



Cisco Unified Workforce Optimization

Workforce Management Installation Guide 8.5(2)
Revised April 2012

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

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

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

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

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

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

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

Workforce Management Installation Guide

© 2011–2012 Cisco Systems, Inc. All rights reserved.

© 2011–2012 Calabrio, Inc. All rights reserved.

Contents

- 1 Overview 7**
 - Introduction 7
 - What's New in This Version 8
 - WFM Documentation 8
 - Workforce Management Services 9
 - Workforce Management ACC Service 9
 - Workforce Management Capture Service 9
 - Workforce Management Compile Service 9
 - Workforce Management Jetty Service 9
 - Workforce Management Mana Service 9
 - Workforce Management Product Adapter Service 9
 - Workforce Management Real Time Service 9
 - Workforce Management Real Time Engine Service 10
 - Workforce Management Request Service 10
 - Workforce Management Schedule Service 10
 - Workforce Management Sync Service 10
 - Workforce Management Tomcat Service 10
 - Environment and Port Usage 11

- 2 System Requirements 13**
 - Overview 13
 - System Requirements 14
 - Cisco Unified Workforce Optimization Environment 14
 - System Environment 14
 - Operating Environment 14
 - Server Operating Systems 14
 - Hardware Requirements and Capacity 14
 - WFM in a Cisco Unified Computing System Environment 15
 - WFM in a Virtual Server Environment 15
 - Desktop Requirements 16
 - Third Party Software 16
 - Web Browser Considerations 17

Contents

- Server Configurations 18
 - Concurrent SQL Server Versions 18
 - Single Server Configuration 18
- Configuration Data 20

3 Before You Install WFM 21

- Overview 21
- Installing Microsoft SQL Server 22
- Creating a SQL Server Login for WFM 24
- Configuring Firewall Port Exceptions 25
- Configuring Regional Settings 26
- Verifying Prerequisites 28
 - Active Directory Prerequisites 28
 - Unified CCX Prerequisites 28
 - WFM Prerequisites 28

4 Installing and Configuring WFM 29

- Overview 29
- Upgrading WFM 30
- Installing WFM 31
- Configuring WFM 33
 - WFM Database Step 34
 - WFM Server Step 35
 - ACD Connection Step 36
 - QM Connection Step 38
 - Administrator Password Step 39
 - WFM Authentication Step 40
 - Configuring Active Directory Domains 40
 - Monitoring and Notification Step 42
 - To configure SNMP Notification 43

Contents

- Configuring Email Addresses for Notification 43
- Verifying the Database Connection to the Unified CCX Database 45

-
- 5 Capturing Historical Data 47**
 - Overview 47
 - Capturing Unified CCX Historical Data 47
 - Verifying Historical Data Capture 48

-
- 6 Removing WFM 49**
 - Overview 49
 - Removing a WFM Service Release 50
 - Removing WFM Services 51

Index 53

Contents

Overview

1

Introduction

The Workforce Management (WFM) InstallShield Wizard guides you through the WFM installation. The installation includes the components listed in [Table 1](#).

Table 1. Workforce Management Installation Components

Installation	Components
Capture Services	<ul style="list-style-type: none">• WFM Capture service
Compile Services	<ul style="list-style-type: none">• WFM Compile service
Process Services	<ul style="list-style-type: none">• WFM Request service• WFM Schedule service
Transaction Services	<ul style="list-style-type: none">• WFM Real Time (RT) service• WFM Real Time Engine (RTE) service• WFM Adherence Conformity Calculator (ACC) service• WFM Jetty service• WFM Mana service• WFM Product Adapter service• WFM Sync service• WFM Tomcat service• WFM web application• BIRT (Business Intelligence Reporting Tools)

These components are installed on a single server. See "[Server Configurations](#)" on [page 18](#) for more information.

After you have successfully installed WFM into a properly configured Workforce Management environment, the basic functionality of WFM is ready to be configured for your use. Users access WFM through a web browser.

For information about configuring WFM, see the *Workforce Management Administrator User Guide*.

What's New in This Version

WFM 8.5(2) includes the following new features.

- Agent access to WFM through the Workforce Management widgets available in Workforce Optimization
- New Monitoring and Notification service to send notification of system problems
- One-click redirection of agents to exceptions and projections that are hyperlinked
- Workforce Management widgets are supported in Mozilla Firefox 3.x
- Integration into WFM of real-time data via the Genesys Connector in systems using a Genesys Telephony Server (T-Server)
- Support for 32-bit Windows Server 2008 R1
- Support for 64-bit Windows Server 2008 R2
- Support for Microsoft SQL Server 2008
- Support for multiple Active Directory domains

WFM Documentation

The following documents contain additional information about WFM.

- *Workforce Management Administrator User Guide*
- *Workforce Management Agent Application User Guide*
- *Workforce Management Troubleshooting Guide*
- *Workforce Management Reports Reference*
- *Workforce Management Release Notes*

Workforce Management Services

Workforce Management ACC Service

The Workforce Management ACC (Adherence Conformity Calculator) service processes data from the daily schedule and agent status table and computes the adherence and conformity percentages used in historical productivity reports.

Workforce Management Capture Service

The Workforce Management Capture service manages the import of historical data.

- In a Cisco environment, the capture service imports data directly from the ACD database.

In all cases, when the Capture service detects new data, it sends a compilation request to the Compile service.

Workforce Management Compile Service

The Workforce Management Compile service listens for compilation requests from the Capture service. The 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 Jetty Service

The Jetty service is a webserver that works with the Mana service to display notification data.

Workforce Management Mana Service

Real-time monitoring of the WFM system is handled by the Mana service. When there are problems, the Mana service notifies the administrators through the Windows Event Viewer, Windows SNMP, or email.

Workforce Management Product Adapter Service

WFM uses the Product Adapter service to get configuration data. The service also handles product-specific authentication and requests.

Workforce Management Real Time Service

The Workforce Management Real Time service is not used at this time.

Workforce Management Real Time Engine Service

The Workforce Management Real Time Engine (RTE) service allows WFM to display agent state information in the Supervisor Adherence dashboard. To get real-time information on agent states, the RTE service uses the following component:

- Advanced Contact Management Interface (ACMI) protocol for Unified CCX

Workforce Management Request Service

The Workforce Management Request service generates distributions and forecasts.

Workforce Management Schedule Service

The Workforce Management Schedule service manages schedule requests.

Workforce Management Sync Service

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

Workforce Management Tomcat Service

The Workforce Management Tomcat service enables desktop clients to access WFM.

Environment and 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.

