Cisco Unified Workforce Optimization

Workforce Management Installation Guide Release 11.0

First Published: August 27, 2015

Last Updated: September 9. 2015

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.

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.

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)

Workforce Management Installation Guide

© 2015 Cisco Systems, Inc. All rights reserved.

Contents

Overview **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 Forecast Service 10

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 11

Port Usage 11

WFM Jetty Service Ports 12

System Requirements **13**

Workforce Management Environment 13

System Environment 13

WFM Server Hardware Requirements 13

HDD Partitioning 14

Recommended Installation Paths 15

Capacity and Sizing 16

WFM in a Cisco UCS Environment 18

Virtual Server Environment 18
Server Operating Systems 19
Desktop Requirements 19
Third Party Software Requirements 19
Browser Requirements 20
Configuration Data Requirements 20
Server Configurations 21
SQL Server Clustering 21
Concurrent SQL Server Versions 21
Single Server/Onboard SQL Server Deployment 21
Single Server/Offboard SQL Server Deployment 23
Web Server Redundancy 24
Before You Install WFM 29
Prerequisites 29
Active Directory 29
Cisco Unified Contact Center Express 29
GIS API 30
SMTP 30
SNMP 30
WFM 30
Installing Microsoft SQL Server 31
Creating a SQL Server Login for WFM 32
Installing SQL Server Native Client 33
Configuring Regional Settings 34
Configuring Firewall Port Exceptions 36
Disabling Internet Information Services for Windows Server 36
Installing WFM 39
Installing a Base Release 39

Installing an Upgrade 40
Upgrading from Version 10.5 or Earlier 41
Upgrading to a Newer Version of WFM 11.0 42
Upgrading Systems with Pending Capture Requests 43
Installing a Patch 43
Repairing WFM 44
Configuring WFM 47
WFM Database Step 48
Data Retention Periods Step 50
WFM Server Step 53
ACD Connection Step 53
Cisco Unified CCX ACD 54
Capture Settings 56
QM Connection Step 57
WFM Authentication Step 57
Configuring Active Directory Domains 59
Managing Active Directory Domains 61
Email Distribution Step 61
Monitoring and Notification Step 63
Configuring SNMP Notification 65
Enterprise Settings Step 66
Configuring the Report Logo 67
Verifying the Connection to the Unified CCX Database 69
Configuring the iCalendar Service 69
Capturing Historical Data 71
Capturing Cisco Unified CCX Historical Data 71
Managing Certificates 73
Updating the WFM Signed Certificate 73

Certificates and Active Directory 77
Generating Certificates with Active Directory 77
Installing Root and Intermediate Certificates on Client Desktops 83
Removing WFM 85
Removing an ET 85
Removing WFM Services 85

Overview

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

Installation Group	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 Real Time Engine (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 11.0 includes the following new features:

WFM 11.0(1)

- Added new features:
  - Dynamic scheduling
  - Multiskill scheduling
  - Scheduling incentives
  - Mentoring requests
  - Strategic planning
  - Vacation planning
- Enhanced the scheduling alorithms for multiskill scheduling
- Support for web redundancy for the Workforce Optimization interface
- Support for non-ACD agents in synced systems
- HRMS import/export files and GIS capture files have been moved from their previous location

  C:\PRogram Filese (x86)\Cisco\WFO_WFM

  to a new location:

  C:\Program Files (x86)\Common Files\WFM
- Support for Cisco Unified Contact Center Express 11.0
- Support for Microsoft SQL Server 2014
- Improvements in how service level percentage rollups are calculated
- Bug fixes

WFM Documentation

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

- *Workforce Management Installation Guide*
- *Workforce Management User Guide*
- *Workforce Management Troubleshooting Guide*
- *Workforce Management Data Import Reference 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

The WFM services are installed in groups (see Overview). A brief description of each service is below.

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 Cisco 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

The following table lists the ports used by WFM and its components.

Note: The port numbers listed are defaults. They can be changed as needed.

Server Application	Destination Listening Port	Client Application
CTI service 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" in the *Cisco Customer Response Solutions Administration Guide*.	TCP 12028 Side A TCP 12028 Side B	WFM Sync service WFM RTE service
Unified CCX instance of Informix		WFM Capture service

Server Application	Destination Listening Port	Client Application
WFM instance of SQL Server	TCP 1433 TCP 1434	WFM ACC service WFM Capture service WFM Compile service WFM Configuration Setup WFM Forecast service WFM iCalendar service WFM MANA service WFM Product Adapter server WFM Reports WFM RTE service WFM Request service WFM Schedule service WFM Sync service
WFM iCalendar service	TCP 4430 (HTTPS) TCP 8086 (HTTP)	Any iCalendar client
WFM Jetty service	TCP 59103 (surrogate)	WFM Product Adapter service
	TCP 443 (HTTPS) TCP 80 (HTTP)	Web browser

WFM Jetty Service Ports

The WFM Jetty service uses TCP ports 80 and 443. Make sure that you do not have any other web service installed on the server that hosts the WFM Transaction services that uses these ports, or the Jetty service might fail.

Examples of other web services include Microsoft SQL Server Reporting Services and Microsoft Internet Information Services (IIS).

SQL Server Reporting Services is a tool that provides a web-based interface to present SQL performance information. You can configure this tool to use another port and so not interfere with the Jetty services. Consult your SQL Server documentation for information on changing the port usage.

System Requirements

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

Workforce Management Environment

WFM 11.0 is compatible with Cisco Quality Management 11.0.

System Environment

WFM 11.0 has been verified in the following environments:

- Cisco Unified Contact Center Express Release 8.5
- Cisco Unified Contact Center Express Release 9.0
- CIsco Unified Contact Center Express Release 10.0
- Cisco Unified Contact Center Express Release 10.5
- Cisco Unified Contact Center Express Release 11.0

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)
Minimum processor speed	2 GHz
Memory	All values include 2 GB dedicated for SQL Server use. 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.)

HDD Partitioning

The recommended hard drive disk partitioning for the servers that host WFM and SQL Server are described in the following table.

Server	Hard Disk Partition	Size
WFM servers	Operating system partition (Windows OS)	32 GB (minimum)
	Applications partition (WFM and SQL Server binaries)	See *Capacity and Sizing*
	Database partition (SQL Server database and log files)	See *Capacity and Sizing*
SQL Server server	Operating system partition (Windows OS)	32 GB (minimum)
	Applications partition (SQL Server binaries)	20 GB
	Database partition (SQL Server database and log files)	See *Capacity and Sizing*

Recommended Installation Paths

The following are the recommended locations for WFM files.

File Type	Location	Example
Software installation and license files	Applications partition <partition drive>:\Software\<product>	D:\Software\WFM
WFM application files	Applications partition <partition drive>:\Cisco\WFO_WFM	D:\Cisco\WFO_WFM
SQL Server application files	Applications partition <partition drive>:\Program Files\Microsoft SQL Server	D:\Program Files\Microsoft SQL Server
SQL Server database filese	Database partition <partition drive>:\<customer preference>	E:\SQL_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

200 max concurrent users | 600 max configured users (cont'd)

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
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

800 maximum concurrent users | 2400 maximum configured users (cont'd)

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 *WFM Server 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 and 2012 R2
- 64-bit Windows Server 2008 and 2008 R2

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. See the *Workforce Optimization Suite Desktop Requirements Guide* for more details.

- Microsoft SQL Server 2008, 2008 R2, 2012, and 2014, 64-bit, Standard and Enterprise Editions, including the latest service pack
- Adobe Reader 6.0 or later (on client desktop)
- Microsoft Internet Explorer 9, 32-bit
- Microsoft Internet Explorer 10 or 11, 32-bit, (Desktop mode if running in a Windows 8.1 operating system)
- Google Chrome
- Microsoft Exchange 2007, 2010, 2013, or Office 365

Note: You can try browsers other than those listed here if you want to try 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.

