cisco.

* For the latest information on supported MCS equivalent platforms (including IBM and HP), go to http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html.

WFM desktops require one of the following operating system and hardware configurations.

Table 5. WFM desktop minimum configuration

Operating System	Hardware
Windows 2000 Professional Service Pack 4 or greater	• 1 GHz processor or higher • 256 MB RAM or higher • 20 GB hard disk space • 100 Mbit NIC or higher
Windows XP Professional Service Pack 1 or greater	• 1 GHz processor or higher • 256 MB RAM or higher • 20 GB hard disk space • 100 Mbit NIC or higher
Windows Vista	• 1 GHz processor or higher • 1 GB RAM or higher • 40 GB hard disk space • 100 Mbit NIC or higher

Third Party Software Requirements

The WFM server requires the third party software listed in the following table.

NOTE: WFM requires the Cisco Media Convergence Server (MCS) platform to be a dedicated standalone server. Running other applications on the WFM server can adversely affect performance.

Table 6. WFM server minimum third party software requirements

Application	Where Installed/Description
Microsoft SQL Server 2005	Cisco MCS platform System configuration data is maintained using Microsoft SQL Server 2005. The customer must purchase and install SQL Server 2005. SQL Server 2005 is not installed as part of the product and must be installed prior to deploying WFM.

Table 6. WFM server minimum third party software requirements

Application	Where Installed/Description
Internet Explorer 6.0 or 7.0	Cisco MCS platform Internet Explorer is required to access the WFM web application. Vista only supports Internet Explorer 7.0.
Java 2 Runtime Environment (JRE) Standard Edition Version 5.0 (v1.5.0_11)	Cisco MCS platform Java 2 Runtime Environment is required to run the Java Server Pages (JSP) used by the WFM application. The version of JRE shipped with WFM meets the minimum requirements and is installed automatically on the Cisco MCS platform.
BIRT v2.1	Cisco MCS platform BIRT is an open source Eclipse-based reporting system. The version of BIRT shipped with WFM meets the minimum requirements and is installed automatically. For more information about BIRT, see http://www.eclipse.org/birt/phoenix.
Omnis v7.1	Cisco MCS platform Omnis is a rapid application development (RAD) tool. The version of Omnis shipped with WFM meets the minimum requirements and is installed automatically. For more information about Omnis, see http://www.omnis.net.
Apache Tomcat v5.5.9	Cisco MCS platform Apache Tomcat is a web container, or application server that provides an environment for Java code to run in cooperation with a web server. The version of Apache Tomcat shipped with WFM meets the minimum requirements and is installed automatically. For more information about Apache Tomcat, see http://tomcat.apache.org.

WFM desktops must have the following software applications:

Table 7. WFM desktop minimum third party software requirements

Application	Where Installed/Description
Internet Explorer 6.0 or 7.0	WFM client desktops Internet Explorer is required to access the WFM web application. Vista only supports Internet Explorer 7.0.

System Capacity

The system capacity for the WFM server can be defined by specific hardware and software configurations. The following table shows the limits of individual feature capacities.

NOTE: Capacity numbers are goals. Actual numbers may vary.

Table 8. System capacity

Attribute	Capacity
Maximum number of configured WFM users	900
Maximum number of concurrent WFM users	300
Maximum number of agents per team	150
Maximum number of skills per agent (for real time reporting)	50
Maximum number of supervisors per site	50
Maximum number of supervisors per team	30
Average agents per supervisor	7.5:1

The following table shows the hardware capacities per MCS server platform model.

Table 9. MCS server platform capacity by model

Administered Users	Concurrent Users	Server Model
Up to 450	Up to 150	MCS 7835
Up to 900	Up to 300	MCS 7845

Configuration Data

The following data needs to be stored persistently and must be backed up on a regular basis:

- WFM database (named CWFM)
- Customer-specific configuration files, such as the files in C:\Program Files\Cisco\WFO_WFM\config

WFM database backups are independent of Unified CCX backup and restore (BARS) tools. Use standard SQL Server 2005 tools to manually back up and restore the WFM database.

> **NOTE:** If you are running Cisco Security Agent (CSA) on your WFM server, shut CSA down before you back up the WFM database. If CSA is running while you run SQL Server utilities to backup the WFM database, the backup may fail.

Before You Install WFM

3

Overview

This chapter describes how to configure the WFM server before you install WFM. This process consists of the following tasks.

- Installing Microsoft SQL Server 2005 (page 24)
- Creating a SQL Server Login for WFM (page 25)
- Configuring Firewall Port Exceptions (page 26)

Installing Microsoft SQL Server 2005

An abbreviated installation procedure is given below. For detailed information about how to install Microsoft SQL Server 2005, see the Microsoft SQL Server 2005 installation documentation.

Complete the following steps of the Microsoft SQL Server 2005 Setup utility:

1. On the Registration Information window, fill in your name, company, and product key.
2. On the Components to Install window, select the SQL Server Database Services and Workstation Components check boxes and any additional components if desired.
3. On the Instance Name window, select either Default instance or Named instance.

   NOTE: If you select Named instance, you must specify the instance name.

4. On the Service Account window, select Use the Built-In System Account, then select Local System from the drop-down list. Under Start Services at the End of Setup, highlight SQL Server, SQL Server Agent, and SQL Browser.
5. On the Authentication Mode window, select Mixed Mode. Enter a password for the SQL Server System Administrator (sa) logon.
6. On the Collation Settings window, under Collation Designator and Sort Order, select Latin1_General from the drop-down list, then select the Accent - sensitive check box. Do not select any of the other check boxes.

   NOTE: The SQL collation name is SQL_Latin1_General_CP1_CI_AS. For more information about SQL Server collation settings, see http://msdn2.microsoft.com/en-us/library/ms180175.aspx.

Creating a SQL Server Login for WFM

NOTE: Store the WFM SQL Server login name and password in a safe place. You will need this information for the WFM Configuration Setup utility, which runs automatically after you install WFM.

To create a SQL Server login for WFM:

1. On the SQL Server computer, start Microsoft SQL Server Management Studio.
2. In the Object Explorer pane, expand the SQL Server instance. Choose **Security > Logins**.
3. Right-click Logins and choose New Login.
4. The Login - New window appears.
5. On the General page, enter the login you want to use for WFM. Select SQL Server Authentication, enter a password, and clear the Enforce password policy check box.
6. On the Server Roles page, select dbcreator from the list of server roles.

   NOTE: The WFM SQL Server login must be able to create databases.

7. Click OK. The new login is added to the list of logins in the right pane.

Configuring Firewall Port Exceptions

Before you install WFM, if Microsoft Windows Firewall is enabled on the WFM server, you must manually add several ports to the firewall exception list. These ports are listed in Table 10.

> **NOTE:** For a complete list of ports used in a WFM environment, see Port Usage (page 13).