Table 2 lists the software running on each of these devices in a Unified CCX environment.

Table 2. Configuration in a Unified CCX environment

Server	Hosted Software
WFM servers	<ul style="list-style-type: none"> • WFM services • WFM web application • WFM instance of SQL Server • Apache Tomcat
Unified CCX server	<ul style="list-style-type: none"> • Unified CCX • Unified CCX instance of SQL Server • CTI server (part of the RmCm subsystem)
Cisco CTI server	<ul style="list-style-type: none"> • CTI service
Client PC	One of these web browsers: <ul style="list-style-type: none"> • Microsoft Internet Explorer 7 or 8 • Mozilla Firefox 3.6 or higher

Table 3 lists the TCP and UDP ports used by WFM and its components on the WFM server.

Table 3. 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 Jetty Service	TCP 59103 TCP 443 TCP 80	HTTPS HTTP
WFM RTE Service	TCP 30001 (configurable)	ACMI Service (GED-188)

Table 3. WFM Port Usage on WFM Server

Server application protocol	Destination port (listening)	Client application protocol
WFM Sync Service	TCP 59011	<i>unused</i>
WFM Tomcat	TCP 8087 TCP 8017 TCP 8007	HTTP AJP 1.3 Shutdown port

Table 4 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 4. WFM Port Usage on Remote Devices

Server application protocol	Destination port (listening)	Client application protocol
CTI server*	TCP 42027 Side A TCP 43027 Side B	ACMI Service
Unified CCX instance of SQL Server	TCP 1433 TCP 1434	WFM Sync Service
WFM RTE Service	TCP 42027 (configurable) NOTE: For Unified CCX 8.0 or newer, use TCP 12028.	Unified CCX instance of SQL Server

* 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 covers the following subjects:

- [System Requirements \(page 14\)](#)
- [Server Configurations \(page 18\)](#)
- [Configuration Data \(page 20\)](#)

System Requirements

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

Cisco Unified Workforce Optimization Environment

Cisco Workforce Management 8.5(2) is compatible with Cisco Quality Management 8.5(2).

System Environment

WFM has been verified in the following environment:

- Cisco Unified Contact Center Express 8.5(1) SU1 and later

Operating Environment

Server Operating Systems

The supported operating systems for WFM servers are the following.

- 32-bit Windows Server 2003
- 32-bit Windows Server 2008
- 64-bit Windows Server 2008

Hardware Requirements and Capacity

[Table 5](#) displays the minimum hardware requirements and capacity for WFM servers in the supported configurations.

NOTE: Running WFM on a platform other than a Cisco MCS or exact equivalent server is not supported.

NOTE: If you are using Unified CCX, WFM requires the Cisco Media Convergence Server (MCS) equivalent platform to be a dedicated standalone server. Running other applications on the WFM server can adversely affect performance.

The system capacity for the WFM server is determined by your hardware and software configuration, as well as by the number of users.

Users are defined as follows.

- Configured users—Any scheduled or recorded agent plus all other users with active login rights to Workforce Optimization (WFO) applications (for example, supervisors, managers, quality evaluators, and schedulers).
- Concurrent users—The users who are logged into WFM at any given time.

Table 5. WFM server minimum requirements and capacity*

	Configuration	
	7835	7845
Cisco MCS Equivalent	7835	7845
Processor	Intel 5140 2.33 GHz Dual Core	Intel 5140 2.33 GHz Dual Core
Memory (RAM)	2 GB DDR2/ DDR3	4 GB DDR2/ DDR3
HDD Storage	40 GB	40 GB
Max Number Configured Users	450	900
Max Number Concurrent Users	150	300

* Capacity numbers are estimates. Actual numbers might vary.

WFM in a Cisco Unified Computing System Environment

WFM 8.5(2) is certified to run on any Cisco UCS server with resources available to support the OVA/OVF template. The virtual server requirements for deployments on UCS servers are specified at the following URL:

http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization_Downloads_%28including_OVA/OVF_Templates%29#Cisco_Unified_Contact_Center_Express

WFM in a Virtual Server Environment

A virtual server environment requires hardware resources equivalent to those required for a physical server for a given number of users (see "[Hardware Requirements and Capacity](#)" on page 14).

NOTE: WFM systems hosted on a VMware ESX server have been tested for functionality only, not for scalability. Due to the many possible virtual server configurations, and the possible impact on WFM of additional hosted virtual servers, the actual server

performance in a VMware environment is the responsibility of the customer. Cisco support for performance and scalability issues is limited to server-based deployments. If a problem occurs in a VMware deployment, the customer might be required to shut down other sessions or reproduce the problem in a non-VMware configuration to assist in isolating the issue.

Desktop Requirements

WFM is operating system-independent. The only requirement is that the OS can run the supported web browsers (see ["Third Party Software"](#)).

Third Party Software

The following applications are required in order for WFM to function correctly.

Table 6. Required third party software

Application	Where Installed	Use
Microsoft SQL Server 2005 32-Bit Standard and Enterprise Edition, including the latest service pack or Microsoft SQL Server 2008 32-Bit and 64-Bit Standard and Enterprise Edition, including the latest service pack	WFM database server	Database
Adobe Acrobat Reader 6.0 or later	Client desktop	PDF-based reports and WFM user documentation
Microsoft Internet Explorer 7 Microsoft Internet Explorer 8 (32- or 64-bit) Mozilla Firefox 3.x	Agent client desktop	WFM desktop gadgets and HTML-based reports
Microsoft Internet Explorer 7 or 8	Supervisor, Scheduler, and Administrator client desktop	WFM administrative interface and HTML-based reports

Web Browser Considerations

While WFM fully supports multiple browsers and version levels, our product testing shows substantial performance improvements when loading a page using Microsoft Internet Explorer 8 over Internet Explorer 7. As a result, Cisco recommends using Internet Explorer 8. Furthermore, testing with Mozilla Firefox 3.x shows the highest performance, so should be considered in situations where page load speed is considered critical.