Browser Requirements

You must disable any popup blockers in your browser 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 C:\Program Files (x86)\Cisco\WFO_WFM\config

WFM database backups are independent of Cisco 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, 2008 R2, 2012, and 2014 can be used concurrently in your system. For example, you might use SQL Server 2014 for the ACD database and SQL Server 2012 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 2014 for your ACD database and SQL Server 2012 for your WFM database, then you must use the 2014 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.

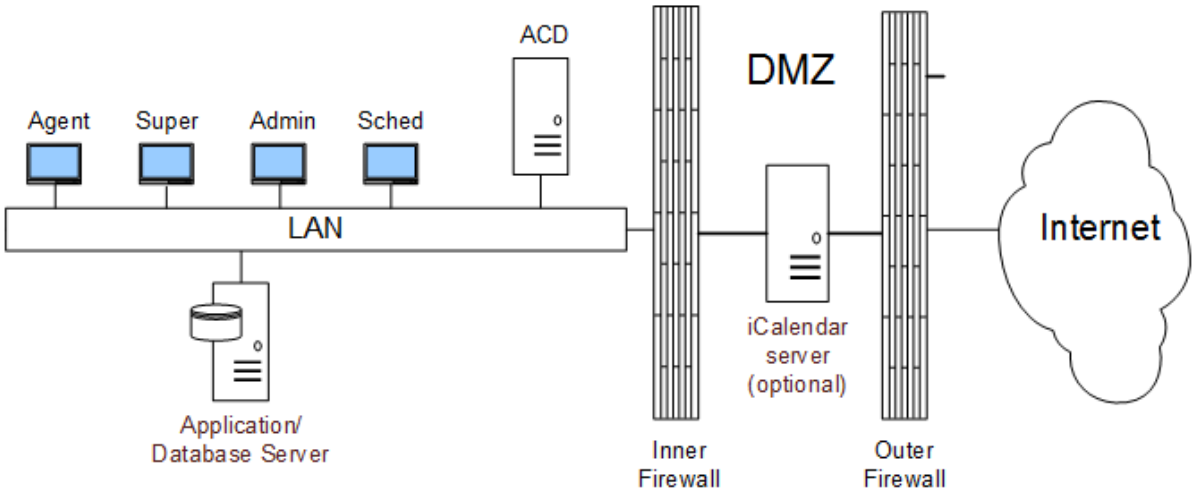
Install components on the server as outlined below.

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	Install on a dedicated server located in your DMZ. 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.



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

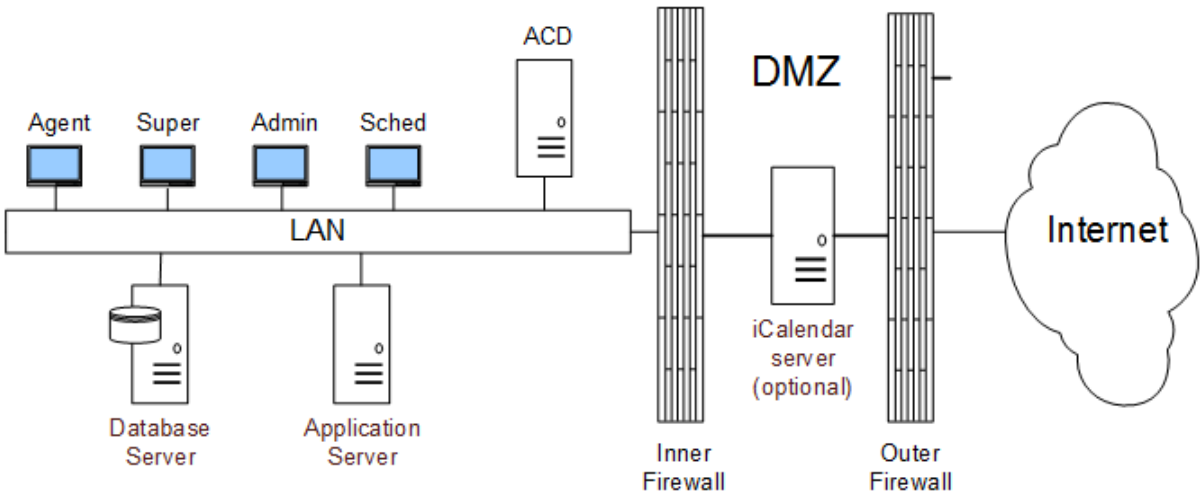
Installed Components	Comments
SQL Server Tools	Install before installing the WFM services
WFM services	

Database Server

Installed Components	Comments
SQL Server	Install before installing WFM services

Optional Application Server

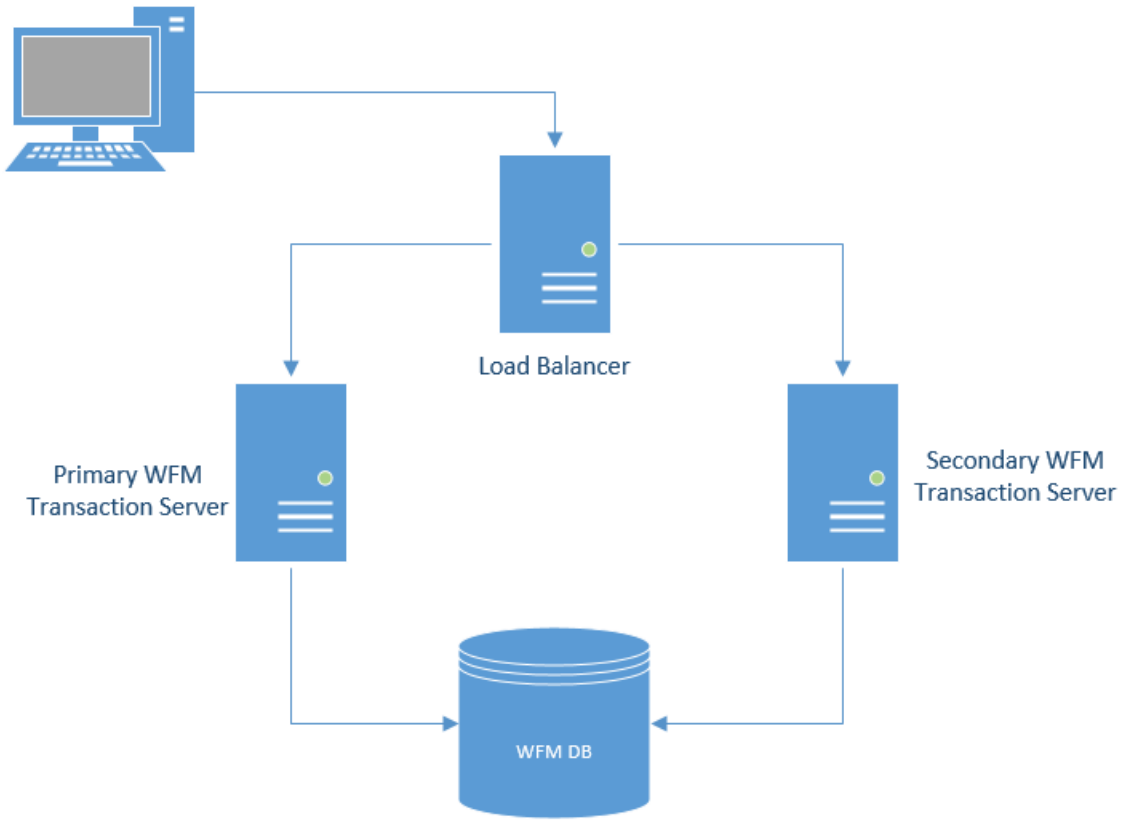
Installed Components	Comments
WFM iCalendar service	Install on a dedicated server located in your DMZ The “Use secure/encrypted connections” option on the WFM Configuration Setup Enterprise Settings step must be set the same as it is on the application/database server.



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
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:

- CTI server IP address and port number
- Cisco Unified CCX server IP address
  - Single node environment: use the primary server IP address
  - Web server redundancy (two node) environment: use the secondary server IP address

Note: The Cisco 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, set up a method 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 *Data Import 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 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 SQL Server Native Client* for more information.