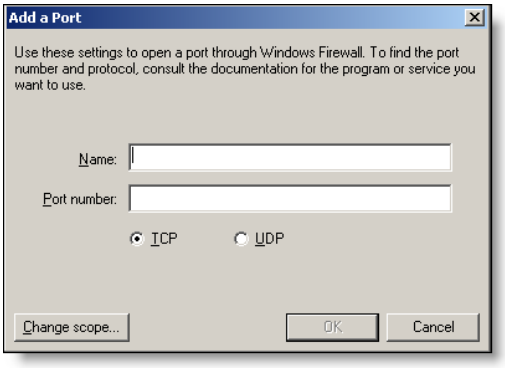
Table 10. Microsoft Windows Firewall Port Exceptions

Server application protocol	Listening Port	Client application protocol
Workforce Management RTE Service	TCP 42027 (configurable)	Unified CCX instance of SQL Server
Apache Tomcat	TCP 8087 TCP 8017 TCP 8007	HTTP AJP 1.3 Shutdown port

To add a port to the Microsoft* Windows *Firewall exceptions list:

1. On the WFM server, choose **Start > Settings > Control Panel > Windows Firewall**.
2. On the Exceptions tab, click Add Port. The Add a Port window appears (Figure 1).

Figure 1. Add a Port



3. Enter a name that describes the port, then enter the port number. Select the appropriate connection type, then click OK.
4. When you are finished adding ports, click OK to close Microsoft Windows Firewall.

Installing and Configuring WFM

4

Overview

This chapter describes how to install and configure WFM. This process consists of the following tasks.

Verifying Prerequisites

NOTE: There is a 25-character limit on team names in WFM. Team names that are longer than 25 characters will not be imported from Unified CCX into WFM. Before you install WFM and start the Workforce Management services, verify that all Unified CCX team names are 25 or fewer characters in length.

Before you install WFM, you must install and configure the following systems.

- Cisco Unified Contact Center Express (Unified CCX)
- Cisco Unified Communications Manager (Unified CM) or Unified Communications Manager Express (Unified CME)
- Cisco Unity server

To install WFM, you need the following information.

- WFM server IP address
- WFM SQL Server database username and password you used in "Creating a SQL Server Login for WFM" on page 25, as well as the instance name you used in "Installing Microsoft SQL Server 2005" on page 24 (if you did not use the default instance)
- Unified CM IP address and port number
- CTI server IP address and port number (see "Port Usage" on page 13)
- Quality Management (QM) server IP address, if you have QM
- Unified CCX database IP addresses for Side A and optionally Side B, as well as the instance name

You also need the following information for Active Directory.

- Active Directory distinguished names (and ports, if you are not using the default port)
- Active Directory paths to the users
- Common names (CN) from the Active Directory account and password

Upgrading from WFM 8.0 to WFM 8.2

NOTE: Before you upgrade, consider running the WFM 8.0 version of WFM Configuration Setup so you can make a note of the settings you used when you installed WFM 8.0. Your WFM 8.0 settings are not maintained during the upgrade process. You will need to enter them again after you install WFM 8.2.

To upgrade from WFM 8.0 to WFM 8.2:

1. Back up your SQL Server WFM 8.0 database using SQL Server backup tools.

   NOTE: The SQL Server WFM 8.0 database is not removed during the upgrade process. However, backing up your database is recommended in case a problem occurs during the upgrade.

2. Uninstall WFM 8.0. For instructions, see "Removing WFM" on page 55.
3. Install WFM 8.2. For instructions, see "Installing WFM" on page 30.

Installing WFM

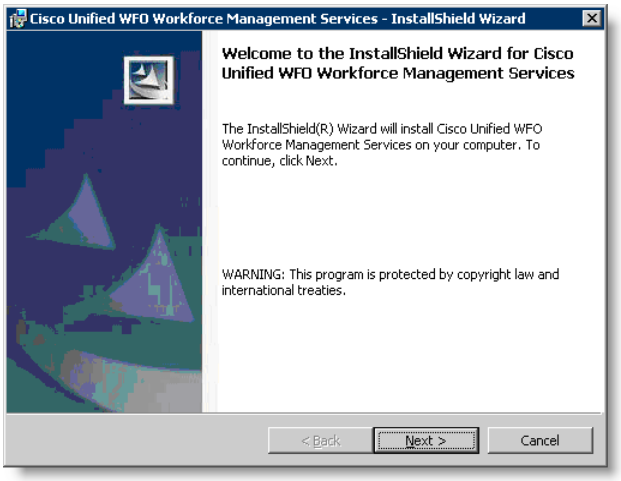
NOTE: If Cisco Security Agent (CSA) is running on your WFM server, shut CSA down before you begin the installation process. If CSA is running while you install WFM, the installation may fail.

To install WFM:

Complete these steps on the Cisco Unified WFO Workforce Management server.

1. Load the installation CD in the server computer, and then navigate to the CD in My Computer or Windows Explorer.
2. Double-click the file setup.exe to start the installation wizard. The Cisco Unified WFO Workforce Management Services - InstallShield Wizard Welcome window appears (Figure 2).

Figure 2. Welcome



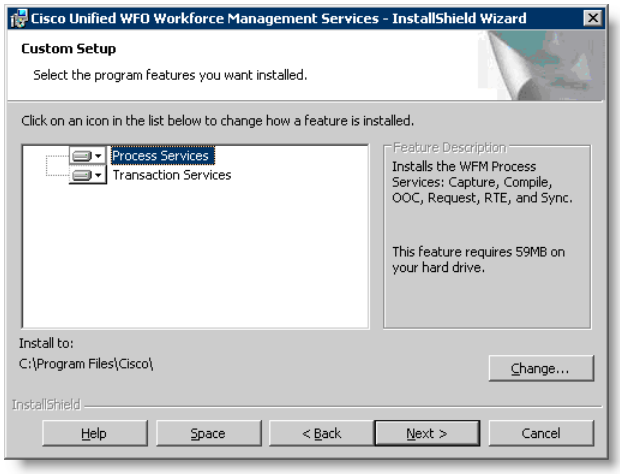
3. Click Next to continue. The Custom Setup window appears (Figure 3).

NOTE: The default installation directory is C:\Program Files\Cisco. If you want to change the default installation directory, click Change and follow the prompts.

NOTE: The only installation setting that is customizable on this window is the installation directory. Both components are required.

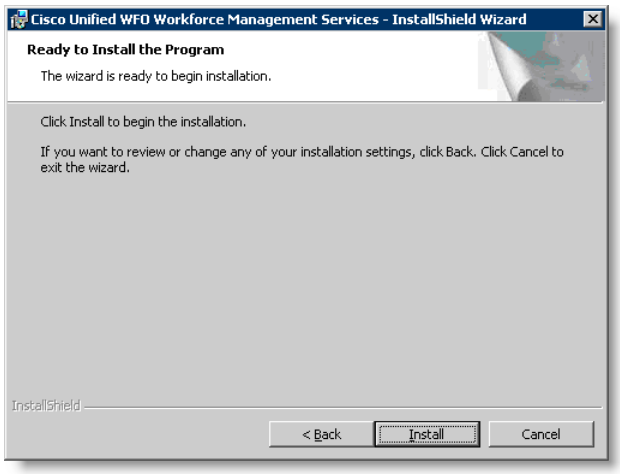
Selecting a single component and clicking Next results in the installation of both components.

