



Cisco Unified Workforce Optimization

Workforce Management Installation Guide Release 10.5

First Published: June 18, 2014

Last Updated: June 23, 2015

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 or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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. (1110R)

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

Workforce Management Installation Guide

© 2014, 2015 Cisco Systems, Inc. All rights reserved.

Contents

Overview	6
What's New in This Version	7
WFM Documentation	8
Workforce Management Services	9
Workforce Management ACC Service	9
Workforce Management Capture Service	9
Workforce Management Compile Service	9
Workforce Management Forecast Service	9
Workforce Management Jetty Service	10
Workforce Management MANA Service	10
Workforce Management Product Adapter Service	10
Workforce Management RTE Service	10
Workforce Management Request Service	10
Workforce Management Schedule Service	10
Workforce Management Sync Service	10
Port Usage	11
System Requirements	12
Workforce Management Environment	12
System Environment	12
WFM Server Hardware Requirements	12
Capacity and Sizing	13
WFM in a Cisco UCS Environment	15
Virtual Server Environment	16
Server Operating Systems	16
Desktop Requirements	17

Third Party Software Requirements	17
Microsoft Internet Explorer Requirements	17
Configuration Data Requirements	17
Server Configurations	20
SQL Server Clustering	20
Concurrent SQL Server Versions	20
Single Server/Onboard SQL Server Deployment	20
Single Server/Offboard SQL Server Deployment	22
Web Server Redundancy	23
Before You Install WFM	26
Prerequisites	26
Active Directory	26
Cisco Unified Contact Center Express	26
GIS API	27
SMTP	27
SNMP	27
WFM	27
Installing Microsoft SQL Server	28
Creating a SQL Server Login for WFM	29
Installing SQL Server Native Client	30
Configuring Regional Settings	30
Configuring Firewall Port Exceptions	32
Disabling Internet Information Services for Windows Server	33
Installing WFM	34
Preinstallation Considerations	34
For All Types of Installs	34
For Upgrades	34
Upgrading Systems with Pending Capture Requests	35

For Patches	35
Installing a Base Release	36
Installing an Upgrade	37
Installing a Patch	38
Configuring WFM	42
WFM Database Step	43
WFM Server Step	44
Data Retention Periods Step	45
ACD Connection Step	48
Cisco Unified CCX ACD	49
Capture Settings	51
QM Connection Step	51
WFM Authentication Step	52
Configuring Active Directory Domains	54
Managing Active Directory Domains	56
Email Distribution Step	56
Monitoring and Notification Step	58
Configuring SNMP Notification	60
Enterprise Settings Step	61
Configuring the Report Logo	61
Verifying the Connection to the Unified CCX Database	63
Configuring the iCalendar Service	63
Capturing Historical Data	66
Capturing Cisco Unified CCX Historical Data	66
Removing WFM	68
Removing Patches	68
Removing WFM Services	69

Overview

The Workforce Management (WFM) InstallShield Wizard guides you through installing WFM. The installation includes these components:

Installation Category	Components
Capture Services	WFM Capture service
Compile Services	WFM Compile service
iCalendar Service	WFM iCalendar service
Process Services	WFM Forecast service WFM Request service WFM Schedule service
Transaction Services	WFM RTE service WFM Adherence Conformance Calculator (ACC) service WFM Jetty service WFM Monitoring and Notification (MANA) service WFM Product Adapter service WFM Sync service

These components are installed on a single server. See [Server Configurations](#) 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 Application User Guide*.

What's New in This Version

WFM 10.5 includes the following new features:

WFM 10.5(1)

- Support for Cisco Unified Contact Center Express 10.5
- Support for Microsoft Internet Explorer 10 and 11
- Support for Google Chrome 34
- Application Management and Scheduling moved from the legacy application to Workforce Optimization
- Multi-channel forecasting with enhanced contact server integration capabilities
- Agent schedules viewable on mobile devices and personal computers via an iCalendar feed
- Shrinkage, Adherence State Mapping, and Service Queue Group pages converted from original Unified Workforce Optimization format to new Unified Workforce Optimization format
- Addition of the Copy Schedule Activities feature
- Report metrics calculation improvements
- Unified Workforce Optimization interface localized in Danish, Dutch, German, French, Italian, Brazilian Portuguese, Spanish, and Swedish
- Contents of the *WFM Reports Reference Guide* moved to the *WFM Application User Guide* and online Help
- Changes in the WFM Configuration Setup utility:
 - Data retention cleanup time is configurable on the Data Retention Periods step
 - Support for multiple Active Directory certificates on the WFM Authentication step
 - Addition of the new Enterprise Settings step, which includes options for customizing report logos on reports output in HTML, PDF, and XLS format, and requiring a secure connection to access WFM
 - Email authentication method can now be specified on the Email Distribution step
 - Entry validation on the ACD Connection and WFM Authentication steps

- Addition of the option to capture data manually through GIS instead of automatically is now configurable on the ACD Connection step
- Improvements on the Agent Schedules page:
 - Addition of the Abandoned Calls metric on the coverage drawer
 - Addition of date and month drop-down fields to provide quick date navigation
 - Support for viewing real time adherence for non-interactive service queues on the adherence drawer
- Support for copying and pasting data when editing forecasts and distributions
- User page now enables administrators to manage multiple users at one time: assign roles, change activation status, and delete users
- Views page now enables administrators to assign a view as a Main View to multiple users
- Navigation links in the long view pane now turn orange when selected and when that page section is being viewed
- Bug fixes

WFM 10.5(1) SR4

- Bug fixes

WFM 10.5(1) SR5

- Support for Cisco Unified Contact Center Express 10.6
- WFM Help localized in Danish, Dutch, French, German, Brazilian Portuguese, and Spanish
- Bug fixes

WFM Documentation

The following documents contain additional information about WFM They are available on the Cisco website (www.cisco.com).

- *Workforce Management Application User Guide*
- *Workforce Management Troubleshooting Guide*

- *Workforce Management GIS API Reference Guide*
- *Workforce Optimization Suite Getting Started Guide*
- *Workforce Optimization Suite Desktop Requirements Guide*
- *Workforce Optimization Suite Firewall Configuration Guide*
- *Workforce Optimization Suite Error Code Dictionary*
- *Workforce Management Release Notes*

Workforce Management Services

Following are short descriptions of the WFM services.

Workforce Management ACC Service

The WFM ACC (Adherence Conformance Calculator) service processes data from the daily schedule and agent status table and computes the adherence and conformance percentages used in historical productivity reports.

Workforce Management Capture Service

The WFM Capture service manages the import of historical data from the ACD database. When the Capture service detects new data, it sends a compilation request to the Compile service.

Workforce Management Compile Service

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

Workforce Management Forecast Service

The WFM Forecast service generates distributions, forecasts, and strategic forecasts.

Workforce Management Jetty Service

The Jetty service is a web server that supports the Unified Workforce Optimization user interface.

Workforce Management MANA Service

The WFM MANA (Monitoring and Notification) service handles real-time monitoring of the WFM system. When there are problems, the MANA service notifies the administrators through the Windows Event Viewer, Windows SNMP (Simple Network Management Protocol), or email.

Workforce Management Product Adapter Service

The WFM Product Adapter service is the conduit through which application data is read from and written to the WFM database.

Workforce Management RTE Service

The WFM RTE (Real Time Engine) service enables WFM to display agent state information. To get real-time information on agent states, the RTE service uses the Advanced Contact Management Interface (ACMI).

Workforce Management Request Service

The WFM Request service processes shift budget analysis requests.

Workforce Management Schedule Service

The WFM Schedule service manages schedule requests.

Workforce Management Sync Service

The WFM Sync service connects to a Unified CCX database using the SQL connection. The Sync service retrieves and processes configuration data such as skill group and precision queue configurations, team configurations, and agent configurations.

Port Usage

Refer to the *Workforce Optimization Suite Firewall Configuration Guide* for a list of all ports used by WFM.

System Requirements

The following topics list the minimum system requirements for WFM servers and clients.

Workforce Management Environment

WFM 10.5 is compatible with Cisco Quality Management 10.5.

System Environment

WFM 10.5 has been verified in the following environments:

- Cisco Unified Contact Center Express Release 9.0
- Cisco Unified Contact Center Express Release 10.0
- Cisco Unified Contact Center Express Release 10.5
- WFM 10.5(1) SR5 and above: Cisco Unified Contact Center Express Release 10.6

WFM Server Hardware Requirements

The following table displays the minimum hardware requirements for a WFM server.