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. **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 *Firewall Configuration Guide* for more information.

Setup window	Complete as follows
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.
Authentication Mode	Select Mixed Mode. Enter a password for the SQL Server Administrator (sa) logon.
Collation Settings	Under SQL Collations, select this option: Dictionary order, case-insensitive, for use with 1252 Character Set 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

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.

Note: 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 WFM Configuration Setup, 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.

The SQL Native Client installation file (sqlncli.msi) can also be downloaded from the Microsoft Download Center from these linked pages:

- SQL Server 2008: http://www.microsoft.com/en-us/-download/details.aspx?id=30440
- SQL Server 2012: http://www.microsoft.com/en-us/download/details.as-px?id=29065
- SQL Server 2014: http://www.microsoft.com/en-us/-download/details.aspx?id=42295

Expand the Install Instructions section on these pages and scroll down to locate the installation file for SQL Native Client.

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	REG_SZ	1
iCountry	REG_SZ	1
iCurrDigits	REG_SZ	2
iCurrency	REG_SZ	0
iDate	REG_SZ	0
iDigits	REG_SZ	2
iFirstDayOfWeek	REG_SZ	6
iFirstWeekOfYear	REG_SZ	0
iLZero	REG_SZ	1
iMeasure	REG_SZ	1
iNegCurr	REG_SZ	0
iNegNumber	REG_SZ	1
iTime	REG_SZ	0

Value	Type	Data
iTimePrefix	REG_SZ	0
iTLZero	REG_SZ	0
Locale	REG_SZ	00000409
NumShape	REG_SZ	1
s1159	REG_SZ	AM
s2359	REG_SZ	PM
sCountry	REG_SZ	United States
sCurrency	REG_SZ	$
sDate	REG_SZ	/
sDecimal	REG_SZ	.
sGrouping	REG_SZ	3;0
sLanguage	REG_SZ	ENU
sList	REG_SZ	,
sLongDate	REG_SZ	dddd, MMMM dd, yyyy
sMonDecimalSep	REG_SZ	.
sMonGrouping	REG_SZ	3;0
sMonThousandSep	REG_SZ	,
sNativeDigits	REG_SZ	0123456789
sNegativeSign	REG_SZ	-
sPositiveSign	REG_SZ	
sShortDate	REG_SZ	mm-dd-yyyy
sThousand	REG_SZ	,

Value	Type	Data
sTime	REG_SZ	;
sTimeFormat	REG_SZ	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 decribes how to install and upgrade WFM.

IMPORTANT: WFM must be installed from the CD or a local drive. Installation from a network drive is not supported.

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.

   Note: Security software (such as Cisco Security Agent) can have an adverse effect on the installation process and cause the installation to fail.

3. On the installation CD, double-click setup_WFM_<version>.exe to start the Installation Wizard.
4. Click Next to display the Select Destination Location window.
5. 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\).

6. Click Next to display the Select Components window.

7. Select the services or group of service you want to install on the server.
8. Click Next to continue. Follow the Installation Wizard prompts until the installation is finished.
9. After the installation is complete and the Installation Wizard closes, WFM Configuration Setup (Postinstall) starts. See *Configuring WFM* for instructions on how to configure the services you just installed.
10. After you have completed Postinstall, restart your security software (if present on the server).

Installing an Upgrade

WFM 11.0 supports upgrades from the following versions:

- WFM 10.0
- WFM 10.5

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

Upgrade paths to WFM 11.0

From version	Instructions
8.5(1), 8.5(2), 10.0, 10.5	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 *WFM Installation Guide* for version 8.5(2).

IMPORTANT: Over the top upgrades from version 10.5 and earlier to 11.0 are not supported. All such 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. Over the top upgrades from 11.0 to newer versions of 11.0 are supported.

Note: If you have a generic 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. Keep 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.

Upgrading from Version 10.5 or Earlier

Upgrades from WFM version 10.5 or earlier are manual upgrades.

Before you install a WFM upgrade from WFM 10.5 or earlier, do the following:

- Schedule the installation for a maintenance period when your WFM system is out of production, because installing a WFM upgrade requires bringing down the WFM system,
- 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. Settings in upgrades from 9.3 to newer versions are preserved so it is not necessary to make note of them.
- 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 an ET*. Removing a patch takes approximately 10 minutes, followed by a server reboot.

To upgrade from WFM 10.5 or earlier to WFM 11.0:

1. On the WFM server, log in as the local administrator.
2. Shut down any security software that might be running.

   Note: Security software (such as Cisco Security Agent) can have an adverse effect on the installation process and cause the installation to fail.

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_<version>.exe to start the installation Wizard.
6. Follow the instructions in the Installation 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 Postinstall has run completely.

Upgrading to a Newer Version of WFM 11.0

Upgrades from WFM 11.0 to a newer version of WFM 11.0 are over the top upgrades. Before you install this type of upgrade, do the following:

- Schedule the installation for a maintenance period when your WFM system is out of production, because installing a WFM upgrade requires bringing down the WFM system,
- Back up your SQL Server WFM database using SQL Server backup tools.
- Uninstall any existing ET.

To upgrade from WFM 11.0 to a newer version of WFM 11.0:

1. On the WFM server, log in as the local administrator.
2. Double-click setup_WFM_<version>.exe to start the Installation Wizard.
3. Follow the instructions in the Installation Wizard.
4. Configure WFM. For instructions, see *Configuring WFM*

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.

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).

Engineering Test	An ET is an additional installable component that contains the files needed to assist developers in diagnosing a problem. ETs are intended for limited scope tests.
Engineering Special	An ES is a version of the product that contains all fixes issued since the base release to the latest ES. Installing an ES replaces the existing installation.
Service Release	An SR is a version of the product that contains all fixes issued since the base release to the latest SR. Installing an SR replaces the existing installation.

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

- Schedule the installation for a maintenance period when your WFM system is out of production, because installing a WFM upgrade requires bringing down the WFM system,
- Back up the SQL Server WFM database using SQL Server backup tools.
- Uninstall any existing ET.

All patches are installed over the top of the existing installation. For instructions, see *Upgrading to a Newer Version of WFM 9.3*.

Repairing WFM

You can use the Repair function in the Windows Programs and Features utility in Control Panel on WFM to correct problems that might arise.

To repair WFM:

1. Log into the WFM server as the local machine administrator.
2. Start the Programs and Features utility in Control Panel.

   There can be up to three programs listed for WFM, depending on what you installed on the server:

   a. Cisco Unified Workforce Management Services Framework

   b. Cisco Unified Workforce Management Services

   c. Cisco Unified Workforce Management Jetty

   The repair function is available only for (b) and (c).

   Note: If you are not sure where the problem lies, run a repair on both programs.
3. Select the Jetty program and run a repair on it first.
4. Select the WFM Services program and run a repair on it.
5. When the repairs are completed, start Postinstall.
6. Complete Postinstall, providing any information that might not be

present. The repair function removes any changes that were made to the Windows Registry so you will have to enter some data to reconnect your WFM installation to the WFM database.

Note: If there was an ET installed before you repaired WFM, you must reinstall it after the repair is completed.

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 (base, upgrade, and patches) finishes. After you configure all of the required parameters, the WFM services start automatically and the system is ready for use.
- **Update Mode**. Whenever you start Postinstall manually, it starts in Update Mode. You start it manually 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.