Server Configurations

Concurrent SQL Server Versions

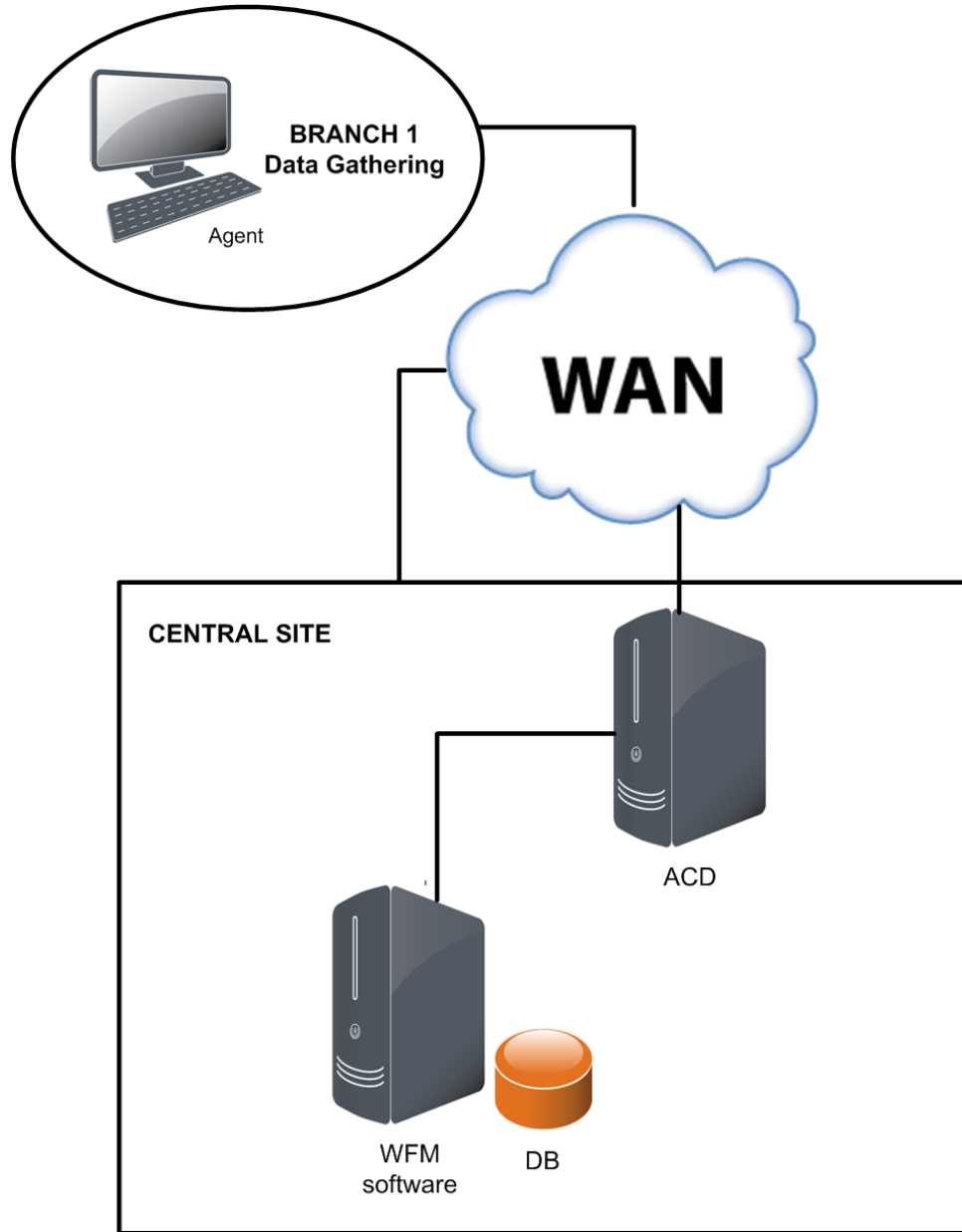
SQL Server 2005 and SQL Server 2008 can be used concurrently in your system. For example, you might use SQL Server 2008 for the ACD database and SQL Server 2005 for the WFM database.

Single Server Configuration

A single server configuration has one ACD cluster with all Workforce Management services located on a single server ([Figure 1 on page 19](#)). The single server configuration supports 150 concurrent users and 450 configured users (MCS 7835) or 300 concurrent users and 900 configured users (MCS 7845).

NOTE: Microsoft SQL Server must be installed on the single server before you install the components.

Figure 1. Single server configuration



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 Management Studio tools to manually back up and restore the CWFM 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 might 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 \(page 22\)](#)
- [Creating a SQL Server Login for WFM \(page 24\)](#)
- [Configuring Firewall Port Exceptions \(page 25\)](#)
- [Configuring Regional Settings \(page 26\)](#)
- [Verifying Prerequisites \(page 28\)](#)

Installing Microsoft SQL Server

You must install Microsoft SQL Server 2005 or 2008 on the WFM server.

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

Complete the Microsoft SQL Server Setup utility windows as shown in [Table 7](#).

Table 7. Microsoft SQL Server Setup utility entries

Window	Complete as follows:
Registration Information	Enter your name, company, and product key.
Components to Install	Select check boxes for: <ul style="list-style-type: none"> • SQL Server Database Services • Workstation Components • Any other desired components
Instance Name	Select one of the following options: <ul style="list-style-type: none"> • Default Instance. If you are upgrading from WFM 8.0, you must select the Default instance. WFM 8.0 required a default instance, and you cannot upgrade from WFM 8.0 to a SQL environment using a named instance. • Named Instance. If you select this option, specify the named instance.
Service Account	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.
Authentication Mode	Select Mixed Mode. Enter a password for the SQL Server System Administrator (sa) logon.

Table 7. Microsoft SQL Server Setup utility entries (cont'd)

Window	Complete as follows:
Collation Settings	<p data-bbox="704 371 1377 436">Under Collation Designator and Sort Order, select Latin1_General from the drop-down list.</p> <p data-bbox="704 457 1377 522">Select the Accent-sensitive check box. Do not select any of the other check boxes.</p> <p data-bbox="704 543 1377 699">NOTE: The SQL collation name is SQL_Latin1_General_CP1_CI_AS. See http://msdn2.microsoft.com/en-us/library/ms180175.aspx for more information about SQL Server collation settings.</p>

Creating a SQL Server Login for WFM

NOTE: If you are using a historical database (HDS) and an administrative workstation (AW) database instead of a single database, make sure the SQL Server login has access to both databases.

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 and log in.
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 WFM services to use to connect to SQL Server. Select SQL Server Authentication, enter a password, and clear the Enforce password policy check box so that the WFM user account does not expire.
6. On the Server Roles page, select dbcreator and sysadmin from the list of server roles.

NOTE: The WFM SQL Server login must be able to create databases and run the WFM administrative scripts.

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

IMPORTANT: If this database user is modified (for example, name or password are changed) after WFM is installed and configured to use it, WFM must be reinstalled.

Configuring Firewall Port Exceptions

If Microsoft Windows Firewall is enabled when WFM is installed, the installation process opens the firewall ports listed in [Table 8](#).