Note: WFM requires the server platform to be a dedicated standalone server. Running other applications on the WFM server can adversely affect performance.

Note: The number of processor cores in your system can be determined by viewing the Performance tab in Windows Task Manager—there is one CPU History Usage graph for every processor core. Note that some types of processors are hyperthreaded, meaning that each physical core is presented as two processor cores. This results in twice the number of processor cores displayed in Windows Task Manager.

WFM server minimum hardware requirements

Processor	Intel: Xeon processor E3 family or higher, running above 2 GHz with hyperthreading enabled (required) AMD: Opteron processor 3000 or higher
Processor cores	2 (small server) 4 (medium server) 8 (large server)
VMWare processor cores	2 (small server) 4 (medium server) 8 (large server)
Minimum processor speed	2 GHz
Memory	4 GB (small server) 4 GB (medium server) 8 GB (large server)
System storage	60 GB (This is for the operating system, the WFM applications, and the SQL Server application. It does not include the SQL Server database.)

Capacity and Sizing

Use the figures in the following tables to determine how to size your WFM deployment.

Note: If you intend to use iCalendar so that agents can access their work calendars from outside the workplace via the internet, then it is strongly recommended that you deploy the iCalendar service on a dedicated server in your DMZ. Otherwise, the iCalendar service can be installed on any WFM application server.

Note: *Configured users* are scheduled agents plus all other users (supervisors, schedulers, and administrators). *Concurrent users* are the users who are logged in to WFM at any given time.

100 max concurrent users | 300 max configured users

Server configuration	Single server
WFM application and database server	Small
Offboard iCalendar Server (optional)	Small
Dedicated SQL Server memory	2 GB
Minimum SQL Server database storage	50 GB
Total storage	WFM server: 110 GB iCalendar server: 60 GB

200 max concurrent users | 600 max configured users

Server configuration	Single server
WFM application and database server	Medium
Offboard iCalendar server (optional)	Small
Dedicated SQL Server memory	2 GB
Minimum SQL Server database storage	100 GB
Total storage	WFM server: 160 GB iCalendar server: 60 GB

400 max concurrent users | 1200 max configured users

Server configuration	Single server
----------------------	---------------

400 max concurrent users | 1200 max configured users (cont'd)

WFM application and database server	Large
Offboard iCalendar server (optional)	Small
Dedicated SQL Server memory	4 GB
Minimum SQL Server database storage	200 GB
Total storage	WFM server: 260 GB iCalendar server: 60 GB

800 maximum concurrent users | 2400 maximum configured users

Server configuration	Single server with offboard SQL Server
WFM application server	Large
Offboard SQL Server database server	Large
Offboard iCalendar server (optional)	Small
Dedicated SQL Server memory	6 GB
Minimum SQL Server database storage	400 GB
Total storage	SQL Server: 460 GB WFM server: 60 GB iCalendar server: 60 GB

WFM in a Cisco UCS Environment

WFM is certified to run on any Cisco Unified Computing System (UCS) server with resources available to support the OVA/OVF template.

The virtual server requirements for deployments on UCS servers are specified on the Cisco wiki page "Virtualization for Cisco Unified Work Force Optimization Suite for Cisco Unified Contact Center Express" located at this URL:

http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_Unified_Work_Force_Optimization_Suite_for_Cisco_Unified_Contact_Center_Express

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](#)).

The following versions of VMware are supported:

- VMware ESX 3.0 and 3.5
- VMware ESXi 4.0, 4.1, and 5.x

It is recommended that you configure the following settings to reduce the possibility of performance issues when running WFM on virtual machines:

- Shares—Guarantees that VMs are given a percentage of an available resource (CPU, RAM, storage I/O, network)
- Limits—Guarantees that a VM does not consume more than a specified resource limit
- Resource Reservation—Provides an allocated resource for a VM on startup

Server Operating Systems

The supported operating systems for WFM servers are the following:

- 64-bit Windows Server 2012
- 64-bit Windows Server 2008

Note: Since the WFM services do not have direct version/update dependencies, it is permissible to apply updates to the server operating system as recommended by Microsoft.

Desktop Requirements

WFM is operating system-independent. The only requirement is that the OS can run the supported web browsers.

Third Party Software Requirements

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

- Microsoft SQL Server 2008 or 2012, 64-bit, Standard and Enterprise Editions, including the latest service pack
- Adobe Reader 6.0 or later (on client desktop)
- Microsoft Internet Explorer 8, 9, 10, or 11, 32-bit (on client desktop)
- Google Chrome 34 (requires SR3) (on client desktop)

Note: You can try browsers other than Internet Explorer (for example, Firefox) if you want to improve performance. However, these browsers were not tested and are not supported. If problems are found while using an unsupported browser, you will be asked to recreate the problem while using a supported browser.

Microsoft Internet Explorer Requirements

You must disable any popup blockers in Internet Explorer in order for WFM to function correctly.

Configuration Data Requirements

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 ...\\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) or any other security software on your WFM server, shut it down before you back up the WFM database. If any security software is running while you run SQL Server backup utilities, the backup might fail.

Server Configurations

The following sections describe the supported server configurations for WFM.

SQL Server Clustering

If you are using SQL Server clustering, the WFM database must be installed on a dedicated SQL Server instance. No other databases can be installed on that instance.

Concurrent SQL Server Versions

SQL Server 2008 and SQL Server 2012 can be used concurrently in your system. For example, you might use SQL Server 2012 for the ACD database and SQL Server 2008 for the WFM database.

If your system has multiple servers, SQL Native Client (part of the SQL Server Tools) must be installed on the servers that do not host SQL Server. SQL Native Client is required to maintain system configuration data. In a multiple version system, you must use the version of SQL Native Client that matches the most recent version of SQL Server in your system.

Example: If you use SQL Server 2012 for your ACD database and SQL Server 2008 for your WFM database, then you must use the 2012 version of SQL Native Client.

Single Server/Onboard SQL Server Deployment

This deployment has one ACD cluster with all WFM services and SQL Server located on one server. It includes the option of installing the iCalendar service on a dedicated server in the DMZ so agents can access their calendars via the internet. If access is from within your network, the iCalendar service can be installed on an application server.

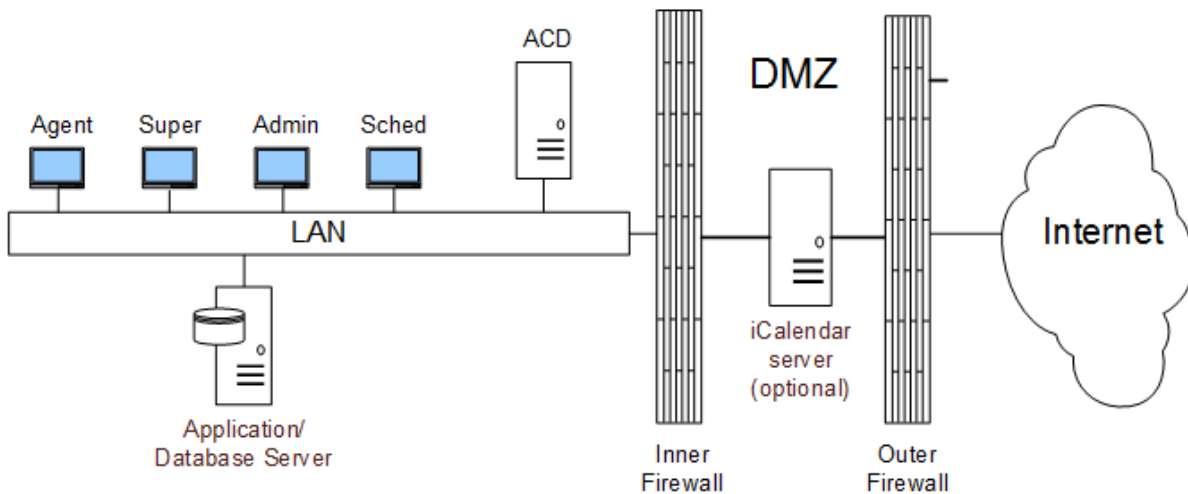
Install components on the server as outlined below.