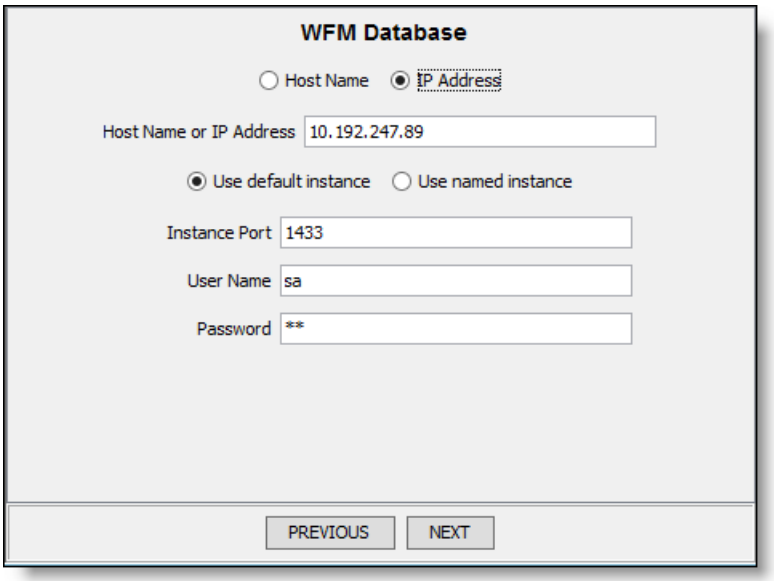
- *WFM Database Step*
- Create WFM DB (action only; this step creates the WFM database)
- *Data Retention Periods Step*
- *WFM Server Step*
- Update KeyStore (action only; this step updates the WFM keystore with the

webserver certificate used when accessing Unified Workforce Optimization via https)

- *ACD Connection Step*
- *QM Connection Step*
- *WFM Authentication Step*
- *Email Distribution Step*
- *Monitoring and Notification Step*
- Jetty Configuration (action only; this step configures Jetty)
- *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

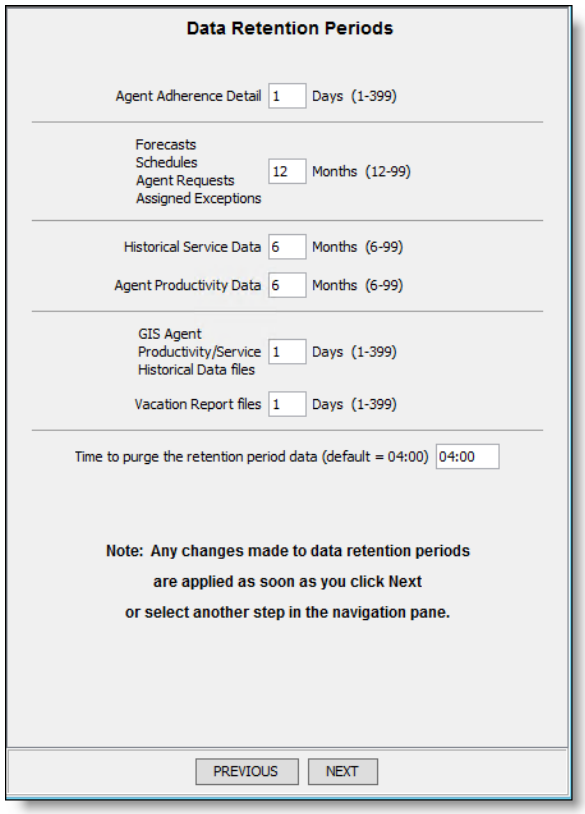
The WFM Database step configures access to the WFM database.



Field	Description
Host Name/IP Address	Select the server name format option.
Host Name or IP Address	The host name or IP address of the server that hosts the WFM database. **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.
Use default instance/ Use named instance	Select the type of database instance you are using for the WFM database. **Note**: You cannot change this setting in Update Mode. If the database instance name changes after WFM is configured, you must reinstall WFM.
Instance Port	The port used by the default database instance. This field appears only if you select the “Use default instance” option. The default port is 1433.
Instance Name	The name of the database named instance. This field appears only if you select the “Use named instance” option.
User Name	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 for WFM*). **Note**: The default language for this user must be set to US English.
Password	The SQL Server user's password.

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.



Field	Description
Agent Adherence Detail	Value from 1-399 days. Default = 15 days. Agent adherence detail information is the agent state data needed to calculate adherence. **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.
Forecasts Schedules Agent Requests Assigned Exceptions	Value from 12-99 months. Default = 13 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.

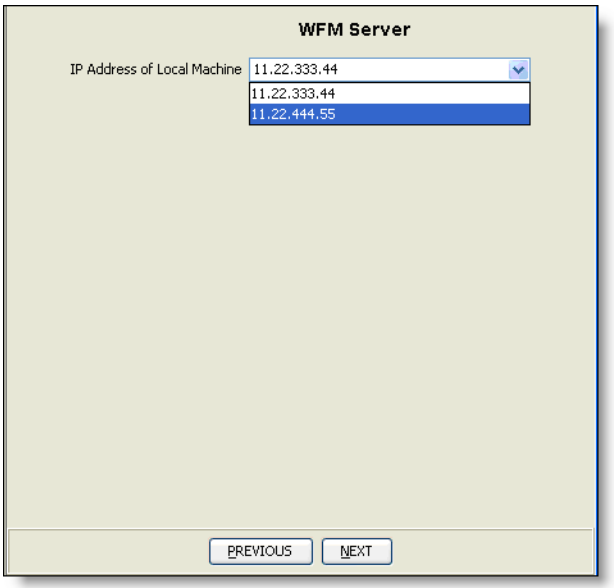
Field	Description
Time to purge the retention period data	Default = 04:00 (24-hour format) Set the time of day that data that is beyond the configured retention period is purged from the database.

- 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).

WFM Server Step

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

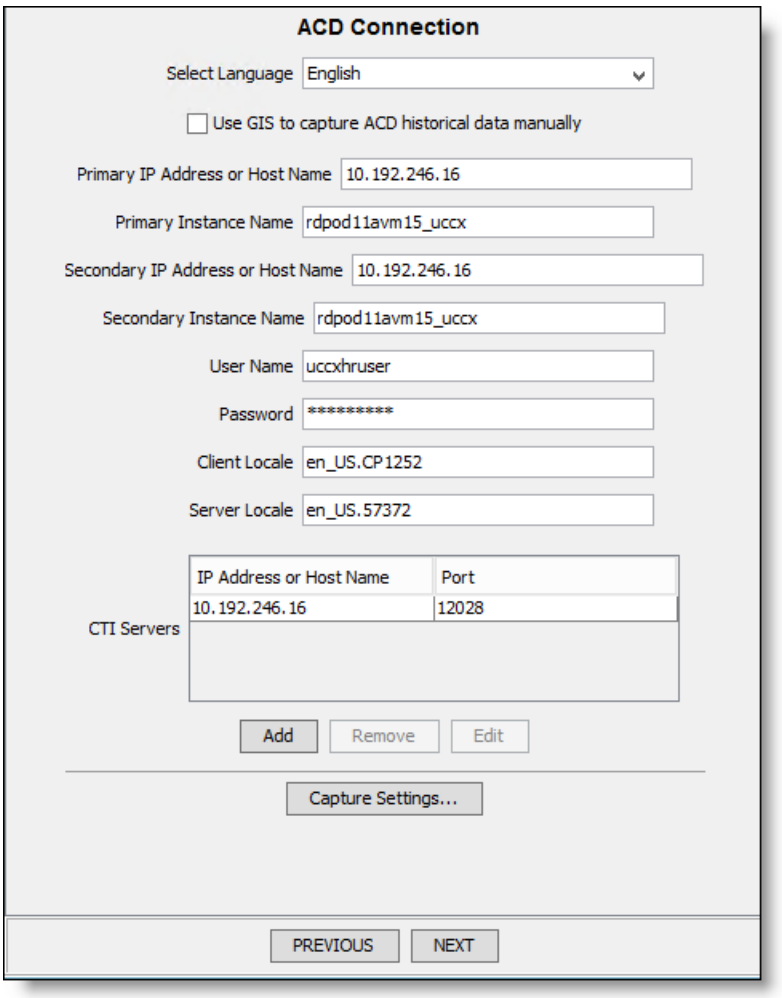
Select the public IP address used by clients to connect to the server from the drop-down list.



ACD Connection Step

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

Cisco Unified CCX ACD



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	The ACD's primary IP address or host name.