Figure 3. Custom Setup



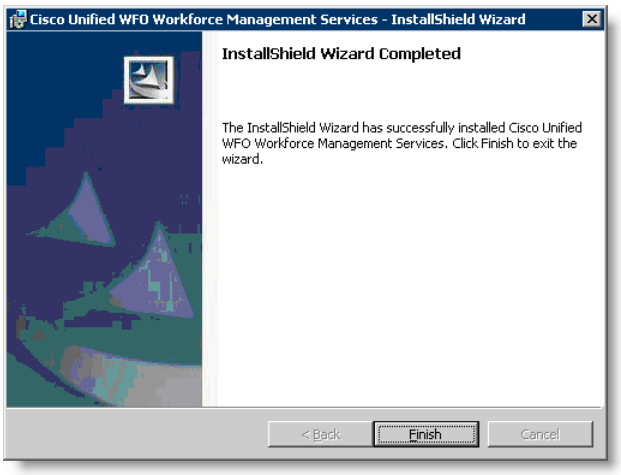
4. Click Next to continue. The Ready to Install the Program window appears (Figure 4).

Figure 4. Ready to Install the Program



5. Click Install to continue. The installation wizard installs WFM, Birt, Omnis, Java 2 Runtime Environment (JRE), and the Apache Tomcat Webserver. The InstallShield Wizard Completed window appears when the InstallShield Wizard completes the installation (Figure 5).

Figure 5. InstallShield Wizard Completed



6. Click Finish to complete the installation. The WFM Configuration Setup utility is launched automatically and the WFM Server window appears (Figure 6). Go to "Step 1. Specifying the WFM Server Address" on page 34.

Configuring WFM

To configure WFM, run WFM Configuration Setup, which consists of the steps below.

- Step 1. Specifying the WFM Server Address (page 34)
- Step 2. Specifying WFM Database Access (page 35)
- Step 3. Configuring WFM Administrator Access (page 36)
- Step 4. Configuring Active Directory (page 37)
- Step 5. Specifying the Unified CCX Database (page 38)
- Step 6. Specifying the CTI Server (page 39)
- Step 7. Specifying the Unified CM Server (page 41)

The WFM Configuration Setup utility has two modes: initial mode and update mode. The utility is launched automatically in initial mode after the WFM installation finishes. After you configure all of the required parameters and exit WFM Configuration Setup, the utility starts the Workforce Management services. If you need to change certain configuration settings later, you can run the utility again manually in update mode.

> **NOTE:** When you are running WFM Configuration Setup in update mode, you cannot modify WFM Database settings or enable/disable Active Directory. To change those settings, you must re-install WFM.

If you need to manually launch WFM Configuration Setup, see "Launching WFM Configuration Setup Manually" below for instructions. Otherwise, skip ahead to "Step 1. Specifying the WFM Server Address" on page 34.

> **NOTE:** If an error message appears while running WFM Configuration Setup, correct the problem and try again. For more information about an error, see *Cisco Workforce Management Service Information*.

> **NOTE:** WFM Configuration Setup runs only on the WFM server.

Launching WFM Configuration Setup Manually

> **NOTE:** If WFM Configuration Setup is already running, skip ahead to "Step 1. Specifying the WFM Server Address" on page 34.

To launch WFM Configuration Setup manually:

1. On the WFM server, navigate to C:\Program Files\Cisco\WFO_WFM\bin.

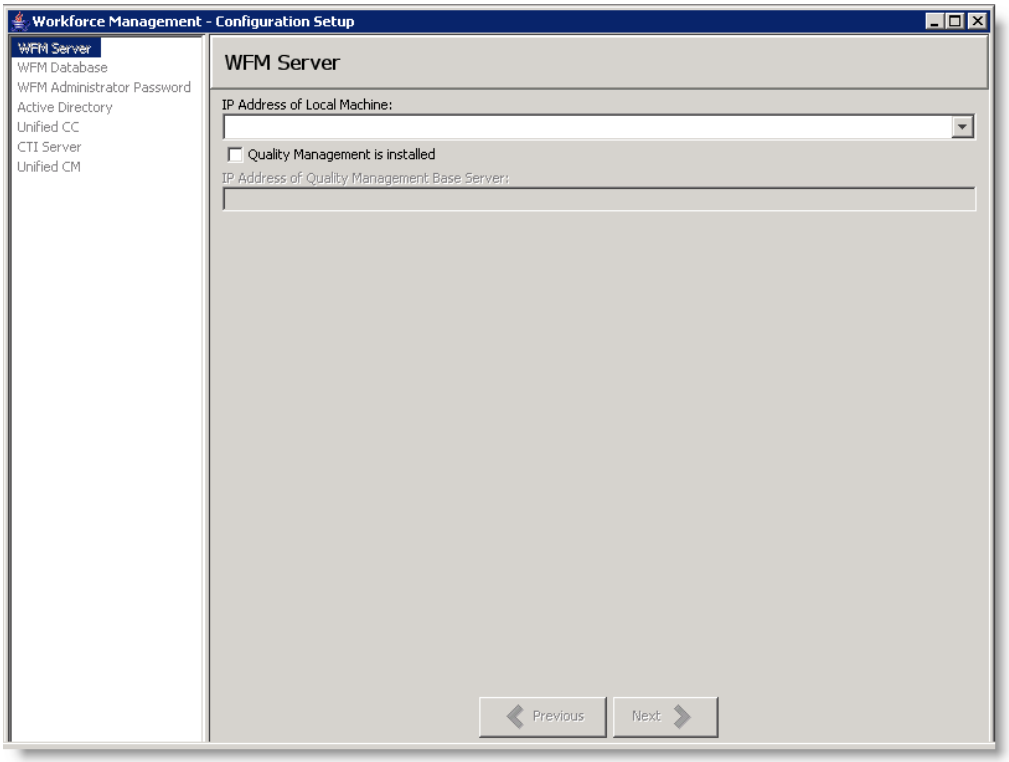
2. Run postinstall.exe. The Workforce Management — Configuration Setup window appears.
3. Go to "Step 1. Specifying the WFM Server Address" on page 34.

Step 1. Specifying the WFM Server Address

To specify the server address:

1. From the WFM Server window (Figure 6), select an IP address from the IP Address of Local Machine drop-down list or enter the IP address for the local machine on which WFM is installed.

Figure 6. WFM Server



2. If QM is installed (as part of WFO), select the Quality Management is Installed check box and enter the IP address for the QM base server.
3. Click Next to go to the next window. The WFM Database window appears.
4. Go to "Step 2. Specifying WFM Database Access" on page 35.