Application/Database Server

Installed Components	Comments
SQL Server	Install before installing any other components
WFM services	

Optional Application Server

Installed Components	Comments
WFM iCalendar service	<p>Install on a dedicated server located in your DMZ.</p> <p>The “Use secure/encrypted connections” option on the WFM Configuration Setup Enterprise Settings step must be set the same as it is on the application/database server.</p>



Single Server/Offboard SQL Server Deployment

This deployment has one ACD cluster with a WFM application server and an offboard SQL Server. It includes the option of installing the iCalendar service on a dedicated server in the DMZ so agents can access their calendars via the internet. If access is from within your network, the iCalendar service can be installed on an application server.

Install components on the servers as outlined below.

Application Server

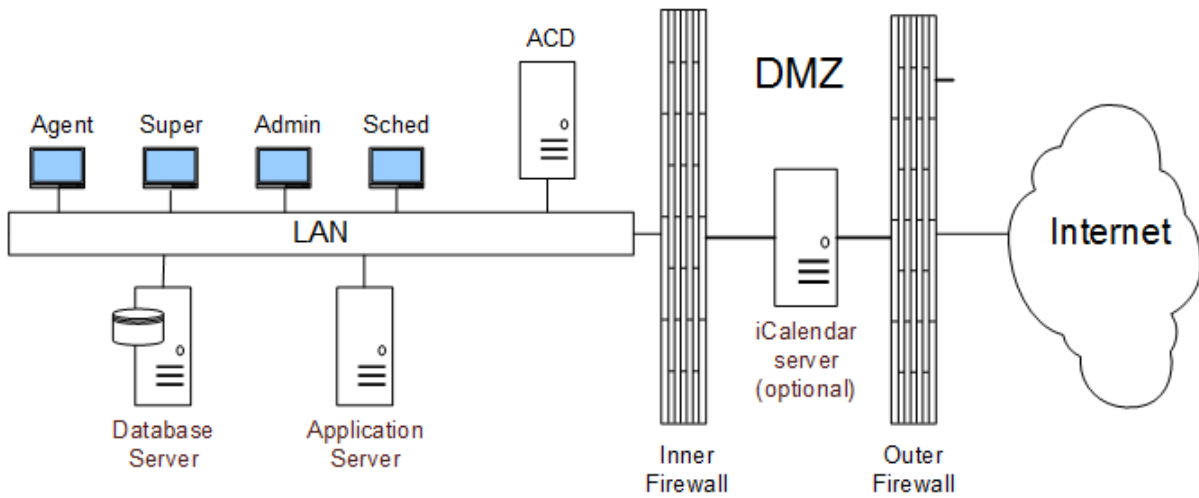
Installed Components	Comments
SQL Server Tools	Install before installing the WFM services
WFM services	

Database Server

Installed Components	Comments
SQL Server	Install before installing WFM services

Optional Application Server

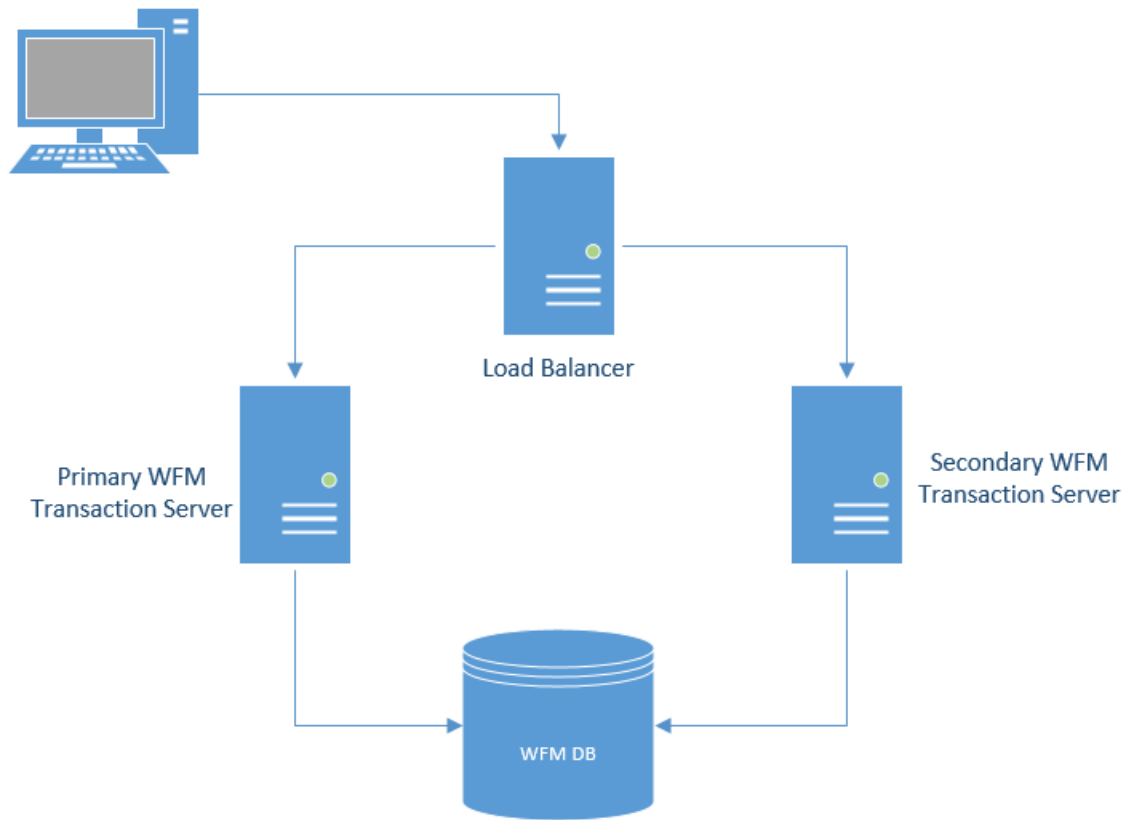
Installed Components	Comments
WFM iCalendar service	<p>Install on a dedicated server located in your DMZ</p> <p>The "Use secure/encrypted connections" option on the WFM Configuration Setup Enterprise Settings step must be set the same as it is on the application/database server.</p>



Web Server Redundancy

WFM can be configured to include third party load balancer hardware and software (not included with WFM) and a second WFM Transaction server in order to provide web server redundancy for the Unified Workforce Optimization interface.

This configuration enables WFM to fail over from a primary Transaction server to a secondary Transaction server in the event that the primary server goes down so there is no interruption for users.



In this type of configuration, the load balancer provides a virtual IP address that the client browsers connect to. The load balancer forwards browser requests to the primary Transaction server if it is up, or to the secondary Transaction server if it is not.

Note: In the event of a failover, users are logged out and must log in again.

Each Transaction server hosts all the WFM Transaction services, but only on the primary server are all services enabled. The services on the secondary server are enabled or disabled manually as per the table below.

Service Status

WFM Transaction Service	Enabled on Primary	Enabled on Secondary
WFM Jetty service	Yes	Yes

Service Status

WFM Transaction Service	Enabled on Primary	Enabled on Secondary
WFM Product Adapter service	Yes	Yes
WFM RTE service	Yes	No
WFM ACC service	Yes	No
WFM MANA service	Yes	No
WFM Sync service	Yes	No

To install the secondary Transaction server:

1. Install the WFM Transaction services on the secondary Transaction server.
2. Disable all WFM services except for the WFM Jetty and WFM Product Adapter services (see table above).
3. Run WFM Configuration Setup (Postinstall) and make sure that you point to the same WFM database as you did on the primary Transaction server.

If WFM is installed in a multiple WFO product environment, you must configure the system as outlined below. This enables the load balancer to fail over all WFO products completely in the event that any of the monitored components fails.

To configure a load balancing system in a multiple WFO product environment:

1. On the primary WFM Transaction server, set the Unified Workforce Optimization container to the IP address of the primary Cisco Quality Management server.
2. On the secondary WFM Transaction server, set the Unified Workforce Optimization container to the IP address of the secondary Cisco Quality Management server.
3. In the load balancer, configure the monitor group for the primary Cisco Quality Management server to include the primary WFM Jetty server (Port 80).
4. In the load balancer, configure the monitor group for the secondary Cisco Quality Management server to include the secondary WFM Jetty server (Port 80).

Before You Install WFM

This section describes the tasks that should be done before you install the WFM services.

Prerequisites

The following sections outline the information you should gather and what needs to be set up before you install WFM.