If another firewall is used, or if you turn on the Windows Firewall after WFM is installed, these ports must be opened manually. See your firewall documentation for instructions.

Table 8. Microsoft Windows Firewall port exceptions

Server Application Protocol	Listening Port	Client Application Protocol
WFM RTE Service *	TCP 30001 (configurable)	ACMI Service (GED-188)
	TCP 42027 (configurable)	Unified CCX instance of SQL Server
WFM Tomcat	TCP 8087 TCP 8017 TCP 8007	HTTP{ AJP 1.3 Shutdown port
WFM Jetty	TCP 59103 TCP 80 TCP 443	

* Open the ports listed here on the server where the WFM RTE service is installed.

NOTE: For a complete list of ports used in a WFM environment, see [Environment and Port Usage \(page 11\)](#).

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

1. On the WFM server where the applicable WFM service is installed, choose Start > Settings > Control Panel > Windows Firewall.
2. On the Exceptions tab, click Add Port. The Add a Port window appears.
3. Enter a name that describes the port, and then enter the port number. Select the appropriate connection type (TCP or UDP), and then click OK.
4. Repeat steps 2 and 3 to add another port to the exceptions list.
5. When you are finished adding ports, click OK to close Microsoft Windows Firewall.

Configuring Regional Settings

If you are installing the Capture services on a server running a non-US English Windows operating system, you must change the default regional settings to US English in the Windows registry.

To change the regional settings in the Windows registry:

1. Open the Windows registry on the Capture services server.
2. Navigate to the following registry key:
HKEY_USERS\DEFAULT\Control Panel\International\
3. Ensure that the registry settings under the International key are as listed in [Table 9](#).

Table 9. Regional settings

Value	Type	Data
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

Table 9. Regional settings (cont'd)

Value	Type	Data
s2359	string	PM
sCountry	string	United States
sCurrency	string	\$
sDate	string	/
sDecimal	string	.
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

Verifying Prerequisites

Active Directory Prerequisites

If you are using Active Directory, the WFM server must be part of the Active Directory domain.

You also need the following information:

- 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

Unified CCX Prerequisites

If you plan to use Unified CCX, you must install and configure the following systems before you install WFM.

- Cisco Unified Contact Center Express (Unified CCX)
- Cisco Unified Communications Manager (Unified CM) or Unified Communications Manager Express (Unified CME)
- Cisco Unity server (if you use Cisco Unity)
- Unified CM IP address and port number
- IP address and port number of the server that hosts the CTI service (see ["Environment and Port Usage" on page 11](#))
- Cisco Quality Management server IP address (if you use Quality Management)
- Unified CCX server IP address:
 - Single node environment: use the primary server IP address
 - High Availability (two node) environment: use the secondary server IP address

WFM Prerequisites

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 24](#)
- SQL Server instance name you used in ["Installing Microsoft SQL Server" on page 22](#) (if you did not use the default instance)

Installing and Configuring WFM

4

Overview

This chapter describes how to install and configure WFM. It covers the following topics:

- [Upgrading WFM \(page 30\)](#)
- [Installing WFM \(page 31\)](#)
- [Configuring WFM \(page 33\)](#)
- [Verifying the Database Connection to the Unified CCX Database \(page 45\)](#)

Upgrading WFM

WFM 8.5(2) supports upgrades from the following versions:

- WFM 8.3(3)
- WFM 8.3(4)
- WFM 8.5(1)

No other upgrade scenarios are supported.

Over the top upgrades are not supported; all upgrades must be manual. In a manual upgrade, you must do the following:

1. Back up the current SQL Server WFM database (CWFM) using SQL Management Studio backup tools
2. Uninstall the current WFM version
3. Install WFM 8.5(2) (see ["Installing WFM" on page 31](#))
4. Restore the SQL Server WFM database

NOTE: After you upgrade WFM, do not reboot the server if prompted to until WFM Configuration Setup has run completely.

Installing WFM

Install the WFM services according to the supported system configuration as described in "[Server Configurations](#)" on page 18.

IMPORTANT: WFM Configuration Setup runs automatically after you install WFM. It must always be run to completion in order for the system to function.

NOTE: After you install WFM, do not reboot the server if prompted to until WFM Configuration Setup has run completely.

NOTE: You can log into WFM servers remotely using Virtual Network Computing (VNC) software. See your VNC documentation for instructions on establishing a remote connection to another machine.

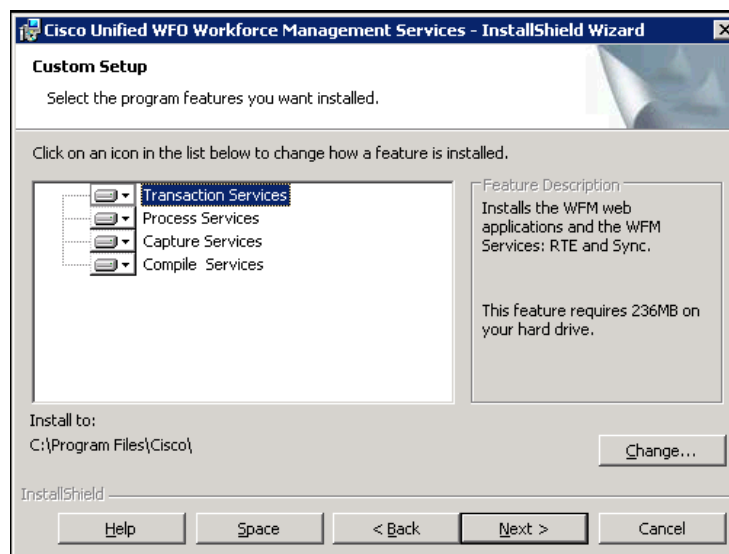
NOTE: If Cisco Security Agent (CSA) is running on a WFM server, shut it down before you begin the installation process. If you do not, the installation might fail.

To install WFM:

1. On the WFM server, log in as a local machine administrator.
2. On the installation CD, double-click setup_WFM_852.exe to start the InstallShield Wizard.

3. Click Next to display the Custom Setup window (Figure 2).

Figure 2. Custom Setup window



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

NOTE: If you choose to change the installation location, do not choose a root level (for example, C:\ or D:\). At least one folder level must be defined (for example, C:\WFM\).

5. Click Next to continue. Follow the InstallShield Wizard prompts until the installation is finished.
6. After the installation is complete and the InstallShield Wizard closes, WFM Configuration Setup starts. See "[Configuring WFM](#)" on page 33 for instructions on how to configure the services you just installed.
7. After you have completed WFM Configuration Setup, restart Cisco Security Agent (if present on the server).