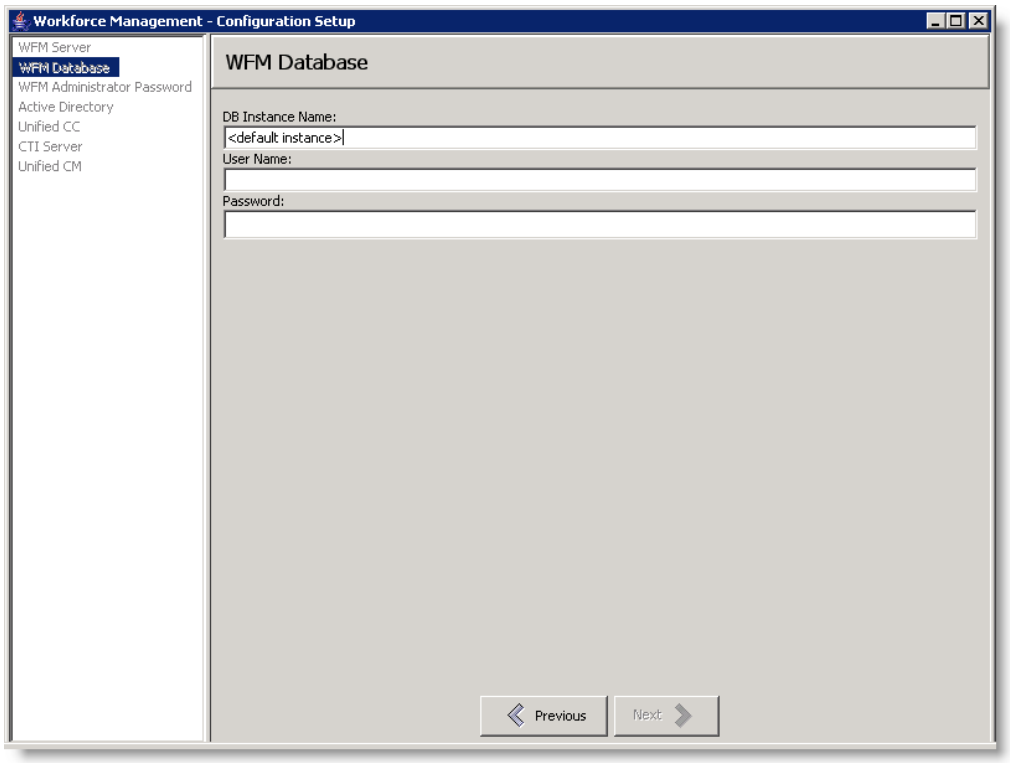
Step 2. Specifying WFM Database Access

To specify WFM database access:

1. From the WFM Database window (Figure 7), enter the instance name, login name, and password you used in "Installing Microsoft SQL Server 2005" on page 24 and "Creating a SQL Server Login for WFM" on page 25.

   NOTE: The DB Instance Name field is pre-populated with the text "<default instance>". Do not edit this unless using a named instance.

Figure 7. WFM Database



2. Click Next. WFM Configuration Setup connects to SQL Server, creates the WFM database, and loads default data. If successful, a confirmation appears.

   NOTE: If an error message appears, verify that SQL Server is running on the local machine and that you entered the correct information in step 1.

3. Click OK to dismiss the dialog box. The WFM Administrator Password window appears.
4. Go to "Step 3. Configuring WFM Administrator Access" on page 36.

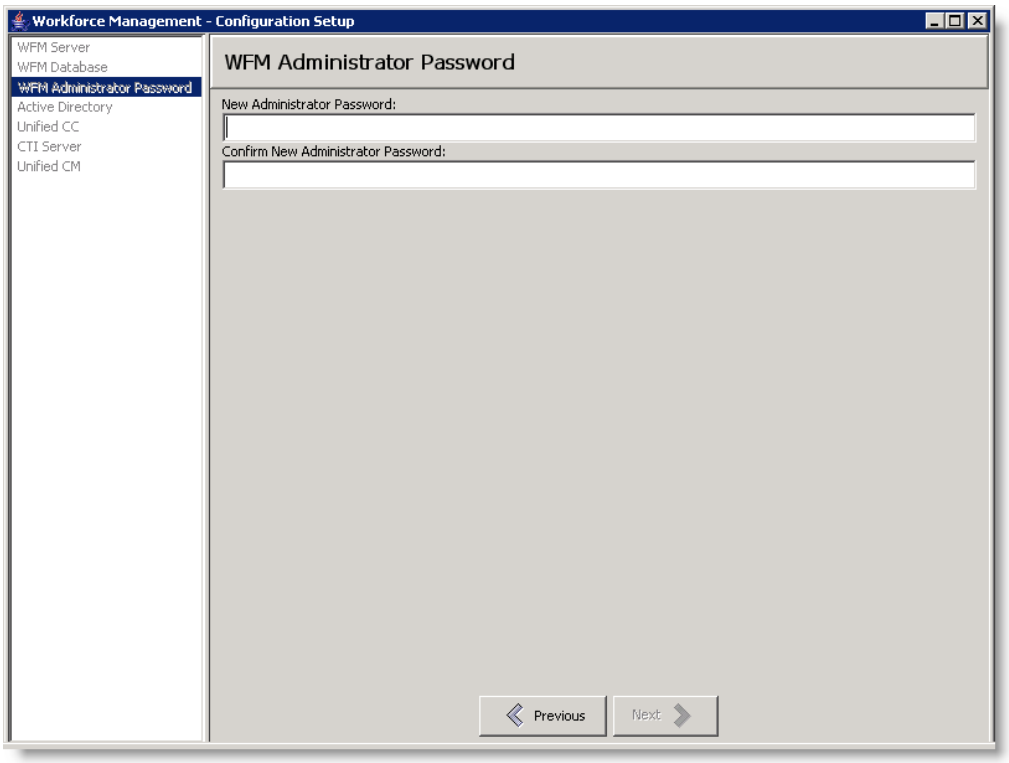
Step 3. Configuring WFM Administrator Access

To configure WFM administrator access:

1. From the WFM Administrator Password window (Figure 8), enter the password for the WFM administrator using one of the methods below.
   - If you are upgrading WFM, enter the password that you used the first time you installed WFM in the Current Administrator Password field.
   - If you are installing WFM for the first time, enter a password in the New Administrator Password and Confirm New Administrator Password fields.

   NOTE: Store this password in a safe place. You will need it to log into WFM as an administrator.