Active Directory

If you are using Active Directory in your WFM installation, you need the following information:

- Active Directory distinguished names and ports (if you are not using a default port)
- Active Directory paths to the users
- Common names (CN) from the Active Directory account and password
- The complete path and file name of the Active Directory certificates. The certificates must be located on a local drive on the WFM server, not on a network drive.

Cisco Unified Contact Center Express

When using a Cisco Unified Contact Center Express (Unified CCX) ACD, you must install and configure the following systems before you install WFM:

- Cisco Unified Contact Center Express
- Cisco Unified Communications Manager

You need to know the following information:

- IP address and port number of the server that hosts the CTI service
- 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

Note: The Unified CCX server IP address and the CTI server IP address are always the same.

GIS API

If you want to include historical data for non-voice contacts, before you install WFM you must install and configure an FTP server to transfer historical data files from the ACD to WFM using the Generic Interface Services (GIS) API.

For more information on using the GIS API, see the *GIS API Reference Guide*.

SMTP

If you are using email notifications in your WFM installation, you need the following SMTP (simple mail transfer protocol) information:

- The host name or IP address of the SMTP server
- The port used to access the SMTP server
- The user and password used to access the SMTP server, if authentication is required

SNMP

If you will use Simple Network Management Protocol (SNMP) to send notification messages in your WFM installation, you must install the Windows SNMP service on the WFM server that hosts the WFM Transaction services.

WFM

To install WFM, you need the following information:

- The IP address for each server in your WFM configuration
- WFM SQL Server database username and password (see [Creating a SQL Server Login for WFM](#))
- SQL Server instance name (see [Installing Microsoft SQL Server](#))
- The IP address of the Cisco Quality Management base services server, if you are using that part of the Unified Workforce Optimization suite

Installing Microsoft SQL Server

If you are not off-boarding SQL Server, Microsoft SQL Server 2008 or 2012 is installed on the WFM server where you plan to install the WFM Transaction services.

If you are off-boarding SQL Server, you must install the SQL Native Client (one of the SQL Server Tools) on the WFM server. See [Installing Microsoft SQL Server Tools](#) for instructions on installing SQL Native Client.

Note: Since the WFM services do not have direct version/update dependencies, it is permissible to apply updates to SQL Server as recommended by Microsoft.

An abbreviated installation procedure is provided below. For detailed installation instructions, see the Microsoft SQL Server installation documentation.

To install Microsoft SQL Server:

Complete the SQL Server Setup utility windows as described below.

Setup window	Complete as follows
Registration Information	Enter your name, company, and product key
Components to Install	Select SQL Server Database Services, Workstation components, and any other desired component. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Note: If you install the SQL Server 2008 Reporting Services Tool, you must configure it so that it does not use TCP port 80 (using this port interferes with the WFM Jetty service). See the <i>Firewall Configuration Guide</i> for more information.</p> </div>
Instance Name	Select one of the following options: Default Instance or Named Instance. If you select Named Instance, specify the named instance.
Service Account	Select Use the Built-In System Account, then select Local System from the drop-down list.

Setup window	Complete as follows
Authentication Mode	Select Mixed Mode. Enter a password for the SQL Server Administrator (sa) logon.
Collation Settings	<p>Under SQL Collations, select this option:</p> <p>Dictionary order, case-insensitive, for use with 1252 Character Set</p> <p>The SQL collation name is SQL_Latin1_General_CP1_CI_AS. For more information on collation settings, see the Microsoft Developer Network topic, "SQL Server Collation Name (Transact-SQL)" at http://msdn2.microsoft.com/en-us/library/ms180175.aspx</p>

Creating a SQL Server Login for WFM

Consult the SQL Server documentation for instructions on creating a login and password that will allow WFM to connect with SQL Server.

The login you create must have the DB_creator role (be able to create databases and run the WFM administrative scripts) during the installation of WFM. After WFM is installed, the role can be reduced to DB_reader and DB_writer if desired.

When configuring the login, be sure to clear the Enforce password policy check box so that the WFM user account does not expire.

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

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.

Installing SQL Server Native Client

SQL Server Native Client must be installed if your system includes an offboard SQL Server.

SQL Native Client is automatically installed when you run the setup for Microsoft Server Tools.

For more information about installing SQL Server Native Client and settings, see the Microsoft Developer Network topic, "Installing SQL Server Native Client" at

<http://msdn.microsoft.com/en-us/library/ms131321.aspx>.

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 editor 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 the following table.

Value	Type	Data
iCalendarType	string	1
iCountry	string	1

Value	Type	Data
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	/

Value	Type	Data
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

Configuring Firewall Port Exceptions

If Microsoft Windows Firewall is enabled when WFM is installed, the installation process opens the necessary firewall ports.

Ports must be opened manually in these situations:

- If another firewall is used
- If you turn on the Windows Firewall after WFM is installed

- If you want to allow agents to access their calendars on mobile devices via the iCalendar service

See your firewall documentation for instructions on configuring manual port exceptions. See the *Workforce Optimization Suite Firewall Configuration Guide* for a list of the ports used by WFM.

Disabling Internet Information Services for Windows Server

Before you install WFM for the first time (a clean install) you must disable Internet Information Services (IIS). If it is not already disabled, IIS overrides the WFM Jetty service and prevents the WFM login page from being displayed in the web browser.

To disable IIS:

1. Use the Windows Services utility to stop the World Wide Web Publishing Service on the server where you intend to install WFM.
2. Change the service's startup type from Automatic to Manual to prevent it from starting again.

Refer to your Windows documentation for more information on disabling services.

Installing WFM

This section describes how to install and upgrade WFM.

Preinstallation Considerations

Before you install, upgrade, or patch WFM, it is recommended that you take the steps outlined below.

For All Types of Installs

It is strongly recommended that you shut down any security software, such as Cisco Security Agent (CSA), before you do any of the following:

- Install WFM
- Upgrade from one version of WFM to another
- Install a patch

Security software can have an adverse effect on the installation process and cause the installation to fail.

For Upgrades

Before you install a WFM upgrade, do the following:

- Because installing a WFM upgrade requires bringing down a WFM system, schedule installation for a maintenance period when your WFM system is out of production.
- Run the old WFM version of WFM Configuration Setup (Postinstall) and note the settings. Not all WFM settings are maintained during the upgrade process. You must enter them again after you install the upgrade.
- Back up the old SQL Server WFM database using SQL Server backup tools.

Note: Do not remove the old SQL Server WFM database. It is required during the

upgrade process. Backing up your database is recommended in case a problem occurs during the upgrade.

- Uninstall any patches (ETs, ESs, and SRs) applied to the old version of WFM. For instructions, see [Removing Patches](#). Removing a patch takes approximately 10 minutes, followed by a server reboot.
- Uninstall the old version of WFM. For instructions, see [Removing WFM Services](#). Removing a WFM base release takes approximately 10 minutes. The system does not reboot.

Note: When you remove WFM, the WFM SQL Server database instance remains.

Upgrading Systems with Pending Capture Requests

The upgrade process deletes pending capture requests. If your system has pending capture requests that you do not want to lose, follow these steps to ensure that your data is captured without interruption.

To capture data without interruption:

1. Stop the Capture service.
2. Ensure that all compile requests that are pending are processed before the upgrade so there is a clean cut-off.
3. Clean up any other pending requests you do not want to run.
4. Upgrade your system.
5. If necessary, put in manual capture requests for the time period that was missed during the upgrade process.

For Patches

Before you install a WFM ET, ES, or SR, do the following:

- Because installing a WFM patch requires bringing down a WFM system, schedule installation for a maintenance period when your WFM system is out of production.

- Run WFM Configuration Setup (Postinstall) and note the settings used. Not all WFM settings are maintained when a patch is installed, and you might need to enter them again.
- Back up the SQL Server WFM database using SQL Server backup tools.

Installing a Base Release

Install the WFM services according to the supported system configuration as described in the section, [Server Configurations](#).

To install a WFM base release:

1. On the WFM server, log in as a local administrator.
2. Shut down any security software that might be running.
3. On the installation CD, double-click setup_WFM_<version>.exe to start the InstallShield Wizard.
4. Click Next to display the Custom Setup window.
5. Select the services or group of service you want to install on the server.
6. The default installation folder is C:\Program Files (x86)\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).