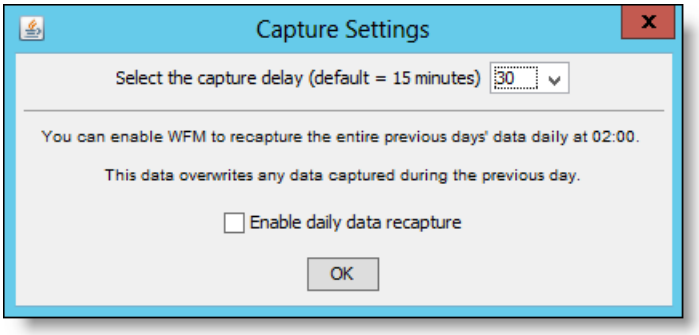
Field	Description
Primary Instance Name	Enter the primary Unified CCX database instance name. When entering the database instance name, use the following guidelines: ■ Convert all uppercase letters to lowercase letters ■ Replace all hyphens with underscores ■ If the host name starts with a number, add the prefix "i" ■ Append _uccx to complete the instance name **Example**: If your host name is 80-ABC, your instance name will be i80_abc_uccx.
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	The secondary Unified CCX database instance name. See Primary Instance Name for the format the instance name must be in.
User Name	The Unified CCX database user name.
Password	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 Servers	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.

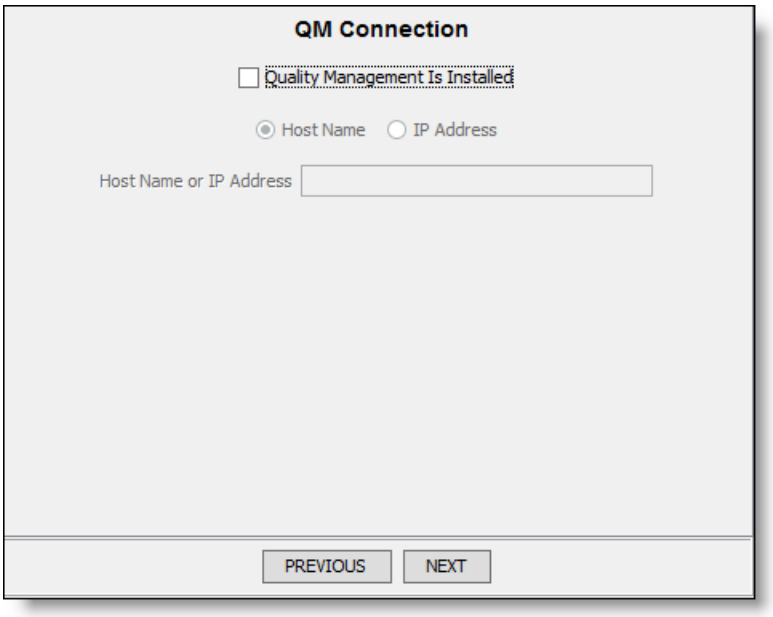
You can use the Capture Settings dialog box to change the capture settings to a value that works best with the length of calls handled by your contact center. You can select a capture delay between 15–135 minutes in 15-minute increments.



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.

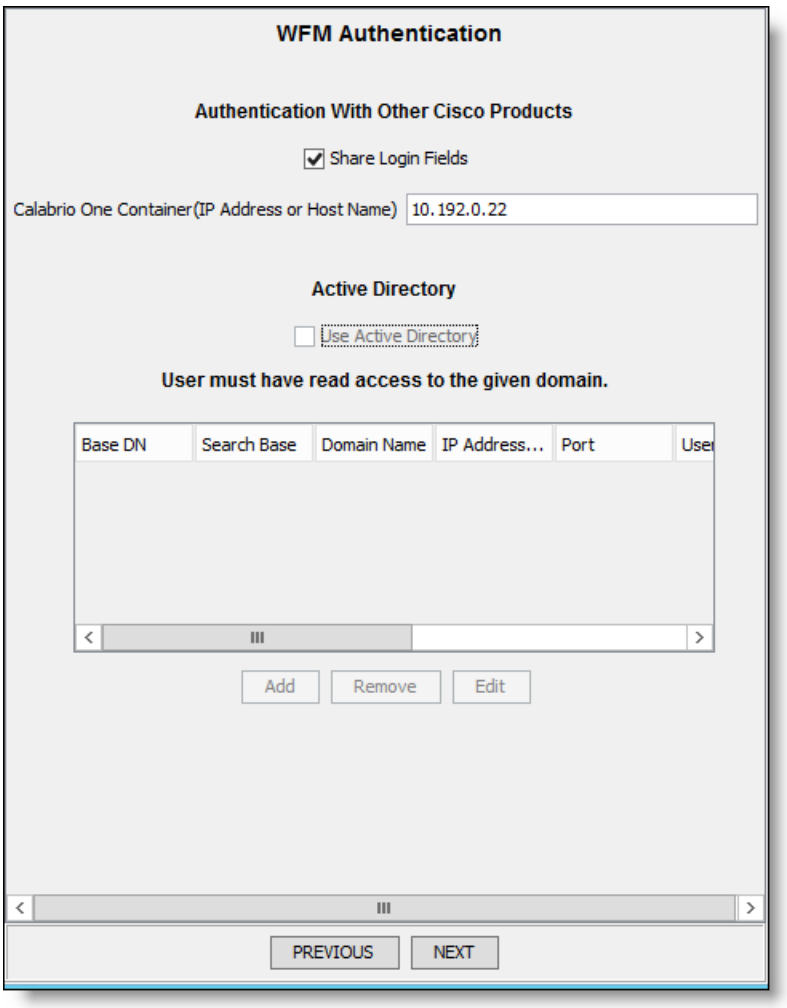


Field	Description
Quality Management is Installed	Select the check box if you are using Cisco Quality Management.
Host Name/IP Address	Select one option to indicate which format is used for the server name.
Host Name or IP Address	The host name or IP address of the Cisco Quality Management base services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



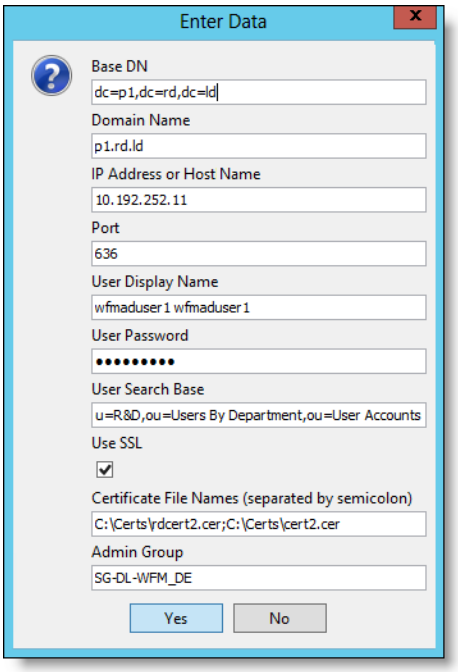
Field	Description
Share Login Fields	Select this check box if you want to share login fields in the Unified Workforce Optimization container with other Unified Workforce Optimization products.
Calabrio ONE Container (IP Address or Host Name)	The host name or IP address of the Unified Workforce Optimization 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	Select this check box if you will be using Active Directory with WFM. **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.

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 dialog box.



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	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. **Note**: The WFM Transaction services server must be able to access the Active Directory server for user authentication using this port number.
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	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
Use SSL	Select this check box if you want to use a Secure Socket Layer (SSL) for the Active Directory.
Certificate File Names	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. **Note**: Certificates must be base-64 encoded.

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.