Figure 8. WFM Administrator Password



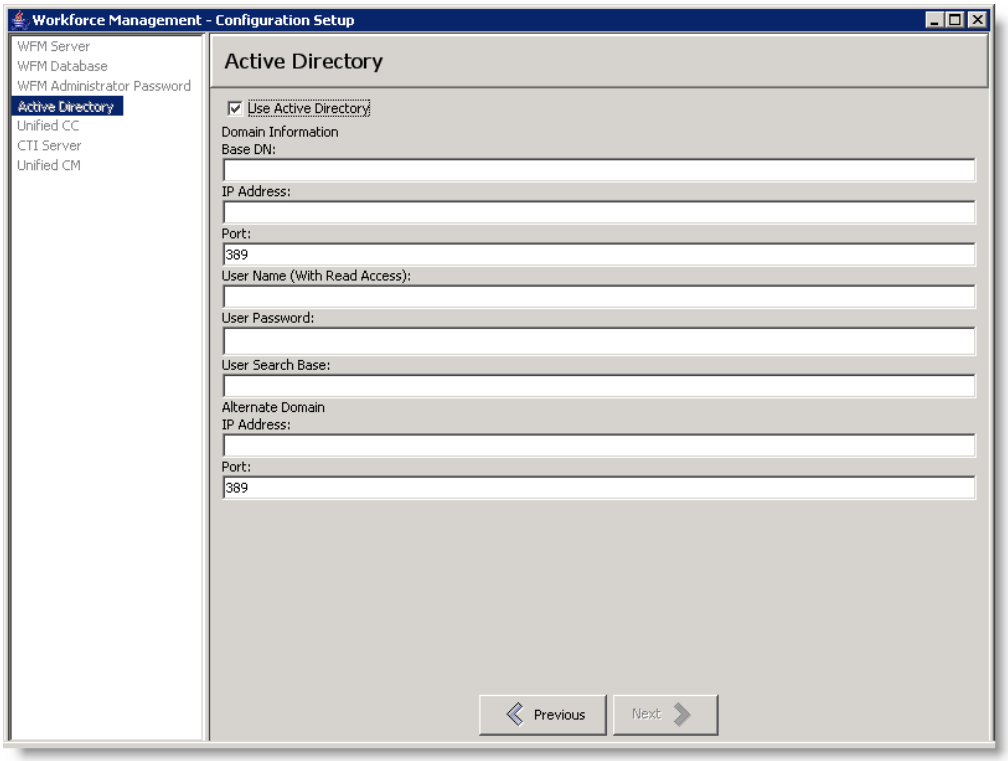
2. Click Next. The Active Directory window appears.
3. Go to "Step 4. Configuring Active Directory" on page 37.

Step 4. Configuring Active Directory

To configure Active Directory:

1. Complete one of the following options.
   - If you want to use Active Directory, leave the Use Active Directory check box selected in the Active Directory window (Figure 9) and go to step 2.
   - If you do not want to use Active Directory, clear the Use Active Directory check box, then skip to step 6 below.

Figure 9. Active Directory



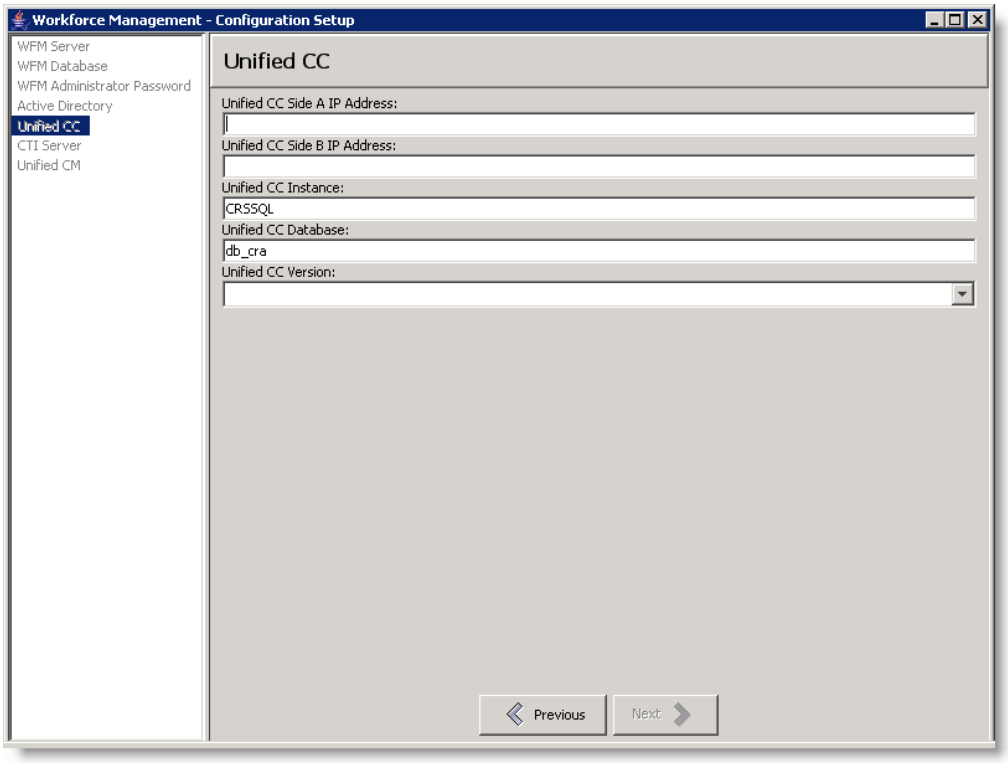
2. Enter the Active Directory distinguished name and IP address in the Base DN and IP Address fields. Update the Port field if you are not using the default.
3. Enter the Active Directory user and password in the User Name and User Password fields. WFM uses this information to access Active Directory.
4. Enter the organizational units (OU) in the User Search Base field.
5. If you have a redundant Active Directory server, enter its IP address in the IP Address field. Update the Port field if you are not using the default.
6. Click Next. The Unified CC window appears.
7. Go to "Step 5. Specifying the Unified CCX Database" on page 38.

Step 5. Specifying the Unified CCX Database

To specify the Unified CCX database:

1. From the Unified CC window, enter the IP address for the Unified CCX (Unified CC) Side A server (Figure 10).

Figure 10. Unified CCX (Unified CC)



2. Complete one of the following actions for the Unified CC Side B IP Address field.
   - If your environment has a Unified CCX Side B server, enter its IP address.
   - If your environment does not have a Side B server, leave the field blank.
3. Enter the Unified CCX (Unified CC) SQL Server instance and database names.

   NOTE: The default settings are most commonly used.

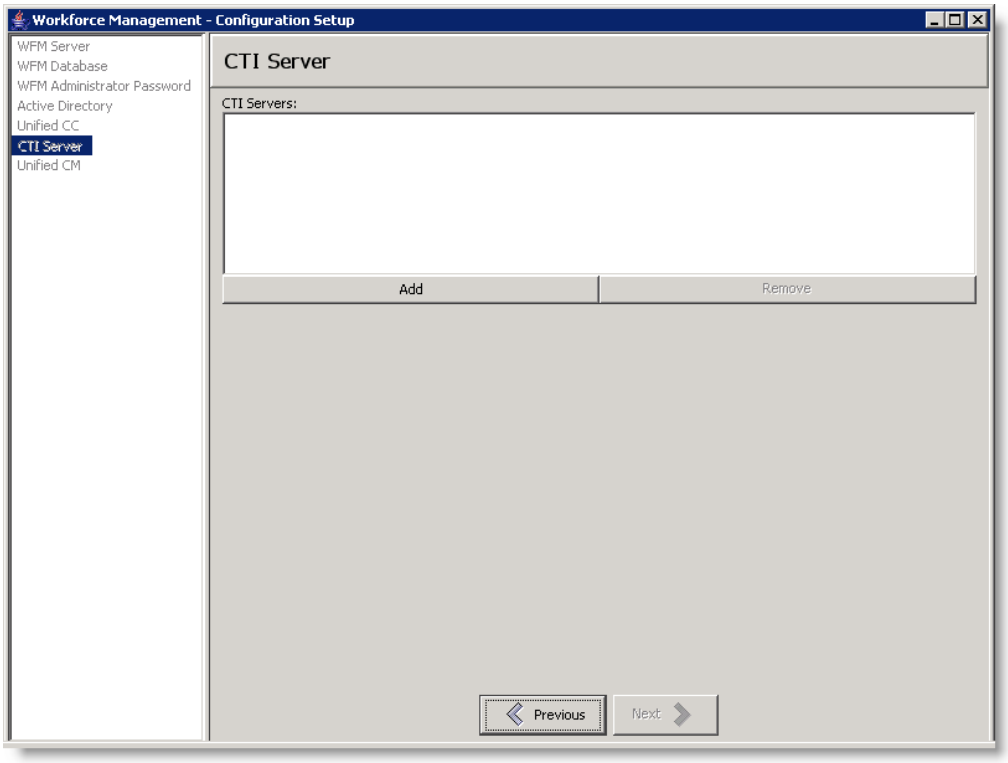
4. Select the Unified CCX version running in your environment from the list. The available options are Express 5.0 and Express 6.0.
5. Click Next. The CTI Server window appears.
6. Go to "Step 6. Specifying the CTI Server" on page 39.