7. Click Next to continue. Follow the InstallShield Wizard prompts until the installation is finished.

Note: During the install process, a command window opens and displays the message, "ATTENTION: This window is part of the Workforce Management installation process. Do not close this window, it will self terminate when finished." Be sure to leave this command window open as instructed. It closes on its own after you complete WFM Configuration Setup.

8. After the installation is complete and the InstallShield Wizard closes, WFM Configuration Setup (Postinstall) starts. See [Configuring WFM](#) for instructions on how to configure the services you just installed.
9. After you have completed WFM Configuration Setup, restart your security software (if present on the server).

Installing an Upgrade

Note: Review [Preinstallation Considerations](#) before installing an upgrade.

WFM 10.5 supports upgrades from the following versions:

- WFM 8.5(1)
- WFM 8.5(2)
- WFM 10.0(1)

Upgrades from all other versions are indirect as per the upgrade paths shown in the following table.

Upgrade paths to WFM 10.5

From version	Instructions
8.5(1), 8.5(2), 10.0(1)	Follow the upgrade instructions in this section.
8.3(3), 8.3(4)	Upgrade to version 8.5(1). Follow the upgrade instructions in the <i>WFM Installation Guide</i> for version 8.5(2).

IMPORTANT: Over the top upgrades are not supported. All upgrades must be manual. This means that the old version of WFM (but not your WFM database) must be uninstalled before the new version is installed.

Note: If you have a generic ACD or Avaya ACD that uses flat capture files, the archived capture files located in the ...WFO_WFM/reports/archive folder will be deleted during

an upgrade. If you want to preserve those archived capture files, copy them to a safe location out of the WFO_WFM file structure before you upgrade. You can restore them to the archive folder after the upgrade is completed. Bear in mind that the data in the capture files is already in the WFM database, which is preserved in the upgrade, so these files are not crucial for running WFM, but you might want to keep them for other reasons.

To upgrade to WFM 10.5:

1. On the WFM server, log in as the local administrator.
2. Shut down any security software that might be running.
3. Stop all the WFM services.
4. Uninstall the old version of WFM.

Note: Do not uninstall the WFM database.

5. Double-click setup_WFM_105.exe to start the installShield Wizard.
6. Follow the instructions in the InstallShield Wizard.
7. Configure WFM. For instructions, see [Configuring WFM](#).
8. If present on the server, restart your security software.
9. After installation and configuration, log into WFM as an administrator and test your WFM system to ensure that it is working properly.

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

Installing a Patch

Note: Review [Preinstallation Considerations](#) before installing a patch.

WFM is upgraded periodically. The upgrade can be one of three types: an engineering test (ET), an engineering special (ES), or a service release (SR).

<p>Engineering Test</p>	<p>An ET is an installable component that contains the files needed to assist developers in diagnosing a problem. ETs are intended for limited scope tests.</p> <p>There can be only one ET on a system at a time. The ET appears in the Windows Programs and Features (Add/Remove Programs) utility in Control Panel and can be removed through that utility.</p>
<p>Engineering Special</p>	<p>An ES is an installable component that addresses a specific bug fix needed by a customer. An ES is cumulative. If multiple ESs are issued against a base release, the latest ES contains all the fixes provided in the ESs previously issued.</p> <p>ESs are installed separately, and each ES appears in the Windows Programs and Features (Add/Remove Programs) utility in Control Panel. This enables each ES to be uninstalled so that it is possible to roll back to a previous state.</p>
<p>Service Release</p>	<p>An SR contains all patches for all bugs found and fixed since the base release of the product. An SR is cumulative. If multiple SRs are issued, the latest SR contains all the fixes in all previously issued patches.</p> <p>SRs are installed separately, and each SR appears in the Windows Programs and Features (Add/Remove Programs) utility in Control Panel. This enables each SR to be uninstalled so that it is possible to roll back to a previous state.</p>

Consider these guidelines when installing a patch:

- Uninstall an ET before installing an ES or SR. Only one ET can exist on a system at a time. You cannot install an ES or SR until the ET is removed.
- Only the latest ES or SR can be removed. The Remove button is disabled for all older ESs and SRs.

To install an ET, ES, or SR:

1. On the WFM server, log in as the local administrator.
2. Shut down any security software that might be running.
3. Stop all WFM services.
4. Uninstall any ET that might be installed.
5. Run WFM_<base version>_SR<version>ES<version>_setup.exe (for ESs and SRs) or WFM_<base version>_ET_setup.exe (for ETs).
6. Follow the instructions in the InstallShield Wizard.
7. After the patch is successfully installed, start WFM Configuration Setup.
8. Click through the steps in WFM Configuration Setup and verify that the information entered in each step is correct. The information should have carried forward from what was entered for the base software release.
9. Close WFM Configuration Setup.
10. If the WFM services do not start after you have completed WFM Configuration Setup, start them manually.
11. If present on the server, restart your security software.

Configuring WFM

The WFM Configuration Setup utility is used to configure the WFM environment after you have installed the WFM services.

Note: WFM Configuration Setup is generally referred to as "Postinstall" since its executable is `postinstall.exe`, and that is how it is referred to in this section.

Postinstall has two modes:

- **Initial Mode.** Postinstall is launched automatically in Initial Mode after the WFM installation finishes. After you configure all of the required parameters, the WFM services start automatically and the system is ready for use.
- **Update Mode.** After Postinstall is run in Initial Mode, you can start it manually in Update Mode to change configuration settings in an existing system.

To launch Postinstall manually on any WFM server, double-click

```
<install folder>\WFO_WFM\bin\postinstall.exe
```

The following is a list of all possible steps that can appear when you run Postinstall in 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](#)
- Create WFM DB (action only; this step creates the WFM database)
- [WFM Server Step](#)
- Update KeyStore (action only; this step updates the WFM keystore with the webserver certificate used when accessing Unified Workforce Optimization via https)
- [Data Retention Periods Step](#)
- [ACD Connection Step](#)
- [QM Connection Step](#)

- [Administrator Password Step](#)
- [WFM Authentication Step](#)
- [Email Distribution Step](#)
- [Monitoring and Notification Step](#)
- [Enterprise Settings Step](#)
- Start Services (action only; this step starts all the WFM services)
- Finish Configuration (action only; this step configures the WFM Windows registry settings)

WFM Database Step

The WFM Database step configures access to the WFM database.

The screenshot shows a dialog box titled "WFM Database". At the top, there are two radio buttons: "Host Name" (unselected) and "IP Address" (selected). Below this, there is a text input field labeled "Host Name or IP Address" containing the value "10.192.100.32". Underneath, there are three more text input fields: "DB Instance Name" with the value "SMAUG", "User Name" with the value "wfmuser", and "Password" with the value "*****". At the bottom of the dialog, there are two buttons: "PREVIOUS" and "NEXT".

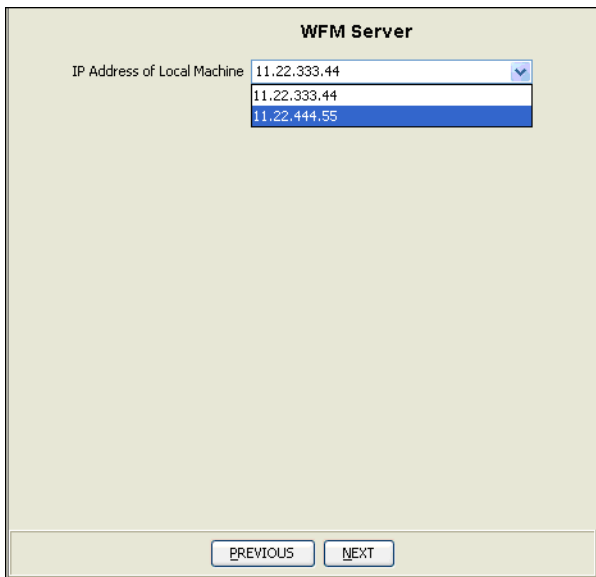
Field	Description
Host Name/IP Address	Select the server name format option.

Field	Description
Host Name or IP	<p>The host name or IP address of the server that hosts the WFM database.</p> <p>Note: You cannot change this setting in Update Mode. If the host name or IP address changes after WFM is configured, you must reinstall WFM.</p>
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>. You can use the default value, a named instance, or leave the field blank. Leaving the field blank is the same as using the default instance.</p> <p>Note: You cannot change this setting in Update Mode. If the database instance name changes after WFM is configured, you must reinstall WFM.</p>
User Name	<p>The user name with access to the SQL Server CWFM database. The user is the one created when installing Microsoft SQL Server (see Creating a SQL Server Login).</p> <p>Note: The default language for this user must be set to US English.</p>
Password	The SQL Server user's password.