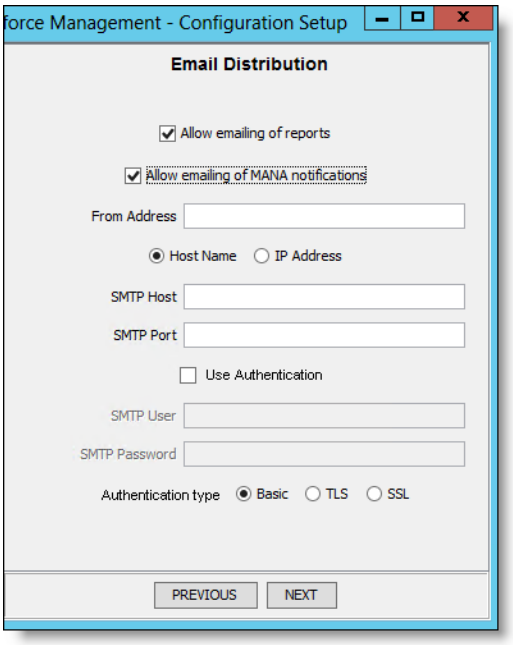
Managing Active Directory Domains

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.



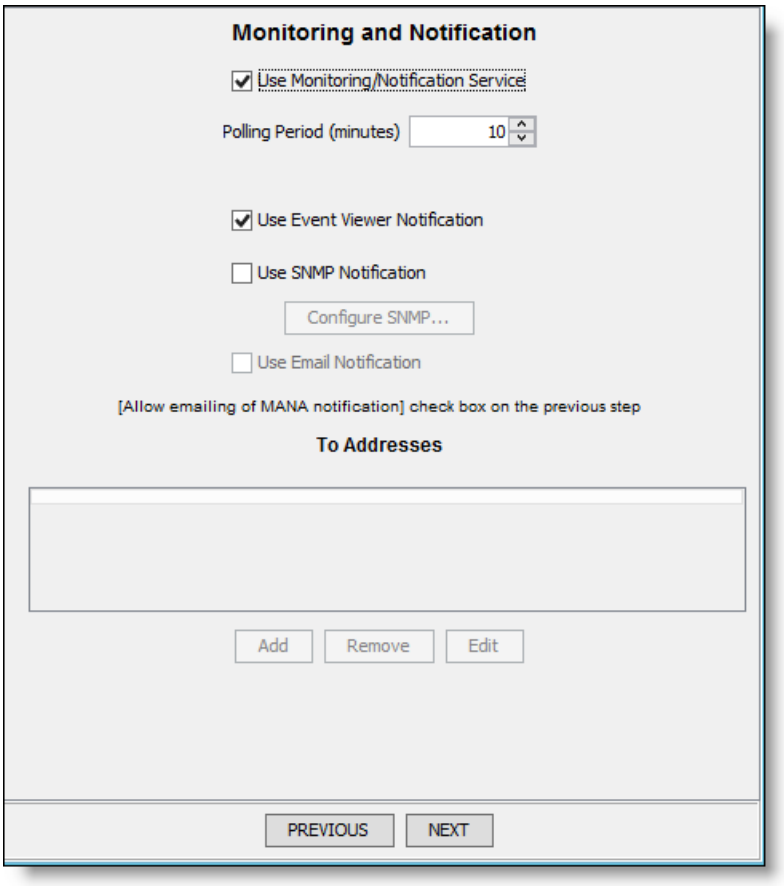
Field	Description
Allow emailing of reports	Select this check box to use email for sending out reports. If selected, the report setup pages in Unified Workforce Optimization display a section that enables the report user to configure the report to be sent to specified email addresses as an attachment.
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



Field	Description
Use Monitoring/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:

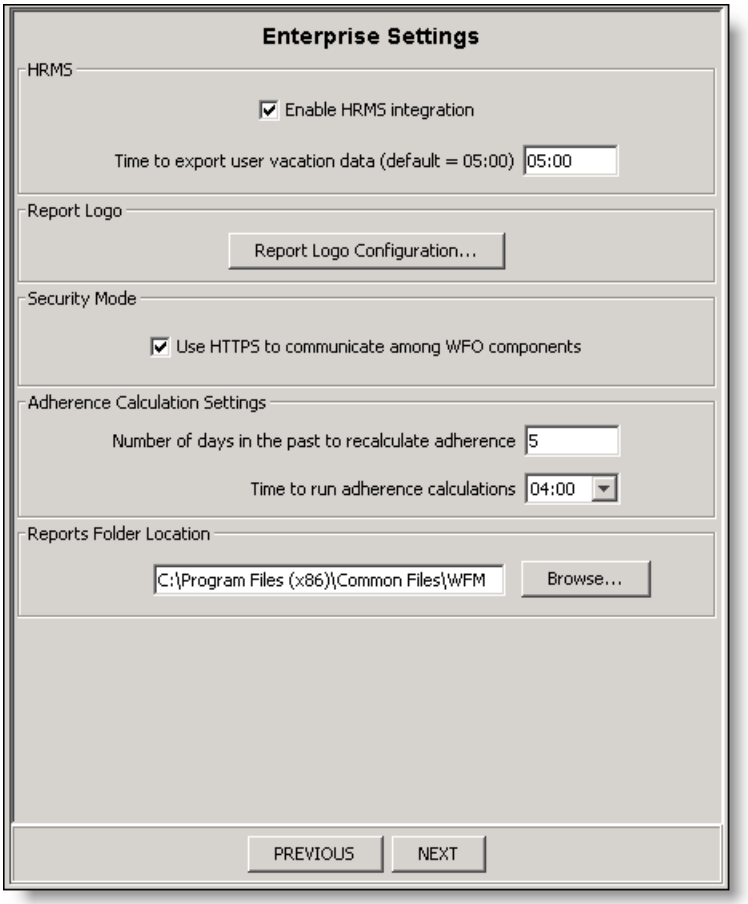
1. In the Monitoring and Notification step window, click Configure SNMP.
2. In the Configure SNMP dialog box, click Add, enter the IP address of the trap destination, and then click OK.
3. Restart the Windows SNMP service to enable the trap destination.

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

Enterprise Settings Step

The Enterprise Settings step is used to configure the following:

- HRMS integration
- The time when vacation data is exported
- Custom logo to be used on reports
- The use of a secure connection among WFO components
- Adherence calculation settings
- The location of the folder where GIS and HRMS files are placed for processing



Field	Description
Enable HRMS Integration	(Appears only in Advanced bundle installations) Select this check box to enable a connection between WFM and your HRMS (Human Resources Management System). For information on how WFM imports vacation data from your HRMS and exports data on vacation hours used to a file for use by your HRMS, see the *Historical and Real-Time Data Import Reference Guide*.
Time to export user vacation hours	(Appears only in Advanced bundle installations) Sets the time when the daily export of user vacation data from your HRMS to WFM occurs, in 24-hour format. Default = 05:00.
Report Logo Configuration	Click this button to add a custom logo to your WFM reports. See *Configuring the Report Logo* more information.
Use HTTPS to communicate among WFO components	Select this check box to force users to access WFM through a secure/encrypted connection (HTTPS).
Number of days in the past to recalculate adherence	The number of days into the past that the AAC service will perform adherence calculations. Default is 5 days, and valid entries are 1-90 days.
Time to run adherence calculations	The time of day you want adherence to be calculated. Default time is 04:00.
Reports Folder Location	(Appears only in WFM 9.3(1) SR1 and newer) The path to the location where you want GIS and HRMS report files to be stored and processed. The field is autofilled with the default path. See the *WFM Historical and Real-Time Data Import Reference Guide* for more information.

Configuring the Report Logo

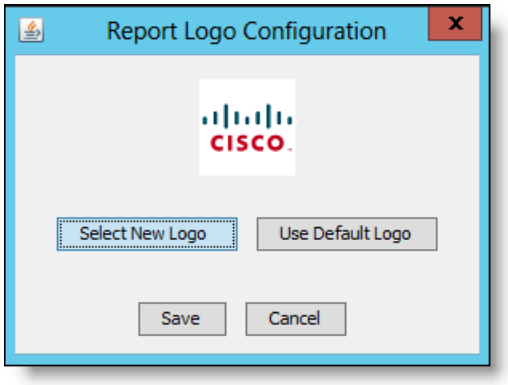
You can customize the logo that appears on WFM reports by replacing the default logo with one of your own.

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 C:\Program Files (x86)\Cisco\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. Refer to the *Workforce Optimization Suite Firewall Configuration Guide* for a list of all 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.