Step 6. Specifying the CTI Server

To specify the CTI server:

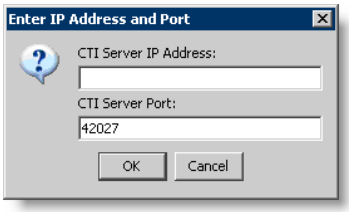
1. From the CTI Server window (Figure 11), add one or more CTI servers by completing the following steps.

Figure 11. CTI Server



a. Click Add. The Enter IP Address and Port dialog box appears (Figure 12).

Figure 12. Enter IP Address and Port



b. Enter the CTI server IP address and port, then click OK. The dialog box closes and the new IP address and port appear in the CTI Servers list.

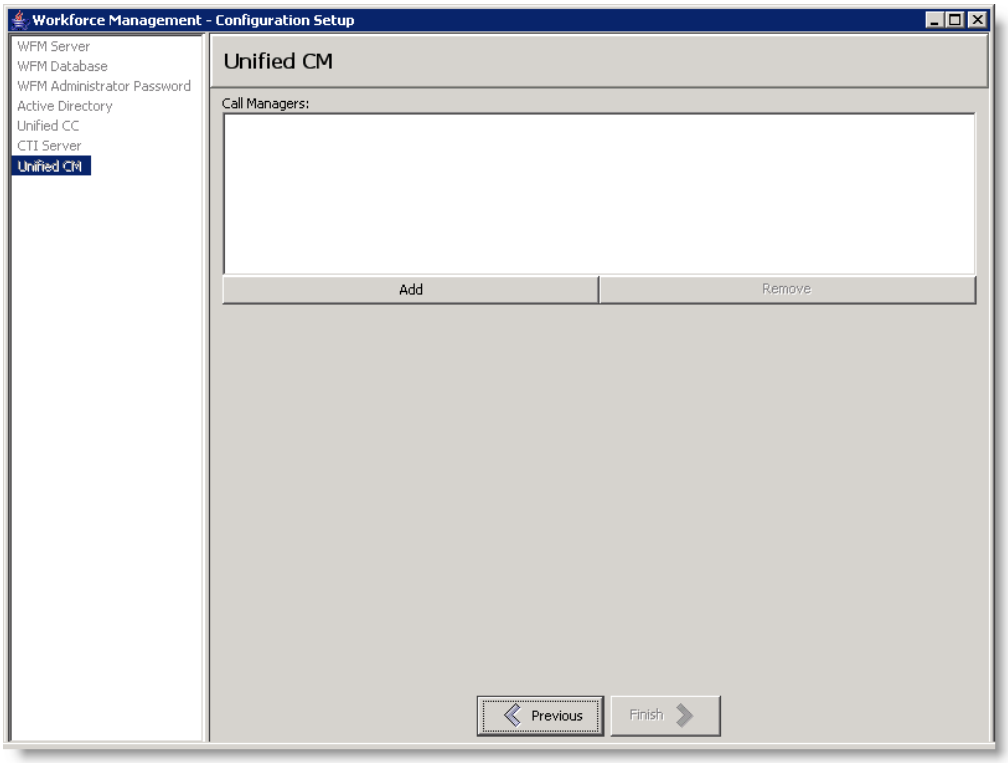
2. If you need to remove a server, complete the following steps.
   a. Select a server from the CTI Servers list.
   b. Click Remove. The IP address and port number disappear from the CTI Servers list.
3. Click Next. The Unified CM window appears.
4. Go to "Step 7. Specifying the Unified CM Server" on page 41.

Step 7. Specifying the Unified CM Server

To specify the Unified CM server:

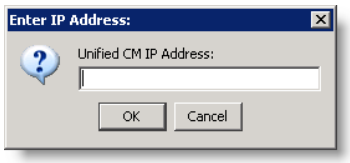
1. From the Unified CM window (Figure 13), add one or more Unified CM servers by completing the following steps.

Figure 13. Unified CM



   a. Click Add. The Enter IP Address dialog box appears (Figure 14).

Figure 14. Enter IP Address



   b. Enter the Unified CM server IP address, then click OK. The dialog box closes and the new IP address appears in the Unified CM Servers list.

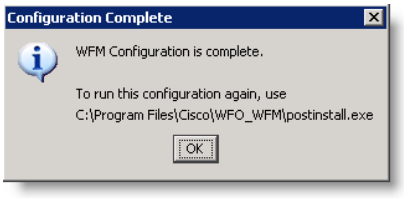
2. If you need to remove a server, complete the following steps.

   a. Select a server from the Unified CM Servers list.

b. Click Remove. The IP address disappears from the Unified CM Servers list.

3. Click Finish. The Workforce Management services are started. After all of the services have started, a confirmation appears.
4. Click OK to dismiss the dialog box. The Configuration Complete dialog box appears (Figure 15).

Figure 15. Configuration Complete



5. Click OK to dismiss the dialog box. The Workforce Management — Configuration Setup window closes. You have now completed the installation of WFM.

Configuring NT Authentication for Unified CC

You must complete the following steps after you install WFM and before you start using WFM to administer users.

Step 1. Creating WFM Users for the Unified CCX Database

On both the WFM server and the Unified CCX server, create Windows logins that WFM can use to connect to the Unified CCX database.

NOTE: The Unified CCX server cannot be on a domain.

NOTE: The WFM user must also have write access to the folder C:\Program Files\Cisco\WFO_WFM\log on the WFM server so the WFM services can write to log files in the directory.

NOTE: The following procedure is written assuming that the Unified CCX server is running Windows Server 2003.

To create WFM users for the Unified CCX database:

1. On the WFM server, create a new user by completing the following steps.
   a. From the Start Menu, choose **Programs > Administrative Tools > Computer Management**.
   b. Expand Local Users and Groups. Right-click Users and choose New User.
   c. Enter a user name and password.
   d. Clear the User Must Change Password at Next Logon check box and select the Password Never Expires check box.
   e. Click Create, then Close. The new user is added to the list of users.
2. On the WFM server, add the new user to the Administrator group by completing the following steps.
   a. Right-click the name of the user you just created and choose Properties. The user properties dialog box appears.

b. Go to the Member Of tab and click Add. The Select Groups dialog box appears.

c. Click Advanced. Another Select Groups dialog box appears.

d. Click Find Now. A list of groups appears.

e. Highlight the Administrators group and click OK twice to close both Select Groups dialog boxes.

f. Click OK again to close the user properties dialog box, then click the close window icon to close the Computer Management window.