WFM Server Step

The WFM Server step configures the IP address of the server where the WFM services are installed. It appears only if Configuration Setup detects that there is more than one network interface card (NIC) on the server.

Select the public IP address used by clients to connect to the server from the drop-down list.



The image shows a configuration dialog box titled "WFM Server". It features a label "IP Address of Local Machine" followed by a dropdown menu. The dropdown menu is open, showing three options: "11.22.333.44", "11.22.333.44", and "11.22.444.55". The second option is currently selected. At the bottom of the dialog box, there are two buttons: "PREVIOUS" and "NEXT".

Data Retention Periods Step

The Data Retention Periods step configures how long WFM historical data, schedule data, productivity data, and user requests are retained in the WFM database.

Data Retention Periods

Agent Adherence Detail Days (1-399)

Forecasts
Schedules
Agent Requests Months (12-99)
Assigned Exceptions

Historical Service Data Months (6-99)
Agent Productivity Data Months (6-99)

GIS Agent
Productivity/Service Days (1-399)
Historical Data files

Vacation Report files Days (1-399)

Time to purge the retention period data (default = 04:00)

Note: Any changes made to data retention periods are applied as soon as you click Next or select another step in the navigation pane.

Field	Description
Agent Adherence Detail	<p>Value from 1–399 days. Default = 15 days.</p> <p>Agent adherence detail information is the agent state data needed to calculate adherence.</p> <div style="border: 1px solid #ccc; background-color: #e6f2e6; padding: 10px; margin-top: 10px;"><p>Note: Agent adherence detail data includes every phone state every agent enters for every day. As a result, the amount of data stored can quickly become very large. The longer the retention period you configure here, the more server storage space is required.</p></div>

Field	Description
Forecasts Schedules Agent Requests Assigned Exceptions	Value from 12–99 months. Default = 25 months. This information is forecast data, agent schedules, agent requests displayed in the Messaging application, and the exceptions assigned to agents.
Historical Service Data	Value from 6–99 months. Default = 25 months. This information is all the ACD contact data gathered for each service queue.
Agent Productivity Data	Value from 6–99 months. Default = 25 months. This information is the ACD data gathered for each agent that measures agent productivity.
GIS Agent Productivity/Service Historical Data files	Value from 1–399 days. Default = 30 days. These are the historical data files imported into WFM by the GIS Connector Tool.
Vacation Report files	Value from 1–399 days. Default = 30 days. These are the files containing agent vacation hours data imported from the HRMS.
Time to purge the retention period data	Default = 04:00 (24-hour format) Set the time of day that data that is beyond the configured retention period is purged from the database.

- Any data that reaches the end of the configured retention period is deleted from the database at the next scheduled purge. By default, the data purge process runs nightly at 04:00, but can be configured to whatever time of day is desired. If the retention period is shortened, all data that exceeds the new retention period is deleted at the next purge. Likewise, if the retention period is extended, no data is purged until the new retention period is exceeded.
- Agent adherence detail data is retained in full days. For example, if the current date is June 15, 2012 and the retention setting is 10 days, then data older than June 5, 2012 will be purged.

- Note that there can be a short time when more than 10 days' worth of data is available. Consider agent adherence detail data that was available as of 01:00 on June 15, 2012. At that time the purge process has not yet run. The last purge was sometime after 04:00 on June 14, so data back to June 4 is still available. Once the June 15 purge runs, the data from June 4 is gone and data is retained from June 5 to the present.
- Agent productivity and historical service data is retained in full months. For example, if the current date is June 15, 2012 and the retention setting is 25 months, then data older than May 1, 2010 will be purged.
- Scheduling and forecasting data is retained in full months, plus any additional days necessary to preserve the schedule week. For example, if the current date is Friday, June 15, 2012, the starting day of the schedule week is configured as Sunday, and the retention time setting is 13 months, then data older than Sunday, April 25, 2011 will be purged. This is because May 1, 2012 is a Saturday, so data is retained for the rest of that schedule week (back through Sunday, April 25, 2011).

ACD Connection Step

The ACD Connection step configures your WFM system's connection to your ACD.

Cisco Unified CCX ACD

ACD Connection

Select Language:

Primary IP Address or Host Name:

Primary Instance Name:

Secondary IP Address or Host Name:

Secondary Instance Name:

User Name:

Password:

Client Locale:

Server Locale:

	IP Address or Host Name	Port
CTI Servers	10.192.252.57	12028
	10.192.252.58	12028

Field	Description
Select Language	Select the language used in the contact center. This field appears only if a localized version of WFM has been installed.
Primary IP Address or Host Name	Enter the ACD's primary IP address or host name.

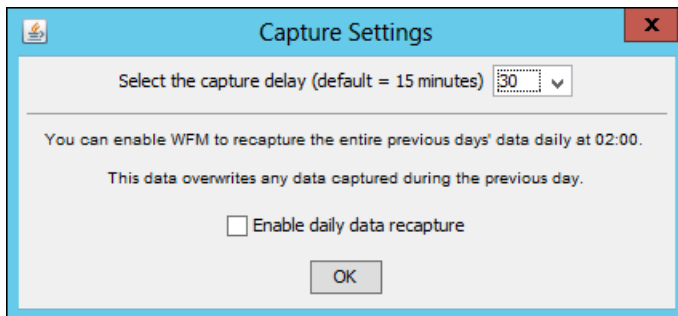
Field	Description
Primary Instance Name	<p>Enter the primary Unified CCX database instance name. When entering the database instance name, use the following guidelines:</p> <ul style="list-style-type: none"> ■ Convert all uppercase letters to lowercase letters ■ Replace all hyphens with underscores ■ If the host name starts with a number, add the prefix “i” ■ Append <code>_uccx</code> to complete the instance name <p>Example: If your host name is 80-ABC, your instance name will be <code>i80_abc_uccx</code>.</p>
Secondary IP Address or Host Name	If this is a redundant system, enter the ACD's secondary IP address or host name.
Secondary Instance Name	Enter the secondary Unified CCX database instance name. See Primary Instance Name for the format the instance name must be in.
User Name	Enter the Unified CCX database user name.
Password	Enter the Unified CCX database user's password.
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 Postinstall.
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 Postinstall.

Field	Description
CTI Server	The CTI servers and ports associated with your system. To add a CTI server to the list, click Add and enter the CTI server host name or IP address and port, then click OK.
Capture Settings button	Click to configure the data capture delay and optional daily data recapture. See Capture Settings for more information.

Capture Settings

By default, the WFM Capture service pulls ACD statistics 15 minutes after an interval ends. If your contact center has calls in progress for longer than 15 minutes at this time, then those calls are not included in that data capture.

You can use the Capture Settings dialog box to change the capture settings to a value that works best with the length of calls handled by your contact center. You can select a capture delay between 15–135 minutes.



If you routinely handle calls that last more than the maximum default delay, you can opt to recapture the entire previous day's data (from midnight to midnight) at 02:00 daily. The recaptured data overwrites what was captured during the day. This ensures that your statistics are correct and that the data for very long calls is in the correct interval.

QM Connection Step

The QM Connection step is used if you are using the Cisco Quality Management part of the Unified Workforce Optimization suite.

QM Connection

Quality Management Is Installed

Host Name IP Address

Host Name or IP

Field	Description
Quality Management is Installed	Select the check box if you are using Cisco Quality Management.
Host Name or IP Address	Indicate which format is used for the server name.
Host Name or IP	The host name or IP address of the Cisco Quality Management base services server.

WFM Authentication Step

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

WFM Authentication

Authentication With Other Calabrio Products

Share Login Fields

Calabrio One Container(IP or Host Name)

Active Directory

Use Active Directory

User must have read access to the given domain.

Base DN	Domain Name	IP Address...	Port	User Displa...	User
dc=p2,dc=r...	p2.rd.ld	10.192.252.12	389	rd ldap	****

<
>

Field	Description
Share Login Fields	Select this check box if you want to share login fields in the Unified Workforce Optimization container with other Unified Workforce Optimization products.
Calabrio ONE Container (IP or Host Name)	Enter the host name or IP address of the Unified Workforce Optimization container. If you are sharing login fields with Cisco Quality Management, this must be the the host name or IP address of the Cisco Quality Management base services server.