Managing Certificates

WFM supports HTTPS using a self-signed certificate. The self-signed certificate is sufficient to encrypt the communication path between the WFM server and client browsers. However, it has the following limitations:

- Agents see a certificate error or security alert the first time they access Unified Workforce Optimization.
- User security is not complete. Users are vulnerable to man-in-the-middle attacks (an active form of eavesdropping where private communication is controlled by a hacker).
- Errors appear when using HTTPS if you use WFO Finesse gadgets.

You can update the certificate so that users are not required to accept self-signed certificates. This prevents the possibility of man-in-the-middle attacks.

Note: For a deployment that includes multiple Unified Workforce Optimization products, if every user connects to Unified Workforce Optimization on the Cisco Quality Management base server, then you only need to update the certificate on that base server.

Updating the WFM Signed Certificate

Follow these steps to update the WFM signed certificate. In order to perform this procedure, you will need the following:

- The file keytool.exe, located in the …\WFO_WFM\Java\bin folder.
- A Certificate Authority (CA) from a commercial service such as Symantec VerifSign or GoDaddy, or a local CA such as Microsoft Active Directory Certificate Services (AD CS).

Step 1: Create the self-signed WFM certificate.

Run WFM Configuration Setup (Postinstall) on the WFM Transaction services server to completion. This automatically creates the WFM self-signed certificate.

Step 2: Create a certificate signing request (CSR) for the WFM Transaction services server.

From the command line on the WFM Transaction services server, enter the following command:

```
"C:\Program Files (x86)\Cisco\WFO_WFM\Java\bin\keytool.exe" -
keystore "C:\Program Files (x86)\Common
Files\WFM\config\.keystore" -storepass Sp@nl1nk -certreq -alias
wfm_webserver -file wfm_webserver.csr
```

This command generates a CSR (wfm_webserver.csr).

Step 3: Submit the CSR to your selected Certificate Authority.

The procedure for obtaining a signed WFM certificate from your Certificate Authority varies by vendor. Consult your chosen vendor's website for instructions for requesting a signed certificate.

Note: Your CA will return to you a signed WFM certificate, a root certificate, and possibly one or more intermediate certificates.

Step 4: Import the signed root certificate from the Certificate Authority into the WFM keystore.

1. From the command line on the WFM Transaction services server, enter the following command:

   ```
   "C:\Program Files (x86)\Cisco\WFO_WFM\Java\bin\keytool.exe"
   -keystore "C:\Program Files (x86)\Cisco\WFO_
   WFM\Java\lib\security\cacerts" -storepass changeit -list -v
   ```

   This command lists the existing root certificates that come bundled with WFM Java. If your Certificate Authority appears in the list, you do not have to proceed. If it is not in the list, continue to the next step.

2. Enter the following command:

   ```
   "C:\Program Files (x86)\Cisco\WFO_WFM\Java\bin\keytool.exe"
   -keystore "C:\Program Files (x86)\Common
   ```

```
Files\WFM\config\.keystore" -storepass Sp@nl1nk -import -
trustcacerts -alias <CA name> -file <CA name>.cer
```

where <CA name> is the certificate file name.

3. Click Yes when the following prompt appears:

   ```
   Trust this certificate?
   ```

   This prompt appears because the certificate is self-signed (the certificate is both the issuer and the owner) and the keytool cannot follow the chain back to the trusted root.

Step 5: Import the intermediate certificates from the Certificate Authority into the WFM keystore.

> **Note**: You can skip this step if the WFM certificate was signed by the root Certificate Authority. If the WFM certificate was signed by an intermediate Certificate Authority, then all intermediate certificates in the chain back to the root must be imported.

From the command line on the WFM Transaction services server, enter the following command:

```
"C:\Program Files (x86)\Cisco\WFO_WFM\Java\bin\keytool.exe" -
keystore "C:\Program Files (x86)\Common
Files\WFM\config\.keystore" -storepass Sp@nl1nk -import -
trustcacerts -alias <CA name> -file <CA name>.cer
```

where <CA name> is the certificate file name.

Step 6: Import the signed WFM certificate into the WFM keystore.

From the command line on the WFM Transaction services server, enter the following command:

```
"C:\Program Files (x86)\Cisco\WFO_WFM\Java\bin\keytool.exe" -
keystore "C:\Program Files (x86)\Common
Files\WFM\config\.keystore" -storepass Sp@nl1nk -import -alias
wfm_webserver -file wfm_webserver-cert-base64.cer
```

This command imports the signed WFM certificate wfm_webserver-cert-base64.cer into the WFM keystore.

Step 7: Restart the WFM Jetty service.

On the WFM Transaction services server, use the Windows Services utility in the Control Panel to restart the WFM Jetty service.

Step 8: Import the root and intermediate certificates into client web browsers.

This step is not necessary in the following situations:

- The WFM certificate was signed by a well-known Certificate Authority such as VeriSign or Thawte. most modern browsers come with the major commercial certificate authority root certificates alreayd installed. Lesser-known Certificate Authorities might not be installed.
- You are using Internet Explorer and an Active Directory Certificate Authority where the WFM Transaction services server and clients are all in the same Active Directory domain.

To determine if you need to perform this step, start the client web browser and try to access Unified Workforce Optimization using the following URL:

`https://<WFM server>/cwfo`

Where <WFM server> is the host name or IP address of the WFM Transaction services server.

- If you can connect without errors or requests to install certificates, you do not have to perform this step.
- If you see a message indicating that the issuer of the certificate is not trusted, you must perform this step.

Best Practices. Chrome provides more descriptive error messages when updating certificates. Use Chrome to troubleshoot certificate errors.

For more information about installing root and intermediate certificates on a client desktop, see *Installing Root and Intermediate Certificates on Client Desktops*.

Certificates and Active Directory

You can generate a signed WFM certificate using Active Directory Certificate Services (AD CS). AD CS is a Certificate Authority.

Generating Certificates with Active Directory

Follow these steps to generate certificates using Active Directory Certificate Services (AD CS).

Step 1: Download the root certificate.

1. Log in to the Active Directory server for the root AD CS.
2. Start Internet Explorer and enter the following URL:

   `http://<myRoot>/certsrv`

   where <myRoot> is the root domain's IP address or host name. The AD CS for this domain is the root for this network.
3. Click Download a CA certificate, certificate chain, or CRL.
4. Select Base 64 for Encoding method.
5. Click Download CA certificate and specify a descriptive name for the root certificate.

   Example. `<myRoot>_root_x509.cer`

   See the Microsoft Knowledge Base article 555252, "How to export Root Certification Authority Certificate" for more information.

Step 2: Download the intermediate certificates.

Perform this procedure for each intermediate certificate.

1. Log into the Active Directory server for the intermediate AD CS.
2. Start Internet Explorer and enter the following URL:

   `http://<myIntermediate>/certsrv`

where <myIntermediate> is the intermediate domain IP address or host name. This is the domain where the WFM Transaction service server resides.

3. Click Download a CA certificate, certificate chain, or CRL.
4. Select Base 64 for Encoding method.
5. Click Download CA certificate and specify a descriptive file name for the intermediate certificate.

   Example. `<myIntermediate>_intermediate-cert_x509.cer`

Step 3: Create the self-signed WFM certificate.

Run WFM Configuration Setup (postinstall.exe) on the WFM Transaction services server to completion. This automatically creates the WFM self-signed certificate.

Step 4: Create a Certificate Signing Request (CSR) for the WFM Transaction services server.

From the command line on the WFM Transaction services server, enter one of the following commands:

If users access Unified Workforce Optimization using only an IP address:

```
"C:\Program Files (x86)\Cisco\WFO_WFM\Java\bin\keytool.exe" -keystore "C:\Program Files (x86)\Common Files\WFM\config\.keystore" -storepass Sp@nl1nk -certreq -alias wfm_webserver -file wfm_webserver.csr
```

If users access Unified Workforce Optimization using and IP address and host name/DNS:

```
"C:\Program Files (x86)\Cisco\WFO_WFM\Java\bin\keytool.exe" -keystore "C:\Program Files (x86)\Common Files\WFM\config\.keystore" -storepass Sp@nl1nk -certreq -alias wfm_webserver -file wfm_webserver.csr -ext san=dns:<DNS>,ip:<IP address>
```

where <DNS> is the host name or DNS in the Unified Workforce Optimization URL and <IP address> is the IP address in the Unified Workforce Optimization URL.