Configuring WFM

After you have installed the WFM server, WFM Configuration Setup is used to configure the WFM environment. WFM Configuration Setup has two modes, Initial Mode and Update Mode.

- **Initial Mode.** WFM Configuration Setup is launched automatically in initial mode after the WFM installation finishes. After you configure all of the required parameters, the WFM services are started automatically and the system is ready for use.
- **Update Mode.** WFM Configuration Setup can be launched manually when you want to change configuration settings in an existing system.

To launch WFM Configuration Setup manually, double-click `postinstall.exe` located in `<install folder>\WFO_WFM\bin` on any WFM server.

NOTE: In a multiple server configuration, launch WFM Configuration Setup on the server that hosts the transaction services.

NOTE: In update mode, you cannot modify the WFM database hostname/IP address or instance name or enable/disable Active Directory. To change those settings, you must reinstall WFM.

The following is a list of all possible steps that can appear when you run WFM Configuration Setup in either initial or update mode. See the section for each step for instructions on completing the fields in the step window.

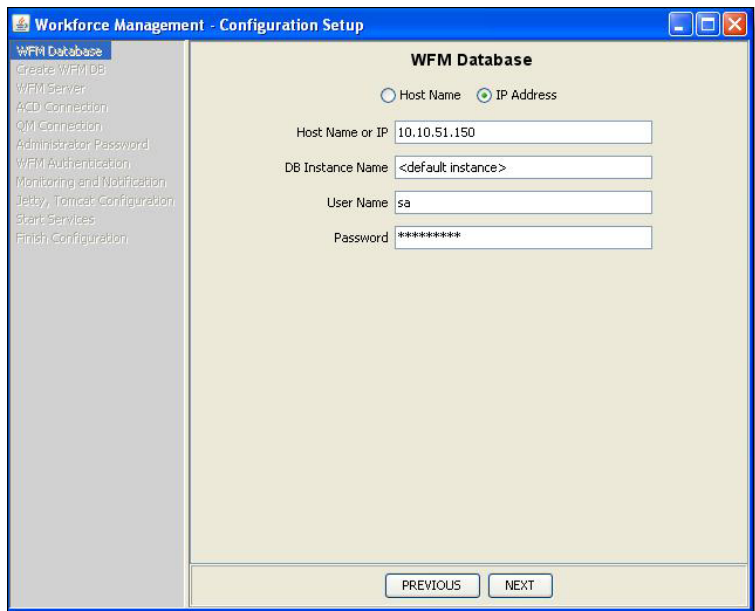
NOTE: Some steps trigger actions and do not display windows that contain fields to be completed.

- [WFM Database Step \(page 34\)](#)
- Create WFM DB—action only. This step creates the WFM database.
- [WFM Server Step \(page 35\)](#)
- [ACD Connection Step \(page 36\)](#)
- [QM Connection Step \(page 38\)](#)
- [Administrator Password Step \(page 39\)](#)
- [WFM Authentication Step \(page 40\)](#)
- [Monitoring and Notification Step \(page 42\)](#)
- Start Services—action only. This step starts all the WFM service.
- Finish Configuration—action only. This step configures the WFM Windows registry settings

WFM Database Step

The WFM Database step (Figure 3) configures access to the WFM database.

Figure 3. WFM Database step



Complete the fields listed in Table 10.

Table 10. WFM Database step fields

Field	Description
Host Name or IP Address	Indicate which format is used for the WFM server name in the Host Name or IP field.
Host Name or IP	The host name or IP address of the WFM server that hosts the WFM database.
DB Instance Name	<p>The WFM database instance name.</p> <p>If this is a new installation of WFM, this field is prepopulated with <default instance>. Use the default value, the named instance, or leave the field blank. Leaving the field blank is the same as using the default instance.</p> <p>NOTE: If you are upgrading from a previous version of WFM, do not enter a named instance in this field. Use the prepopulated <default instance>.</p>

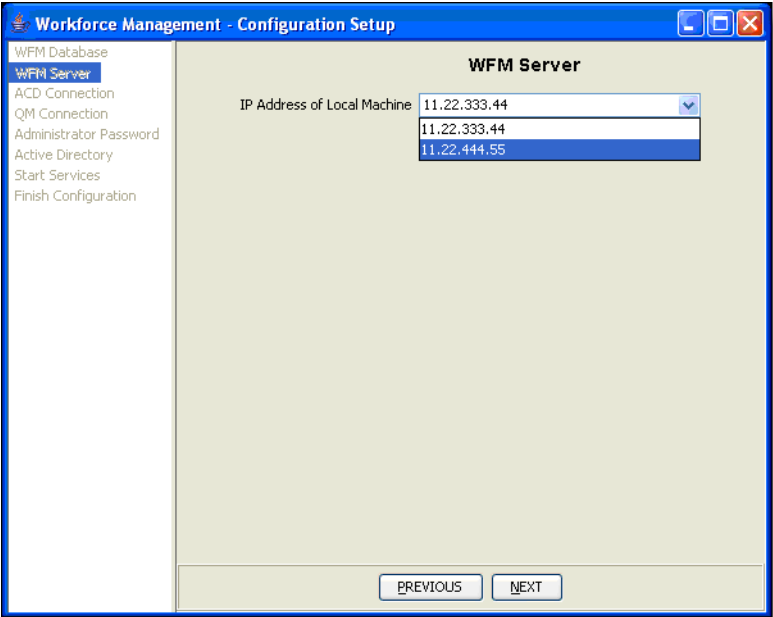
Table 10. WFM Database step fields (cont'd)

Field	Description
User Name	User name with access to the SQL Server CWFM database. The user is the one created when installing Microsoft SQL Server 2005. See "Creating a SQL Server Login for WFM" on page 24.
Password	User's password.

WFM Server Step

The WFM Server step (Figure 4) configures the IP address of the server where WFM is installed. It appears only if Configuration Setup detects that there is more than one network interface card (NIC) on the server. Select the appropriate IP address from the drop-down list.