Field	Description
Use Active Directory	<p>Select this check box if you will be using Active Directory with WFM.</p> <div style="border: 1px solid #ccc; background-color: #e6f2e6; padding: 10px; margin-top: 10px;"> <p>Note: You cannot change this setting in Update Mode. If you want to enable or disable using Active Directory after WFM is configured, you must reinstall WFM.</p> </div>

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.

Field	Description
Base DN	The location in the directory server tree under which all Active Directory users are located.

Field	Description
Domain Name	The name of the Active Directory domain.
IP Address or Host Name	The IP address or host name of the Active Directory server.
Port	<p>The port used to access the Active Directory server. If you have selected the Use SSL check box, use 636. If you have not selected the Use SSL check box, use 389.</p> <div data-bbox="597 600 1377 785" style="background-color: #e1f5fe; padding: 10px; border-radius: 5px;"> <p>Note: The WFM Transaction services server must be able to access the Active Directory server for user authentication using this port number.</p> </div>
User Display Name	The display name as configured in Active Directory of a user with read access to the Active Directory database.
User Password	The user's password.
User Search Base	<p>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:</p> <p>ou-Users.ou=Minneapolis,ou=Minnesota,ou=US</p>
Use SSL	Select this check box if you want to use a Secure Socket Layer (SSL) for the Active Directory.
Certificate File Names	<p>The complete path and file name of the Active Directory certificate. The certificate must be located on a local drive on the WFM server, not on a network drive. If you have multiple AD certificates, separate the paths/file names with semicolons and no spaces.</p> <div data-bbox="597 1579 1377 1680" style="background-color: #e1f5fe; padding: 10px; border-radius: 5px;"> <p>Note: Certificates must be base-64 encoded.</p> </div>

Field	Description
Admin Group	The name of the user group set up in Active Directory for users who are to be WFM administrators. The name of the group can be anything. As long as a user is a member of the named group, that user will have administrator privileges in WFM.

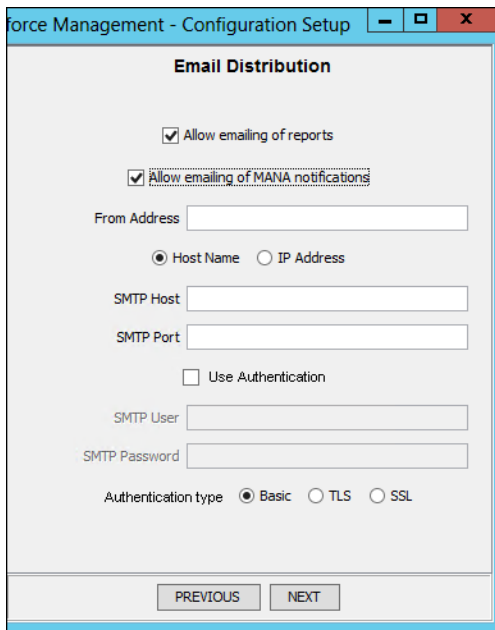
Managing Active Directory Domains

Active Directory domains that have already been added are listed in a table in the WFM Authentication step window. You can edit the information for an existing domain by double-clicking any of the cells in the table and entering new information. When you finish editing the information, click another cell. The change is saved when you move to another step by either clicking Next (in Initial Mode) or selecting another step from the navigation tree (in Update Mode).

To delete an existing domain, highlight the appropriate row in the table and click Remove. You are asked to confirm the deletion.

Email Distribution Step

The Email Distribution step configures whether the system uses email to distribute reports and MANA notifications, and the SMTP server settings needed to generate the emails.



Field	Description
Allow emailing of reports	Select this check box to use email for sending out reports. If selected, the report setup pages in Unified Workforce Optimization display a section that enables the report user to configure the report to be sent to specified email addresses as an attachment.
Allow emailing of MANA notifications	Select this check box to use email for sending out notification messages.
From Address	The email address that all notifications and reports are sent from.
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 to communicate with the SMTP server.
Use Authentication	Select this check box if authentication is needed to access the SMTP server.

Field	Description
SMTP User	The username required to gain access to the SMTP server.
SMTP Password	The SMTP user's password.
Authentication Type	Choose the type of authentication used to access the SMTP server.

Monitoring and Notification Step

The Monitoring and Notification (MANA) step 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

Monitoring and Notification

Use Monitoring/Notification Service

Polling Period (minutes)

Use Event Viewer Notification

Use SNMP Notification

Use Email Notification

[Allow emailing of MANA notification] check box on the previous step

To Addresses

Field	Description
Use Monitoring and Notification Service	Select this check box to use the MANA service. If selected, at least one notification method must be selected as well.
Polling Period (minutes)	Sets the interval at which the MANA service checks for notification triggers. Default = 10 minutes.
Use Event Viewer Notification	Select this check box to use the Microsoft Event Viewer utility (Control Panel > Administrative Tools > Event Viewer) to display notification messages.
Use SNMP Notification	Select this check box to use SNMP for sending notification messages. The Windows SNMP Service must be installed in order to use SNMP notification.

Field	Description
Configure SNMP	Click this button to add an SNMP trap destination. See Configuring SNMP Notification for more information.
Use Email Notification	Select this check box to use email for sending notification messages. The email addresses the notifications are sent to are configured in the To Addresses section. Note: You must also select the Allow emailing of MANA notifications check box on the Email Distribution step to enable MANA emails.
To Addresses	A list of email addresses that MANA notifications are sent to. Use the Add, Remove, and Edit buttons to create the list.

Configuring SNMP Notification

You can use SNMP notification if the Microsoft Simple Network Management Protocol (SNMP) service is installed on the WFM Transaction 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 Turn Windows features on and off link in the Programs and Features utility in Control Panel. Select Simple Network Management Protocol from the list of features.

To add a trap destination for SNMP notification, follow these steps:

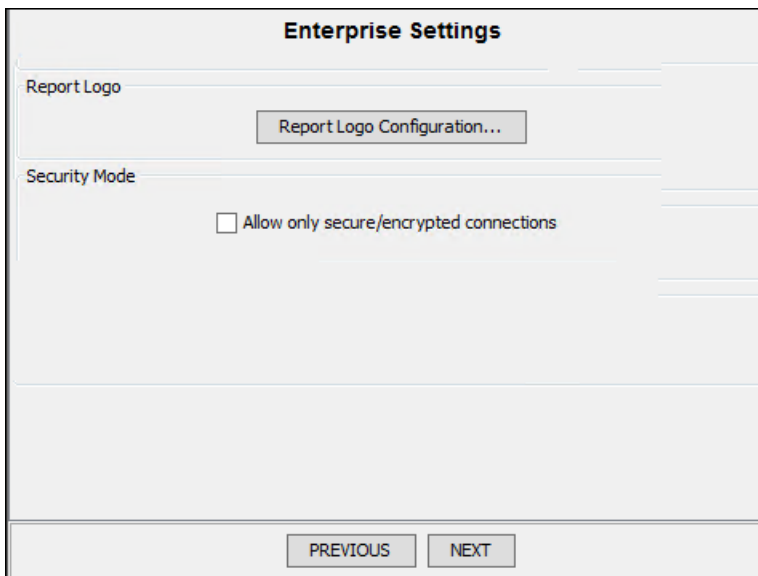
1. In the Monitoring and Notification step window, click Configure SNMP.
2. In the Configure SNMP dialog box, click Add, enter the IP address of the trap destination, and then click OK.
3. Restart the Windows SNMP service to enable the trap destination.

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

Enterprise Settings Step

The Enterprise Settings step is used to configure the following:

- Customize the logo used on reports
- Require the use of a secure connection to access WFM



Field	Description
Report Logo Configuration	Click this button to add a custom logo to your WFM reports. See Configuring the Report Logo for more information.
Allow only secure/encrypted connections	Select this check box to use a secure/encrypted HTTPS connection between WFM and Cisco Quality Management. When this check box is selected, Port 80 is not blocked.