3. On the WFM server, grant the new user permission to log on as a service by completing the following steps.

a. Choose **Start > Programs > Administrative Tools > Local Security Policy**. The Local Security Settings window appears.

b. In the left pane, choose **Local Policies > User Rights Assignment**.

c. In the right pane, double-click Log on as a service. The Log on as a service Properties dialog box appears.

d. Click Add User or Group. The Select Users, Computers, or Groups dialog box appears.

e. Click Advanced. The Select Users or Groups dialog box appears.

f. Click Find Now. A list of users and groups appears.

g. Select the name of the new user from the list, click OK twice to close the Select Users or Groups dialog boxes, then click OK to close the Log on as a service Properties dialog box.

h. Choose **File > Exit** to close the Local Security Settings window.

4. On the Unified CCX server, create a new user by completing the following steps.

a. From the Start Menu, choose **Programs > Administrative Tools > Computer Management**.

b. Expand Local Users and Groups. Right-click Users and choose New User.

c. Enter a user name and password.

NOTE: Use the same name and password for the new user that you used on the WFM server in step 1.

d. Clear the User Must Change Password at Next Logon check box and select the Password Never Expires check box.

e. Click Create, then Close. The new user is added to the list of users.

5. On the Unified CCX server, add the new user to the Administrators group and the Users group by completing the following steps.
   a. Right-click the name of the user you just created and choose Properties. The user properties dialog box appears.
   b. Go to the Member Of tab and click Add. The Select Groups dialog box appears.
   c. Click Advanced. Another Select Groups dialog box appears.
   d. Click Find Now. A list of groups appears.
   e. Highlight the Administrators group and the Users group and click OK twice to close both Select Groups dialog boxes.
   f. Click OK again to close the user properties dialog box, then click the close window icon to close the Computer Management window.

Step 2. Configuring WFM Services to Run As the New User

To configure the Workforce Management Sync and OOC services to run as the new user:

1. On the WFM server, choose **Start > Programs > Administrative Tools > Services**.
2. Complete the following steps for the Workforce Management Sync Service.
   a. Right-click the name of the service and choose Properties. The properties dialog box for the service appears.
   b. Click Stop and wait for the service to stop.
   c. Go to the Log On tab and select This Account. Enter the name and password of the Windows user you created in Step 1.
   d. Click OK, then click the General tab.
   e. Click Start to restart the service.

   NOTE: The service must be restarted for your changes to take effect.

   f. After the service starts, click OK to dismiss the properties dialog box for the service.
   g. Choose **File > Exit** to close the Services Management Console.
3. Repeat the previous step for the Workforce Management OOC Service.

Step 3. Granting the New User Access to the Unified CCX Database

NOTE: The following procedure is written assuming that the Unified CCX database is in Microsoft SQL Server 2000.

To grant the new user access to the Unified CCX database:

1. On the Unified CCX server, start Microsoft SQL Server Enterprise Manager.
2. Under the Unified CCX instance, choose **Security > Logins**. A list of Windows and SQL Server users who have permission to access the databases in this instance appears.
3. Right-click Logins and choose New Login. The SQL Server Login Properties - New Login dialog box appears.
4. Click the button to the right of the name field to browse for the new user you created in Step 1 (page 43). A second SQL Server Login Properties - New Login dialog box appears.
5. Select the machine name from the List Names From list. A list of users and groups defined on the machine appears.
6. Select the new user, then click Add. The user name appears in the Add Name field.
7. Click OK to dismiss the second SQL Server Login Properties - New Login dialog box.
8. On the Database Access tab, select the Permit check box for the side A database, then select the Permit in Database Role check box for db_datareader.
9. If there is a side B database, select the Permit check box for the side B database, then select the Permit in Database Role check box for db_datareader.
10. Click OK to dismiss the SQL Server Login Properties - New Login dialog box.
11. Choose **Console > Exit** to close SQL Server Enterprise Manager.

Step 4. Verifying the Database Connection

To verify the database connection from WFM to the Unified CCX database:

1. Enter the following URL in your web browser, where *wfm* is either the name or the IP address of the server on which WFM is installed.

   `http://wfm:8087/c3/`

   NOTE: The website address is case sensitive.

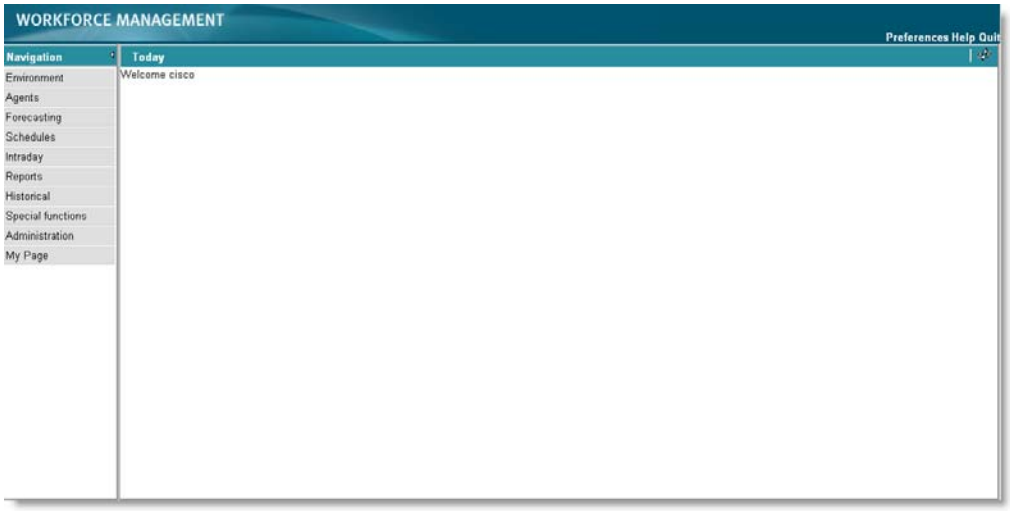
   The Workforce Management login window appears (Figure 16).

Figure 16. Workforce Management login window

2. Enter **administrator** in the username field.

3. Enter the password that you specified in WFM Configuration Setup on page 36, then click GO. The Workforce Management window appears (Figure 17).

Figure 17. Workforce Management



4. Choose **Agents** > **Agents**. If the right pane displays a list of agents, the synchronization was successful.
5. Navigate to C:\Program Files\Cisco\WFO_WFM\log. Open the Workforce Management OOC Service log file, which is named *yyyymmdd*-ooCollector.log, where *yyyymmdd* is the date. Verify that the log file does not contain any error messages.

Configuring Regional Settings

The Workforce Management OOC Service must use US English regional settings. Verify that the server hosting WFM has the following registry settings.