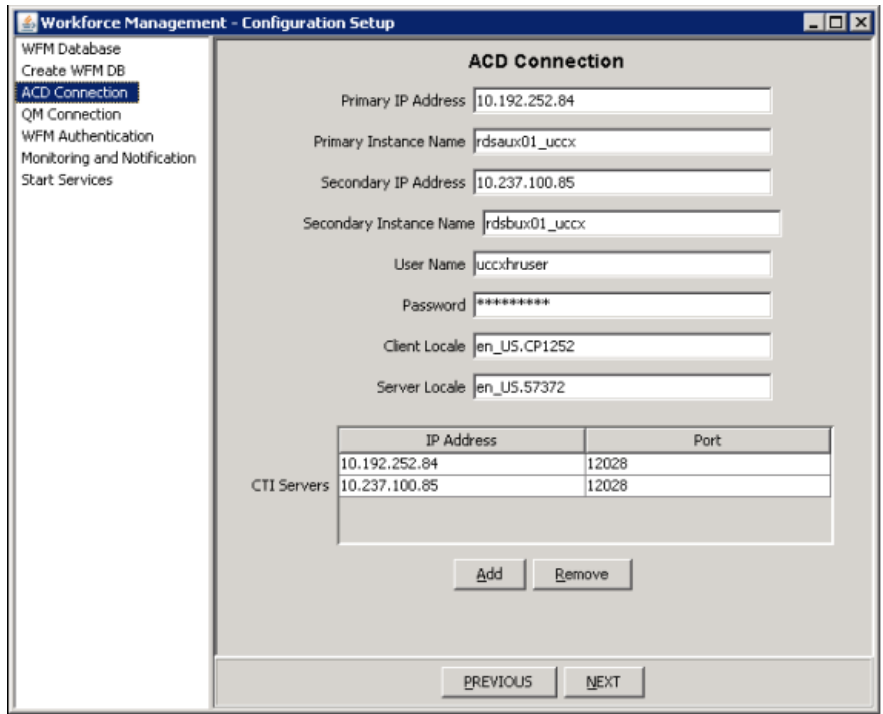
Figure 4. WFM Server step



ACD Connection Step

The ACD Connection step (Figure 5) configures which ACD is used with your WFM system.

Figure 5. ACD Connection step



Complete the following fields listed in Table 11.

Table 11. ACD Connection step fields

Field	Description
Primary IP Address	Enter the IP address of the primary ACD.

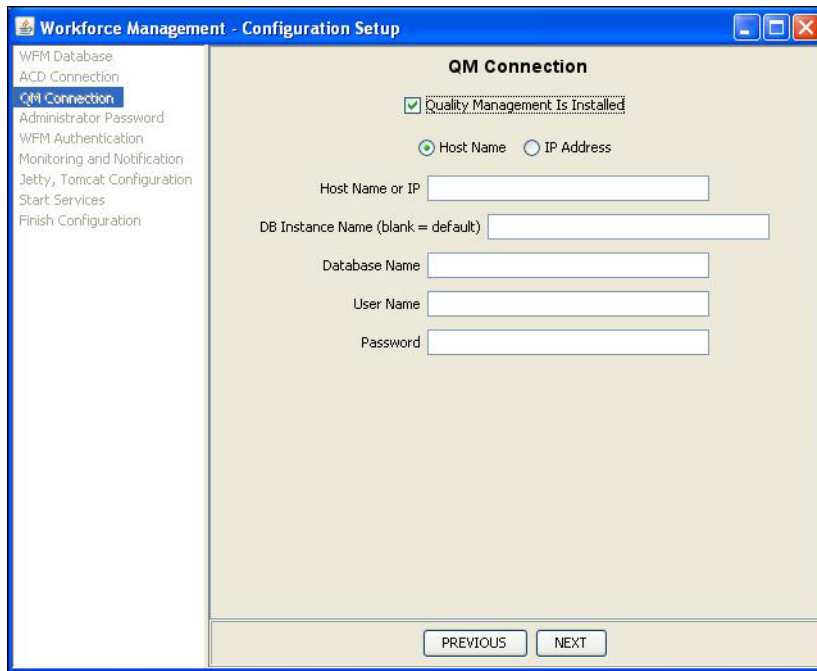
Table 11. ACD Connection step fields (cont'd)

Field	Description
Primary Instance Name	<p>Enter the instance name of the primary Unified CCX database. When typing the database instance name, use the following guidelines:</p> <ul style="list-style-type: none"> ■ Convert all uppercase characters to lowercase characters ■ Replace all hyphens with underscores ■ If the host name starts with a number, add the prefix i ■ Append _uccx to complete the instance name <p>For example, if your host name is 80-ABC, your instance name will be i80_abc_uccx.</p>
Secondary Instance Name	<p>Enter the instance name of the secondary Unified CCX database</p> <p>NOTE: Follow the guidelines for Primary Instance Name when entering the instance name of the secondary Unified CCX database.</p>
Secondary IP Address	Enter the IP address of the secondary ACD, if this is a redundant system.
User Name	The database authorized user name. Type uccxhruser in this field.
Password	The password for the authorized database user.
Client Locale	The client locale that is configured in Unified CCX. The locale for US English appears by default in this field. If the client locale is changed in Unified CCX, then it must also be manually changed in Configuration Setup.
Server Locale	The server locale that is configured in Unified CCX. The locale for US English appears by default in this field. If the server locale is changed in Unified CCX, then it must also be manually changed in Configuration Setup.
CTI Servers	The CTI server(s) and port(s) associated with your system. to add a CTI server to the list, click Add and enter the CTI server IP address and port, then click OK.

QM Connection Step

NOTE: The QM Connection step (Figure 6) is used if you are using the Quality Management part of the Workforce Optimization suite..

Figure 6. QM Connection step



Complete the fields listed in Table 10.

Table 12. QM Connection step fields

Field	Description
Quality Management is Installed	Select the check box if you are using QM.
Host Name or IP Address	Indicate which format is used for the server name in the Host Name or IP field.
Host Name or IP	The host name or IP address of the QM base services server.
DB Instance Name	The QM database instance name. Leave this field blank if using the default instance name.
Database Name	The name of the QM database.