Configuring the Report Logo

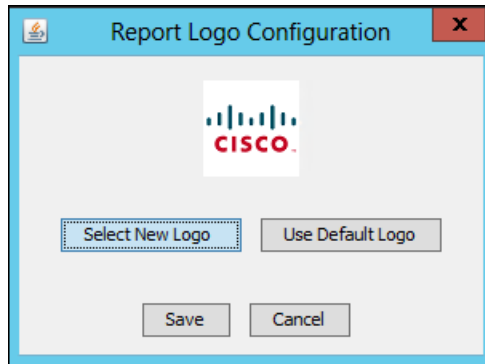
You can customize the logo that appears on WFM reports by replacing the default logo with one of your own.

Custom logos must conform to the following specifications

- The logo must be no larger than 60 × 60 pixels
- It must be in PNG format
- The file must be named “logo.png”

To replace the default logo with your own custom logo, follow these steps:

1. On the Enterprise Settings step, click the Report Logo Configuration button to display the Report Logo Configuration dialog box.



The dialog box displays the logo currently in use.

2. Click Select New Logo, navigate to the location where your custom logo is stored, and click Select Image. The logo will now be displayed in the Report Logo Configuration dialog box.
3. Click Save.

Note: Logos that exceed the 60 × 60 size are reduced proportionally to fit in the allowed area. This can result in a logo that becomes very small and hard to see. It is recommended that you create a logo of the required size for the best results.

To revert a custom logo to the default logo, follow these steps:

1. On the Enterprise Settings step, click the Report Logo Configuration button to display the Report Logo Configuration dialog box.
2. Click Use Default Logo
3. Click Save.

Verifying the Connection to the Unified CCX Database

To verify that WFM has successfully synced to the Unified CCX database:

1. Start WFM and log in as an administrator.
2. Choose Application Management > Agents. If there are agents listed in the Select Agents drop-down list, the synchronization was successful.
3. Navigate to <install folder>\WFO_WFM\log and open the WFM 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.

Configuring the iCalendar Service

The iCalendar service is configured with the ...\\Cisco\WFO_WFM\config\C1Calendar.properties file on the server that hosts the WFM Compile services.

This file can be edited in a text editor to change the logging and debugging parameters. For more information on configuration files, refer to the Configuration Files section of the *Workforce Management Troubleshooting Guide*.

This file can also be edited to configure request filtering to prevent too many requests from being handled by the iCalendar service in a period of time per user.

Configuring the Requests Filter

Request filtering has two parameters:

- Period of time (in minutes)
- Number of requests

The default settings for these parameters are as follows.

```
# period in minutes (<= 0 means no filter)
calendar.requests-filter.period = 10
# max number of requests in period (>0)
calendar.requests-filter.number = 5
```

This ensures that no more than 5 requests are handled in a period of 10 minutes per user. If you want to adjust the period of time or number of requests per user, then change these settings.

If an agent submits more requests that the configured limit, an HTTP error code 403 (forbidden) is displayed.

Note: In order for agents to access their calendars on mobile devices, you must configure your firewall to open the ports used by iCalendar. See [Port Usage](#) for a list of the ports used by WFM.

Capturing Historical Data

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

Note: The WFM Capture service captures data for all periods, regardless of service queue open/closed hours. The Forecast module takes this into account by trimming forecast data to service queue open hours.

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

Capturing Cisco Unified CCX Historical Data

If you use Cisco Unified CCX, import historical data with WFM's Capture Historical Data feature (Application Management > Capture Historical Data). See the *Workforce Management Application User Guide* for information on using this feature.

Removing WFM

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

1. Uninstall all patches and roll back to the previous state
2. Uninstall the WFM services

Removing Patches

Follow these steps to remove a Workforce Management patch from a WFM server. When the patch is removed, your WFM deployment will be reverted to its previous state.

Note: If you cancel the removal process while it is running, the patch might continue to be listed in the Windows Programs and Features utility, and you will not be able to remove or repair the patch or reinstall it. Contact Cisco Technical Support for assistance.

To remove a WFM patch:

1. Log into the WFM server as the local machine administrator.
2. Start the Programs and Features utility in Control Panel.
3. Select the Cisco Unified Workforce Management patch, click Remove Me First, and follow the prompts. After all patches are removed, your system is back to its base level software state.

Note: You can only remove the most recent ES or SR. The Remove Me First button indicates which one is the most recent. All other ES and SR Remove buttons are disabled until that particular ES or SR becomes the most recent one on your system.

Removing WFM Services

When you remove WFM services, the WFM software is completely removed except for the WFM database. The services can be removed in any order.

Note: If there is a patch installed on the Workforce Management server and you want to remove WFM, you must remove the patch first. See [Removing Patches](#) for more information.

To remove WFM services, follow these steps:

1. Log into the WFM server as the local machine administrator.
2. Start the Programs and Features utility in Control Panel.
3. Select Cisco Unified Workforce Management Services, click Remove, and follow the prompts.

Note: A reboot might be required when you remove a base release. If you are prompted to reboot, click No. This reboot prematurely terminates background removal activities. You can manually reboot the machine after the removal process is completed.

Index

A

ACC service 9
ACD Connection step 48
 capture settings 51
 Cisco Unified CCX 49
Active Directory 26
Active Directory domains
 configuring 54
 managing 56

B

Backup and restore database 17
Base release
 installing 36
Browsers
 Internet Explorer
 requirements 17
 supported versions 17

C

Capture requests 35

Capture service 9
Cisco UCS environment 15
Cisco Unified Contact Center
 Express (CCX) 26
Compile service 9
Concurrent SQL Server
 versions 20
Configuration
 single server 20
 single server with offboard SQL
 Server 22
Configuration data
 requirements 17
Custom report logos 61

D

Data Retention Periods step 45
Database requirements 17
Desktop requirements 17

E

Email Distribution step 56

Enterprise Settings step 61

Environment 12

F

Firewall port exceptions 32

Forecast service 9

G

GIS API 27

H

Hardware requirements 12

Historical data, capturing 66

 Unified CCX 66

I

iCalendar service

 configuring 63

Installing WFM

 base release 36

 patch 38

 upgrade 37

Internet Explorer requirements 17

Internet Information Services (IIS)
 for Windows Server

 disabling 33

J

Jetty service 10

M

MANA service 10

MANA step 58

Monitoring and Notification step 58

N

New features 7

P

Patches

 installing 38

 removing 68

Port usage 11

 configuring firewall port excep-
 tions 32

Postinstall 42

preinstallation considerations

 patches 35

Preinstallation considerations

 all types of installs 34

 upgrades 34

 upgrades with pending capture
 requests 35

Prerequisites

 Active Directory 26

 Cisco Unified Contact Center
 Express 26

 GIS API 27

 SMTP 27

 SNMP 27

 WFM 27

Product Adapter service 10

Q

QM Connection step 51

R

Regional settings 30

Removing patches 68

Removing WFM 68

 patches 68

 services 69

Report logos 61

Request service 10

RTE service 10

S

Schedule service 10

Security software 34

Server operating systems 16

Server requirements 12

Single server configuration 20

Single server with offboard SQL
 Server configuration 22

SMTP prerequisites 27

SNMP prerequisites 27

SQL Server

 clustering 20

 concurrent versions 20

 creating a login for WFM 29

 installing 28

 supported versions 17

SQL Server Native Client

 installing 30

SQL Server Tools 30

Supported ACDs 12

Supported operating systems 16

Sync service 10

System environment 12

System requirements 12

T

Third party software

 requirements 17

U

UCS server 15

Unified CCX database, verifying
 connection 63

Unified Computing System
 server 15

Uninstalling WFM 68

Upgrade

 installing 37

V

Verifying connection to Unified
 CCX database 63

Virtual server environment 16

Virtual server requirements 16

VMWare 16

W

WFM

environment 12

removing 68

WFM Authentication step 52

configuring Active Directory
domains 54

managing Active Directory
domains 56

WFM components 6

WFM Configuration Setup 42

ACD Connection step 48

capture settings 51

Cisco Unified CCX 49

Data Retention Periods step 45

Email Distribution step 56

Enterprise Settings step 61

Monitoring and Notification
step 58

QM Connection step 51

WFM Authentication step 52

configuring Active Directory
domains 54

managing Active Directory
domains 56

WFM Database step 43

WFM Server step 44

WFM Database step 43

WFM documentation 8

WFM prerequisites 27

WFM Server step 44

WFM services 9

ACC service 9

Capture service 9

Compile service 9

Forecast service 9

Jetty service 10

MANA service 10

Product Adapter service 10

removing 69

Request service 10

RTE service 10

Schedule service 10

Sync service 10