



Cisco Unified Workforce Optimization

Workforce Management Installation Guide Release 11.5

First Published: July 28, 2016

Last Updated: March 6, 2020

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

© 2016, 2017, 2018, 2019, 2020 Cisco Systems, Inc. All rights reserved.

Contents

Overview	7
What's New in This Release	7
WFM Documentation	10
Workforce Management Services	11
Port Usage	12
WFM Jetty Service Ports	13
System Requirements	15
Environment	15
WFM Server Hardware Requirements	15
HDD Partitioning	16
Deployment Capacity and Sizing	17
Memory Recommendations	17
Single Server Deployment Models	18
Single Server 100/300 Sizing	19
Single Server with Offboard SQL Server 200/600 Sizing	20
Single Server with Offboard SQL Server 400/1200 Sizing	21
Single Server with Offboard SQL Server 800/2400 Sizing	22
Approximating Additional Storage Requirements	23
Agent Adherence Detail Data	23
WFM in a Cisco UCS Environment	23
Server Operating System Requirements	24
Virtual Server Environment	24
Desktop Requirements	24
Third Party Software Requirements	24
Browser Requirements	25
Configuration Data Requirements	25
Before You Install WFM	27

Prerequisites	27
Active Directory	27
Cisco Unified Contact Center Express	27
GIS API	27
SMTP	28
SNMP	28
WFM	28
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	32
Installing WFM	35
Recommended Installation Paths	35
Order of Installation	35
Single Server/Onboard SQL Server Deployment	35
Single Server/Offboard SQL Server Deployment	36
SQL Server Considerations	37
SQL Server Clustering	37
Concurrent SQL Server Versions	37
Time Zone, Date, and Time	37
Installing a Base Release	38
Installing an Upgrade	39
Upgrading Systems with Pending Capture Requests	40
Installing an Update	41
Installing the Unified Workforce Optimization Notification Client	41
Manual Installation	42

Elevating User Privileges	43
Automated Installation	43
Requirements	43
Recommended Deployment Preparation Model	44
Configuring the Notification Client Installation File	44
Repairing WFM	45
SNMP Integration	47
Definitions	47
SNMP Implementation	47
MIBs	48
Using MIBs	48
Generic Trap	48
Configuring WFM	51
WFM Database Step	52
Data Retention Periods Step	53
WFM Transaction Server Step	57
ACD Connection Step	57
Cisco Unified CCX ACD	58
Capture Settings	60
QM Connection Step	61
WFM Authentication Step	61
Configuring Active Directory Domains	63
Managing Active Directory Domains	65
Email Distribution Step	65
Monitoring and Notification Step	67
Configuring SNMP Notification	68
Enterprise Settings Step	69
Configuring the Report Logo	71

Verifying the Connection to the Unified CCX Database	72
Configuring the iCalendar Service	73
Capturing Historical Data	75
Capturing Cisco Unified CCX Historical Data	75
Managing Certificates	77
Updating the WFM Signed Certificate	77
Generating Certificates with Active Directory	80
Installing Root and Intermediate Certificates on Client Desktops	86
Removing WFM	87
Removing an ET	87
Removing WFM Services	87

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 Release

WFM 11.5 includes the following new features:

WFM 11.5(1)

- Intraday Dynamic Scheduling feature
- Workflows feature

- Audit Trail report
- Support for Cisco Unified Contact Center Express Release 11.0 and 11.5
- Support for Windows 10
- Reporting functionality for non-interactive service queues
- Option to capture real-time data for non-interactive service queues via native support or through GIS
- Notifications page enables you to configure the types of alert notifications sent to users
- Import and Export page enables you to import and export user, agent, and team data
- WFO alerts and notifications now delivered via the Windows system tray and toaster popups
- Ability to configure minimum/maximum hours per agent
- Dynamic Availability feature
- Range-based work conditions
- Partial day schedule trades and offers
- Ability to restrict agents from viewing other agents' schedules
- Ability to customize a supervisor's ability to edit agent schedules either individually or by group
- Ability to customize when agents can view specified weeks in future schedules
- Ability to optimize lunches and breaks by service queue for better coverage
- Redesigned Dynamic Scheduling Events feature
- Added paging to the Agent Schedules page to make navigating a long list of agents easier
- Added Calls Offered field to the View and Edit Historical Data page
- Added coverage information for non-interactive service queues in the Schedule, Reforecast, and Intraday Data coverage drawers on the Agent Schedules page
- Strategic Forecasts features has been moved to the Planning application, and new metrics have been added to strategic forecasts
- New alert types have been added: agent notifications for schedule changes, schedule reminders, and request status changes
- Forecast editing functionality has been expanded to allow users to make edits at the daily, weekly, and monthly total levels