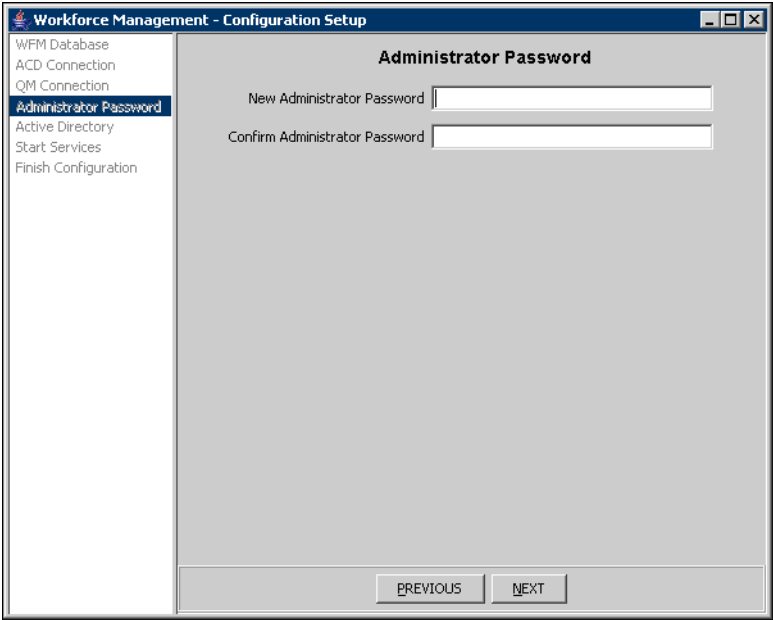
Table 12. QM Connection step fields (cont'd)

Field	Description
User Name	User name with access to the QM database.
Password	User's password.

Administrator Password Step

The Administrator Password step (Figure 7) creates the password used by the WFM administrator to access the application. This step appears only in Initial Mode.

Figure 7. Administrator Password step



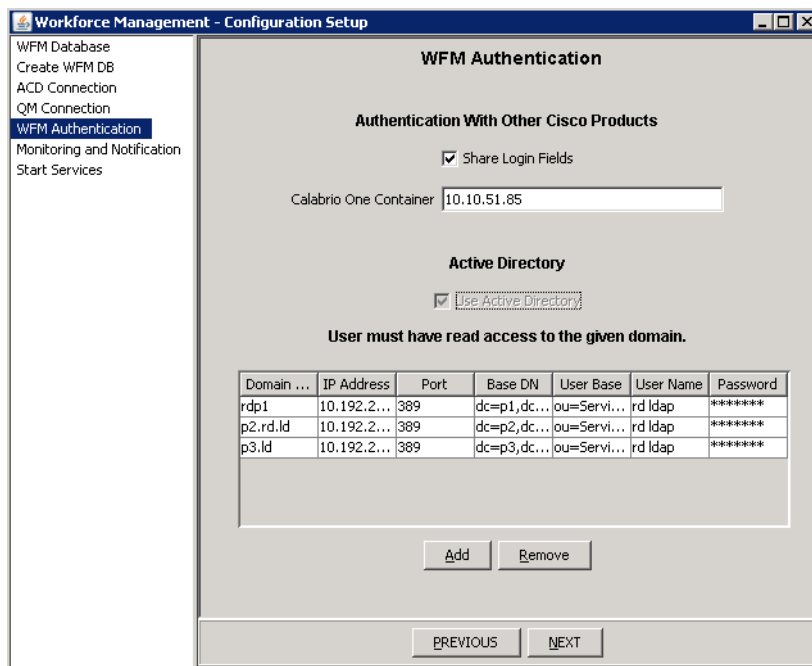
Enter the WFM administrator password in the New Administrator Password and Confirm New Administrator Password fields.

NOTE: Store this password in a safe place. You will need it to log into WFM as an administrator. The password can be changed using WFM Administrator.

WFM Authentication Step

The WFM Authentication step (Figure 8) configures shared login with other Cisco products, the IP address of the Workforce Optimization container, and Active Directory domains, if used in your system.

Figure 8. WFM Authentication step



Complete the fields listed in Table 13.

Table 13. WFM Authentication step fields

Field	Description
Share Login Fields	Select this check box is you want to share login fields in the Workforce Optimization container with other Cisco products.
Calabrio One Container	The IP address of the Workforce Optimization container. If you are sharing login fields with Quality Management, this must be the Quality Management IP address.
Use Active Directory	Select this check box if you will be using Active Directory.

Configuring Active Directory Domains

If you are using Active Directory, you must add the connection data for each Active Directory domain.

To add a domain, click Add to display the Enter Data window.

Figure 9. Enter Domain window

Complete the fields listed in [Table 14](#).

Table 14. Active Directory domain Enter Data window fields

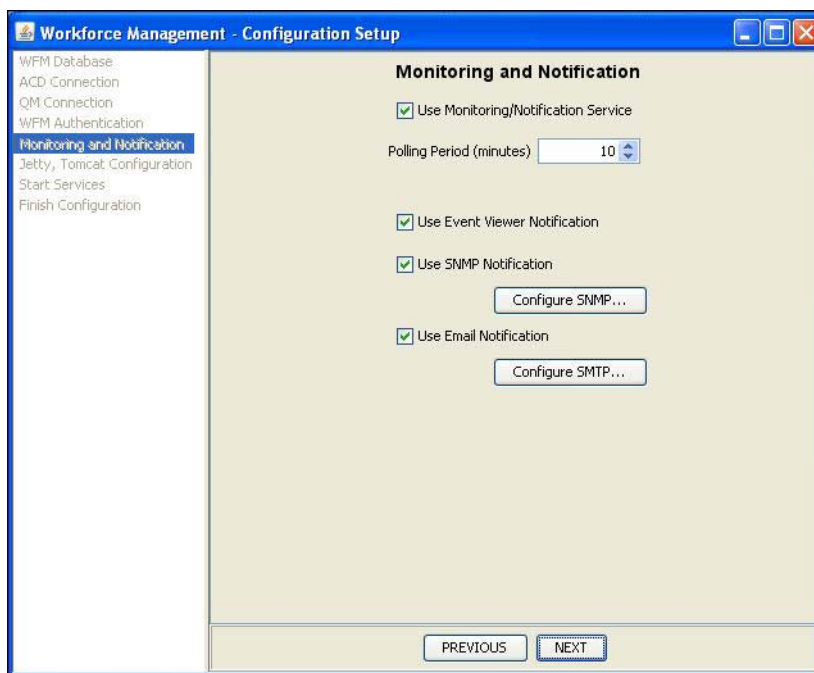
Field	Description
Domain Name	The name of the Active Directory domain. This is usually the first part of the Base DN.
IP Address	The IP address of the Active Directory server.
Port	The port used to access the Active Directory server. The default value is 389.
Base DN	The location in the directory server tree under which all Active Directory users are located.
User Base	The path to organizational units (OU) for user records. The path must be specified from the most specific to the least specific (from left to right in the path statement). For example: ou=Users,ou=Minneapolis,ou=Minnesota,ou=US
User Name	The display name as configured in Active Directory of a user with read access to the Active Directory database.
Password	The user's password.

Monitoring and Notification Step

The Monitoring and Notification step (Figure 10) is used to enable the monitoring and notification feature, and to configure the following:

- Enable or disable the use of monitoring and notification of system problems.
- Set the interval at which the Mana service checks for notification triggers.
- Configure any or all of three means of notification: the Event Viewer, SNMP, and email notification.