HKEY_USERS\.DEFAULT\Control Panel\International\

Table 11. Regional settings

Key	Value	Type	Data
International	iCalendarType	string	1
	iCountry	string	1
	iCurrDigits	string	2
	iCurrency	string	0
	iDate	string	0
	iDigits	string	2
	iFirstDayOfWeek	string	6
	iFirstWeekOfYear	string	0
	iLZero	string	1
	iMeasure	string	1
	iNegCurr	string	0
	iNegNumber	string	1
	iTime	string	0
	iTimePrefix	string	0
	iTLZero	string	0
	Locale	string	00000409
	NumShape	string	1
	s1159	string	AM
	s2359	string	PM
	sCountry	string	United States
	sCurrency	string	$
	sDate	string	/
	sDecimal	string	.

Table 11. Regional settings

Key	Value	Type	Data
International	sGrouping	string	3;0
	sLanguage	string	ENU
	sList	string	,
	sLongDate	string	dddd, MMMM dd, yyyy
	sMonDecimalSep	string	.
	sMonGrouping	string	3;0
	sMonThousandSep	string	,
	sNativeDigits	string	0123456789
	sNegativeSign	string	-
	sPositiveSign	string	
	sShortDate	string	mm-dd-yyyy
	sThousand	string	,
	sTime	string	;
	sTimeFormat	string	h:mm:ss tt

Capturing Historical Call Data

5

Overview

The WFM forecasting feature uses your contact center's historical call data to estimate future call volume and scheduling requirements. The Workforce Management OOC Service retrieves data automatically every 30 minutes, starting from the time you installed WFM.

If you want to use historical call data from the time before you installed WFM, you must complete the procedures in this chapter to capture the data manually.

For more information about the forecasting feature, see *Workforce Management Administrator User Guide for Cisco Unified Workforce Optimization*.

NOTE: You must complete the procedures described in this chapter immediately after you install WFM.

NOTE: There is a 25-character limit on team names in WFM. Team names that are longer than 25 characters will not be imported from Unified CCX into WFM. Before you complete the procedures in this chapter, verify that all Unified CCX team names are 25 or fewer characters in length.

Capturing CSQ Historical Call Data

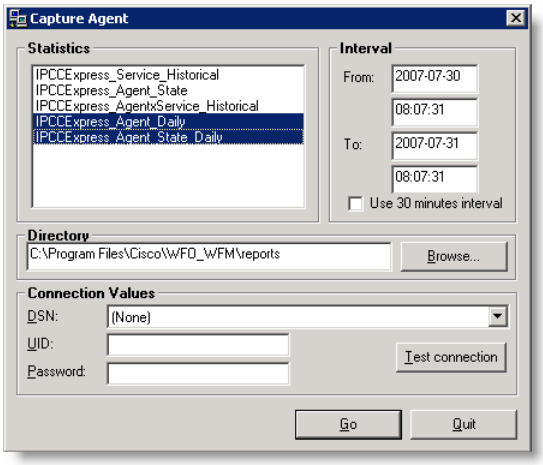
To capture CSQ historical call data:

1. From the WFM server, choose **Start** > **Programs** > **Cisco** > **WFO** > **WFM** > **OOC**. The Odysoft ODBC Collector window appears (Figure 18).

Figure 18. Odysoft ODBC Collector

2. Choose **Collector** > **Capture**. The Capture Agent window appears (Figure 19).

Figure 19. Capture Agent - Historical CSQ data



3. In the From fields in the Interval pane on the right, enter the beginning date and time for the historical call reference period.
4. In the To fields, enter the ending date and time for the historical call reference period.
5. Highlight the last two statistics queries in the Statistics pane as shown in Figure 19.
6. Clear the Use 30 minutes interval check box.
7. Enter the following directory path in the Directory field:

   `C:\Program Files\Cisco\WFO_WFM\reports`

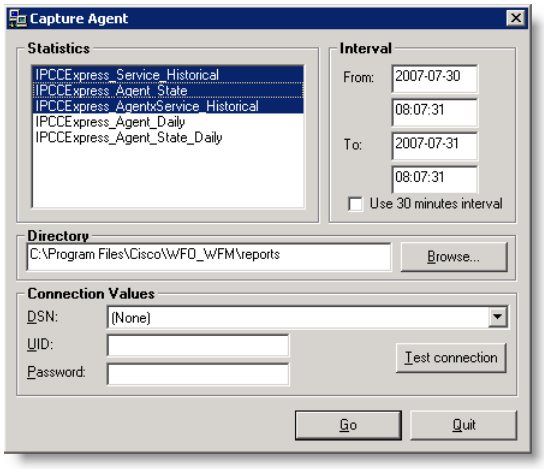
8. Select the Unified CCX DSN from the DSN field.
9. Enter the Unified CCX user ID and password.
10. Click Test connection to verify the connection is working.
11. Click Go to capture the historical call data. The reports are created and saved to the folder C:\Program Files\Cisco\WFO_WFM\reports.
12. When the hourglass disappears, click Quit to exit the Capture Agent window.
13. Choose **Collector > Quit** to exit Odysoft ODBC Collector.

Capturing Agent Historical Call Data

To capture agent historical call data:

1. From the Odysoft ODBC Collector window, choose **Collector** > **Capture**. The Capture Agent window appears (Figure 20).

Figure 20. Capture Agent - Historical Agent data



2. In the From fields in the Interval pane on the right, enter the beginning date and time for the historical call reference period.
3. In the To fields, enter the ending date and time for the historical call reference period.
4. Highlight the first three statistics queries in the Statistics pane as shown in Figure 20.
5. Select the Use 30 Minutes Interval check box.
6. Enter the following directory path in the Directory field:

   `C:\Program Files\Cisco\WFO_WFM\reports`
7. Select the Unified CCX DSN from the DSN field.
8. Enter the Unified CCX user ID and password.
9. Click Test Connection to verify the connection is working.
10. Click Go to capture the historical call data. The reports are created and saved to the folder C:\Program Files\Cisco\WFO_WFM\reports.
11. When the hourglass disappears, click Quit to exit the Capture Agent dialog.
12. Choose **Collector** > **Quit** to exit Odysoft ODBC Collector.

Verifying Historical Call Data Capture

When you finish capturing the historical call data, the capture module processes the reports in the folder C:\Program Files\Cisco\WFO_WFM\reports and moves them to the folder C:\Program Files\Cisco\WFO_WFM\archives.

The historical call data capture is complete when there are no more reports in the folder C:\Program Files\Cisco\WFO_WFM\reports.

Removing WFM

6

Removing WFM

NOTE: When you remove WFM, the SQL Server WFM database is not removed.

To remove WFM:

1. From the **Start** menu, choose **Settings** > **Control Panel**.
2. Double-click Add or Remove Programs.
3. Select Cisco Unified WFO Workforce Management Services, click Remove, and follow the prompts.

The following table lists the programs you will find on the server.

Table 12. Applications on the server

Server	Applications to Remove
Cisco Unified WFO Workforce Management Server	Cisco Unified WFO Workforce Management Services*

* JRE and Tomcat are automatically removed when you remove Cisco Unified WFO Workforce Management Services.

Index