- MANA reporting for the WFM RTE service has been enhanced to report ACD and WFM database connection issues
- All WFM services except for the WFM RTE service have been converted to 64-bit
- Increased data retention times
- Real Time Adherence enhancements
- Vacation Plan enhancements
 - Custom date ranges for vacation plans
 - Assign multiple plans to a single agent
 - Customize/add new vacation types
 - Add up to 20 vacation types to a vacation plan
- Work condition enhancements:
 - Create and assign work condition profiles to agents for simplified management of work conditions
 - Work conditions can be either of two types: Shift Length work conditions or Paid Hours work conditions
- Removed support for Unified CCX 8.5
- Bug fixes

WFM 11.5(1) SR5

- WFM authentication can now use OpenLDAP (Lightweight Directory Access Protocol) to bind with standard LDAP servers and query for users. Full user management functionality may be limited by your LDAP directory architecture.
- Allow the option of not automatically associating all new agents to the NewAgent team. If turned off, new agents are associated with their ACD team, which is configured as the agent's main team. If turned on, new agents are synced with both the NewAgent and Main teams.
- Global WFM setting enhancements:
 - Assign workflow administrators to modify workflow, vacation type, and exception type settings. While workflow administrators are working in workflows, vacation types, or exception types, they have Enterprise View permissions.

- Users who have been assigned the Enterprise View can continue to manage workflows, vacation types, and exception types.
- Set the rate at which real time adherence metrics are refreshed on the screen.
- Workforce Management user interface is localized in Danish, Dutch (Standard), German, English (US), French (European), French (Canadian), Italian, Portuguese (Brazil), Spanish (International/Neutral), and Swedish.
- Bug fixes.

WFM 11.5(1) SR6

- Support for Cisco Unified Contact Center Express Release 11.6
- Added the ability to select the preferred method of generating variable schedules for agents who have assigned exceptions. You can opt to avoid assigned exceptions in order to maximize coverage, or include assigned exceptions (which might be for required events like team meetings) but that might result in insufficient coverage.,
- Added mobile device support for agents. Agents can now access My Schedule and Messaging on smart phones and tablets.
- Bug fixes.

WFM 9.5(1) SR7

- 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*
- *Unified Workforce Optimization End User Software License Agreement*
- *Unified Workforce Optimization 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.

Service	Description
WFM 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.
WFM 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.
WFM 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.
WFM Forecast Service	The WFM Forecast service generates distributions, forecasts, and strategic forecasts.
WFM Jetty Service	The Jetty service is a web server that supports the Unified Workforce Optimization user interface.
WFM 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 administrators through the Windows Event Viewer, Windows SNMP (Simple Network Management Protocol), or email.
WFM Product Adapter Service	The WFM Product Adapter service is the conduit through which application data is read from and written to the WFM database.
WFM 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).
WFM Request Service	The WFM Request service processes shift budget analysis requests.
WFM Schedule Service	The WFM Schedule service manages schedule requests.

Service	Description
WFM Sync Service	The WFM Sync service connects to a Cisco database using the SQL connection. The Sync service retrieves and processes configuration data for agents, users, service queues, and other entities.

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 (Unified CCX only) 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 <i>Cisco Customer Response Solutions Administration Guide</i> .	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.

Environment

WFM 11.5 is compatible with Quality Management 11.5.

WFM 11.5 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
- Cisco Unified Contact Center Express Release 11.0
- Cisco Unified Contact Center Express Release 11.5
- Cisco Unified Contact Center Express Release 11.6
- Cisco Unified Contact Center Express Release 12.0

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.