Figure 10. Monitoring and Notification step



Complete the fields listed in Table 15.

Table 15. Monitoring and Notification step fields

Field	Description
Use Monitoring/Notification Service	Enable this check box to use the Mana service. If enabled, at least one notification method (event viewer, SNMP, or email) must be enabled as well.
Polling Period (minutes)	Sets the interval at which the Mana service checks for notification triggers. The default period is 10 minutes.

Table 15. Monitoring and Notification step fields (cont'd)

Field	Description
Use Event Viewer Notification	Enable this check box to use the Microsoft Event Viewer utility (Control Panel > Administrative Tools > Event Viewer) to display notification messages.
Use SNMP Notification	Enable this check box to use SNMP for sending notification messages. The Windows SNMP Service must be installed in order to be able to use SNMP notification.
Use Email Notification	Enable this check box to use email for sending out notification messages.

To configure SNMP Notification

You can use SNMP notification if the Microsoft Simple Network Management Protocol (SNMP) service is installed on the WFM base services server.

In SNMP notification, Mana notification messages are sent from the WFM services server to specified trap destination IP addresses. Use the Configure SNMP button to manage the list of trap destinations.

The SNMP service can be installed using the Add/Remove Windows Components button in the Add or Remove Programs utility in Control Panel. Select Management and Monitoring Tools from the list of available components, and then choose Simple Network Management Protocol.

To add a trap destination for SNMP notification:

1. Click Configure SNMP.
2. In the Configure SNMP dialog box, click Add and enter the IP address of the trap destination, and then click OK.
3. Restart the Windows SNMP service to enable the trap destination.

NOTE: You must restart the SNMP service any time you make a change in trap destination, including on the initial setup.

Configuring Email Addresses for Notification

Notification emails will be sent from the sender email and the recipient email addresses configured in the Configure SMTP dialog box.

To configure the SMTP settings for email notification:

1. Click SMTP Configuration. The SMTP dialog box appears.

2. Complete the fields as listed in [Table 16](#) and then click OK.

Table 16. SMTP Configuration dialog box fields

Field	Description
From Address	The email address from which all notification emails are sent.
To Addresses	The email addresses to which notifications are sent.
Host Name/IP Address	Choose the format of the SMTP host address.
SMTP Host	The host name or IP address of the SMTP server.
SMTP Port	The port used by the Mana service to communicate with the SMTP server.
Use Authorization	Enable this check box if authentication is needed to access the SMTP server.
SMTP User	The user name needed to access the SMTP server.
SMTP Password	The user's password.

Verifying the Database Connection to the Unified CCX Database

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 where WFM is installed.

`http://<wfm>:8087/c3/`

NOTE: The website address is case sensitive.

The Workforce Management login window appears.

2. Enter administrator in the username field and the password that you specified in WFM Configuration Setup (see "[Administrator Password Step](#)" on [page 39](#)), then click GO or press the Enter key. The Workforce Management window appears.
3. Choose Agents > Agents. If the right pane displays a list of agents, the synchronization was successful.
4. Navigate to C:\Program Files\Cisco\WFO_WFM\log. Open the Capture Service log file. Verify that the log file does not contain any error messages. If there are error messages, correct the errors before proceeding.

Capturing Historical Data

5

Overview

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

If you want to use historical data from the time before you installed WFM, you must capture the data manually.

Capturing Unified CCX Historical Data

If you use Unified CCX, import historical data with the WFM Administrator's Request ACD Data feature (Special Functions > Request ACD Data). See the *Workforce Management Administrator User Guide* for information on using this feature.

Verifying Historical Data Capture

When you finish capturing the historical call data for Unified CCX, 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 contact data capture is complete when there are no more reports in the folder C:\Program Files\Cisco\WFO_WFM\reports.

Removing WFM

6

Overview

To remove WFM, you must proceed in the following order:

1. Remove all service releases (see ["Removing a WFM Service Release" on page 50](#)).
2. Remove WFM (see ["Removing WFM Services" on page 51](#)).

Removing a WFM Service Release

Follow these steps to remove a Workforce Management service release from a WFM server. When the service release is removed, your WFM deployment will be reverted to the base release.

NOTE: If you cancel the removal process while it is running, the service release might continue to be listed in the Add or Remove Programs window, and you will not be able to remove or repair the service release, or reinstall it. Contact Cisco TAC for assistance.

To remove a Workforce Management service release:

1. Log into the WFM server as the local machine administrator.
2. Choose Start > Settings > Control Panel > Add or Remove Programs.
3. Select Cisco Unified WFO Workforce Management Service Release, click Remove, and follow the prompts.

During the removal process, a DOS window named srRollbackRepair.exe appears. Do not close this window. The srRollbackRepair.exe DOS window closes automatically.

4. Your computer automatically reboots. After the computer restarts, the system will be back to its base level software state.

Removing WFM Services

When you remove WFO Workforce Management Services, JRE and Tomcat are automatically removed, but the WFM database is not removed.

NOTE: If there is a service release installed on the Workforce Management server and you want to remove WFM, you must remove the service release before you can remove WFM. See ["Removing a WFM Service Release" on page 50](#) for more information.

To remove Workforce Management services:

1. Log into the WFM server as the local machine administrator.
2. From the Start menu, choose Settings > Control Panel.
3. Double-click Add or Remove Programs.
4. Select Cisco Unified WFO Workforce Management Services, click Remove, and follow the prompts.

Index

	A	Active Directory 28 verifying 28 WFM 28 prerequisites Unified CCX 28 Product Adapter Service described 9
ACC Service described 9 Active Directory prerequisites 28		
	C	
Capture Service described 9 Compile Service described 9 Configuring WFM 33		
	I	
Installing WFM 31		
	J	
Jetty Service described 9		
	M	
Mana Service described 9		
	P	
Password Active Directory 28 SQL Server Login for WFM 24 SQL Server System Administrator logon 22 WFM SQL Server database username 28 Prerequisites		
		R
		Removing WFM application 49 Request Service described 10 Requirements system 14 RTE Service described 10
		S
		Schedule Service described 10 Sync Service described 10 System environment 14 requirements 14
		T
		Tomcat Service described 10
		U
		Unified CCX prerequisites 28

- verifying historical call data 48
- Uninstalling
 - WFM 51

W

- WFM
 - installing 31
 - prerequisites 28
 - uninstalling 51
- WFM Configuration Setup tool 33