This command generates a CSR (wfm_webserver.csr).

Step 5: Use the CSR to create a signed WFM certificate.

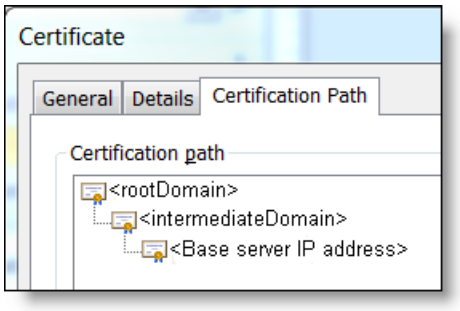
1. Log in to the Active Directory server for the intermediate AD CS.
2. Start Internet Explorer and enter the following URL:

   `http://<myIntermediate>/certsrv`

   where <myIntermediate> is the intermediate domain IP address or host name. This is the domain where the WFM Transaction service server resides.
3. Click Request a certificate.

   Note: On some Certificate Authority servers you might get an additional page where you must click Advanced Certificate Request.
4. Click Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
5. Paste the contents of the CSR that you created earlier (wfm_web-server.csr) into the Saved Request field.
6. Select the Web Server in Certificate Template field.
7. Click Submit.
8. Select Base 64 Encoded and click Download certificate.
9. When prompted, enter a descriptive file name for the certificate.

   Example. `wfm_webserver-cert-base64.cer`
10. Double-click the certificate file, select the Certification Path tab, and verify that the certification path is correct. It should include the IP address of the WFM Transaction services server and the chain of certificates back to the root CA (see graphic).



If the certification path is not correct, download the root and intermediate certificates again from the correct AD CS domains.

Note: The self-signed WFM certificate was created to be valid for 100 years from its creation date, but when the Certificate Authority signs it, that valid period is typically reduced to 1–5 years. Check the Valid From and Valid To fields in the certificate for the certificate's valid period.

Note: The WFM Transaction services server's IP address must be used in the Unified Workforce Optimization secure URL rather than the server's host name, since the IP address is in the Subject/Owner field in the signed WFM certificate. Using the host name will result in a certificate error or security alert the first time the URL is accessed.

Step 6: Import the root certificate into the WFM keystore.

1. From the command line on the WFM Transaction services server, enter the following command:

   ```
   "C:\Program Files (x86)\Cisco\WFO_WFM\Java\bin\keytool.exe"
   -keystore "C:\Program Files (x86)\Cisco\WFO_
   WFM\Java\lib\security\cacerts" -storepass changeit -list -v
   ```

   This command lists the existing root certificates that come bundled with WFM Java. If your Certificate Authority appears in the list, you do not have to proceed. If it is not in the list, continue to the next step.

2. Enter the following command:

   ```
   "C:\Program Files (x86)\Cisco\WFO_WFM\Java\bin\keytool.exe"
   -keystore "C:\Program Files (x86)\Common
   Files\WFM\config\.keystore" -storepass Sp@nl1nk -import -
   trustcacerts -alias <CA name> -file <CA name>.cer
   ```

   where <CA name> is the certificate file name.

3. Click Yes when the following prompt appears:

   ```
   Trust this certificate?
   ```

   This prompt appears because the certificate is self-signed (the certificate is both the issuer and the owner) and the keytool cannot follow the chain back to the trusted root.

Step 7: Import the intermediate certificates into the WFM keystore.

Note: You can skip this step if the WFM certificate was signed by the root Certificate Authority. If the WFM certificate was signed by an intermediate Certificate Authority, then all intermediate certificates in the chain back to the root must be imported.

From the command line on the WFM Transaction services server, enter the following command:

```
"C:\Program Files (x86)\Cisco\WFO_WFM\Java\bin\keytool.exe" -
keystore "C:\Program Files (x86)\Common
Files\WFM\config\.keystore" -storepass Sp@nl1nk -import -
trustcacerts -alias <CA name> -file <CA name>.cer
```

where <CA name> is the certificate file name.

Step 8: Import the signed WFM certificate into the WFM keystore.

From the command line on the WFM Transaction services server, enter the following command:

```
"C:\Program Files (x86)\Cisco\WFO_WFM\Java\bin\keytool.exe" -
keystore "C:\Program Files (x86)\Common
Files\WFM\config\.keystore" -storepass Sp@nl1nk -import -alias
wfm_webserver -file wfm_webserver-cert-base64.cer
```

This command imports the signed WFM certificate wfm_webserver-cert-base64.cer into the WFM keystore.

Step 9: Restart the WFM Jetty service.

On the WFM Transaction services server, use the Windows Services utility in the Control Panel to restart the WFM Jetty service.

Step 10: Import the root and intermediate certificates into client web browsers.

This step is not necessary in the following situations:

- The WFM certificate was signed by a well-known Certificate Authority such as VeriSign or Thawte. Most modern browsers come with the major commercial certificate authority root certificates alreayd installed. Lesser-known Certificate Authorities might not be installed.
- You are using Internet Explorer and an Active Directory Certificate Authority where the WFM Transaction services server and clients are all in the same Active Directory domain.

To determine if you need to perform this step, start the client web browser and try to access Unified Workforce Optimization using the following URL:

`https://<WFM server>/cwfo`

Where <WFM server> is the host name or IP address of the WFM Transaction services server.

- If you can connect without errors or requests to install certificates, you do not have to perform this step.
- If you see a message indicating that the issuer of the certificate is not trusted, you must perform this step.

Best Practices. Chrome provides more descriptive error messages when updating certificates. Use Chrome to troubleshoot certificate errors.

See *Installing Root and Intermediate Certificates on Client Desktops* for more information.

Installing Root and Intermediate Certificates on Client Desktops

To install the root and any intermediate certificates on a client desktop:

1. Copy the root and any intermediate certificates to any location on the client desktop.

   > **Note**: The root certificate must be installed first, and after that any intermediate certificates. Follow these steps for each certificate you want to install.

2. Double-click the certificate to open the Certificate dialog box.
3. On the General tab, click Install Certificate to start the Certificate Import wizard.
4. Select the Place all certificates in the following store option and click Browse to select a certificate store.
   - For the root certificate, choose the Trusted Root Certificate Authorities store
   - For any intermediate certificates, choose the Intermediate Certificate Authorities store
5. Click Next and then Finish. When asked if you want to install the certificate, click Yes.
6. Click OK after the certificate is installed.

To verify that the certificates were installed correctly:

Open Internet Explorer and enter the following URL:

`https://<WFM server>/cwfo`

Where <WFM server> is the URL of the WFM Transaction services server. If the certificates are correctly installed you should not see any security warnings.

Removing WFM

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

1. Uninstall any ET present.
2. Uninstall the WFM services.

Removing an ET

Follow these steps to remove a Workforce Management ET from a WFM server. When the ET 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 ET:

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 ET, click Uninstall and follow the prompts.

Removing WFM Services

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

To remove WFM services:

1. Log into the WFM server as the local machine administrator.
2. Start the Programs and Features utility in Control Panel.

   There can be up to three programs listed for WFM, depending on what you installed on the server:

   a. Cisco Unified Workforce Management Services Framework
   b. Cisco Unified Workforce Management Services
   c. Cisco Unified Workforce Management Jetty

   If you choose (a) for removal, (b) and, if present, (c) are also removed. If you choose either (b) or (c) for removal, only that program is removed.
3. Click Uninstall, and follow the prompts.
4. After the uninstall is completed, you are prompted to reboot. You are given the option to reboot now or later. It is recommended that you reboot immediately to complete the uninstallation process.