Element	Minimum Hardware Requirement
Processor	Intel: Xeon processor E3 family or higher, running above 2 GHz with hyperthreading enabled (required) AMD: Opteron processor 3000 or higher

Element	Minimum Hardware Requirement
Processor cores	4 (small server) 6 (medium server) 8 (large server)
VMWare processor cores	6 (small server) 8 (medium server) 16 (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 Deployment Capacity and Sizing
	Database partition (SQL Server database and log files)	See Deployment Capacity and Sizing

Server	Hard Disk Partition	Size
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 Deployment Capacity and Sizing

Deployment Capacity and Sizing

Use the information below 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.

Note: In a virtual environment, all servers must have dedicated resources that match the sizing specifications described in this section.

Memory Recommendations

There is a table of memory recommendations for each deployment model. Memory settings are configured in the service's properties file. These files can be located in this folder (default location):

```
C:\Program Files\cisco\WFO_WFM\config\
```

For example, to change the maximum memory setting for the WFM Capture service from 512MB to 256 MB, open the wfmcapture.properties file in a text editor and locate this line. The text that needs to be changed is highlighted in bold red:

```
service4j.jvmOptions=-
Dsplk4j.configuration=../config/wfmcapture.properties | -
Dcom.cisco.wfm.basePath=.. | -Xmx512M | -Xrs | -
Djava.library.path=..\bin
```

Change the highlighted text to:

```
service4j.jvmOptions=-
Dsplk4j.configuration=../config/wfmcapture.properties | -
Dcom.cisco.wfm.basePath=.. | -Xmx256M | -Xrs | -
Djava.library.path=..\bin
```

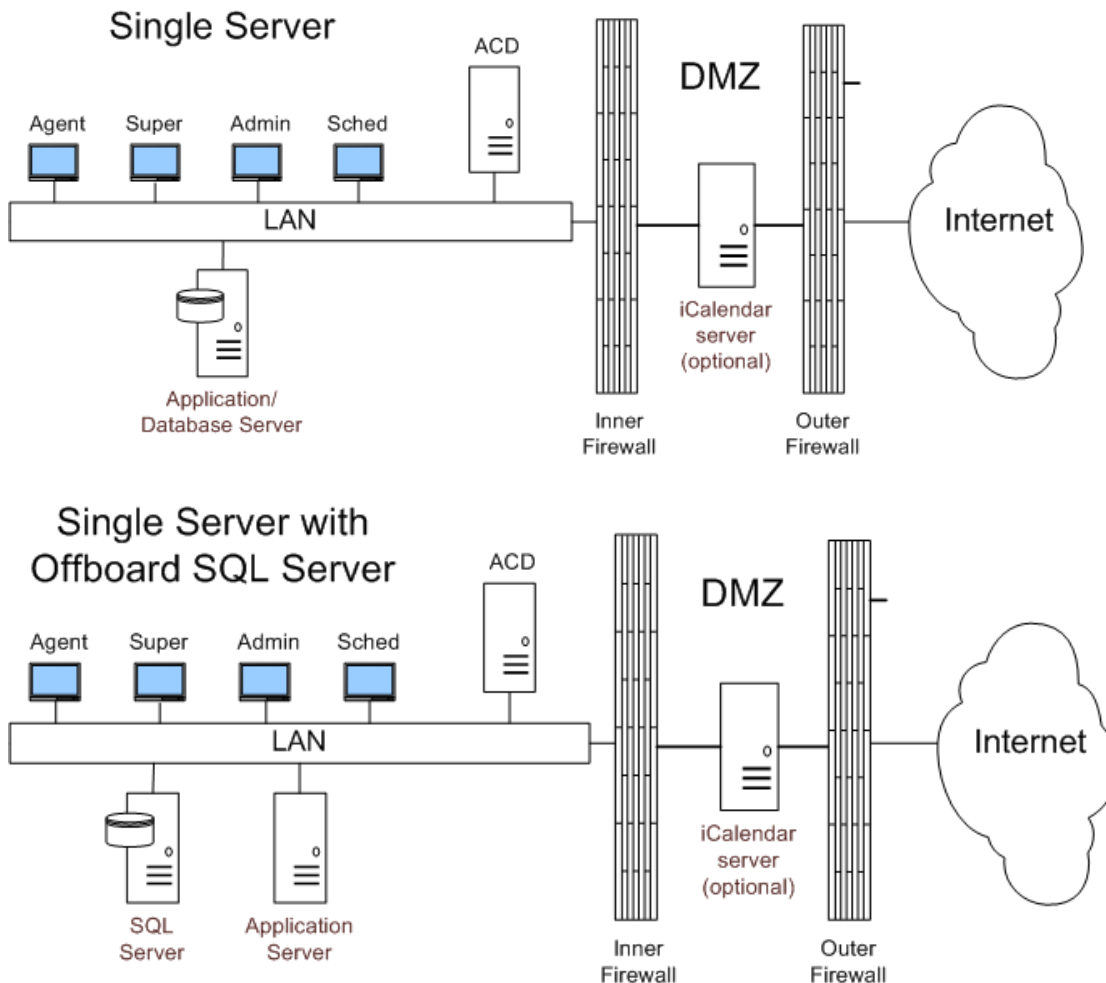
Single Server Deployment Models

This deployment has one ACD cluster with all WFM services and SQL Server located on one server.

The single server deployment can also be configured to have an offboard SQL Server. This deployment has one ACD cluster with a WFM application server and an offboard SQL Server.

All single server deployments include the following optional servers:

- 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.



Single Server 100/300 Sizing

- 100 peak concurrent users
- 300 maximum configured users

Server	Type	Installed Components
Server 1	Small	SQL Server WFM Transaction Services WFM Capture Services WFM Compile Services WFM Process Services
Server 2 (optional)	Small	WFM iCalendar Services

Memory Recommendations

Service	Minimum		Maximum	
	Default	Recommended	Default	Recommended
SQL Server	N/A	N/A	None	1 GB
ACC	None	None	256 MB	256 MB
Product Adapter	1024 MB	None	1024 MB	1 GB
Capture	None	None	512 MB	256 MB
Compile	None	None	256 MB	256 MB
Forecast	None	None	512 MB	256 MB
Jetty	None	None	512 MB	512 MB
Request	None	None	256 MB	256 MB
RTE	None	None	512 MB	256 MB
Schedule	1024 MB	None	4 GB	512 MB
Sync	None	None	512 MB	256 MB

Single Server with Offboard SQL Server 200/600 Sizing

- 200 peak concurrent users
- 600 maximum configured users

Server	Type	Installed Components
Server 1	Medium	WFM Transaction Services WFM Capture Services WFM Compile Services WFM Process Services
Server 2	Small	SQL Server
Server 3 (optional)	Small	SQL Server Reporting Services
Server 4 (optional)	Small	WFM iCalendar Services

Memory Recommendations

Service	Minimum		Maximum	
	Default	Recommended	Default	Recommended
SQL Server	N/A	N/A	None	2 GB
ACC	None	None	256 MB	256 MB
Product Adapter	1024 MB	None	1024 MB	2 GB
Capture	None	None	512 MB	256 MB
Compile	None	None	256 MB	256 MB
Forecast	None	None	512 MB	256 MB
Jetty	None	None	512 MB	512 MB
Request	None	None	256 MB	256 MB
RTE	None	None	512 MB	256 MB
Schedule	1024 MB	None	4 GB	512 MB
Sync	None	None	512 MB	256 MB

Single Server with Offboard SQL Server 400/1200 Sizing

- 400 peak concurrent users
- 1200 maximum configured users

Server	Type	Installed Components
Server 1	Large	WFM Transaction Services WFM Capture Services WFM Compile Services WFM Process Services
Server 2	Medium	SQL Server
Server 2 (optional)	Small	WFM iCalendar Services

Memory Recommendations

Service	Minimum		Maximum	
	Default	Recommended	Default	Recommended
SQL Server	N/A	N/A	None	4 GB
ACC	None	None	256 MB	256 MB
Product Adapter	1024 MB	None	1024 MB	4 GB
Capture	None	None	512 MB	256 MB
Compile	None	None	256 MB	256 MB
Forecast	None	None	512 MB	256 MB
Jetty	None	None	512 MB	1 GB
Request	None	None	256 MB	256 MB
RTE	None	None	512 MB	256 MB
Schedule	1024 MB	None	4 GB	1 GB
Sync	None	None	512 MB	256 MB

Single Server with Offboard SQL Server 800/2400 Sizing

- 800 peak concurrent users
- 2400 maximum configured users

Server	Type	Installed Components
Server 1	Large	WFM Transaction Services WFM Capture Services WFM Compile Services WFM Process Services
Server 2	Large	SQL Server
Server 3 (optional)	Small	WFM iCalendar Services

Memory Recommendations

Service	Minimum		Maximum	
	Default	Recommended	Default	Recommended
SQL Server	N/A	N/A	None	6 GB
ACC	None	None	256 MB	256 MB
Product Adapter	1024 MB	None	1024 MB	6 GB
Capture	None	None	512 MB	1 GB
Compile	None	None	256 MB	512 MB
Forecast	None	None	512 MB	512 MB
Jetty	None	None	512 MB	2 GB
Request	None	None	256 MB	256 MB
RTE	None	None	512 MB	256 MB
Schedule	1024 MB	None	4 GB	2 GB
Sync	None	None	512 MB	512 MB

Approximating Additional Storage Requirements

Considering the following details when determining database storage requirements.

Agent Adherence Detail Data

In addition to application and system data, The WFM database stores agent adherence detail data which includes every phone state an agent enters for every day. The total database storage T required to store this data can be approximated as:

$$T = A \times C \times S \times D \times 200 \text{ bytes}$$

Where:

- A = Average agents per day
- C = Average calls per agent per day
- S = Average state changes per contact per day
- D = Number of days to retain agent adherence detail data

And 200 bytes is the average space consumed by a single agent state change.

Example: For a call center with 1000 agents, 20 calls per agent per day, 5 state changes per contact per day, and an agent adherence data retention period of 365 days, then the total storage space T is approximately:

$$1000 \times 20 \times 5 \times 365 \times 200 \text{ bytes} = 7.3 \text{ GB}$$

Note: The WFM server also stores other items including historical data, schedule data, productivity data, and user requests. The retention periods for these items is configured post-install. See [Data Retention Periods Step](#) for more information.

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:

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-work-force-optimization-suite.html

Server Operating System Requirements

The supported operating systems for WFM servers are the following:

- 64-bit Windows Server 2016
- 64-bit Windows Server 2012 R2
- 64-bit Windows Server 2012
- 64-bit Windows Server 2008 R2

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.

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 ESXi 5.0, 5.1, 5.5, 6.0, and 6.5

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

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
- (optional) Microsoft SQL Server Reporting Services 2012 and 2014

- Microsoft Exchange 2007, 2010, 2013, and Office 365
- 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
- Google Chrome

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\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.

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

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, 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 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.

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.
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.aspx?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
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	,

Value	Type	Data
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	,
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 [Port Usage](#) 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.

Recommended Installation Paths

The following are the recommended locations for WFM files. For information on partitions, see [WFM Server Hardware Requirements](#).

File Type	Location	Example
Software installation and license files	Applications partition <partition drive>:\Software\<product version>	D:\Software\WFM_95
WFM application files	Applications partition <partition drive>:\cisco\WFO_WFM\	D:\Software\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

Order of Installation

The components in your WFM system should be installed in the order outlined here. For deployment configuration diagrams and capacity and sizing information, see [Deployment Capacity and Sizing](#).

Single Server/Onboard SQL Server Deployment

Application/Database Server

Installed Components	Comments
SQL Server	Install before installing any other components

Installed Components	Comments
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>

Optional SQL Server Reporting Services Server

Installed Components	Comments
SQL Server Reporting Services	Install on a dedicated server.

Single Server/Offboard SQL Server Deployment

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>

Optional SQL Server Reporting Services Server

Installed Components	Comments
SQL Server Reporting Services	Install on a dedicated server.

SQL Server Considerations

Consider the following when installing and configuring SQL Server.

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, 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.

Time Zone, Date, and Time

The time zone, date, and time on the server that hosts the SQL Server database and the server that hosts WFM must be the same. If they are not identical, WFM events and data will not show the correct date and time.

Note: If your servers are hosted or in a datacenter outside the users' time zone, you must change the WFM and SQL Server servers to match the users' time zone to see the data in the appropriate time.

Installing a Base Release

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

Note: After any installation or upgrade, clear your browser cache in order to be sure of viewing the latest version of WFM.

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 InstallShield Wizard.
4. Click Next to display the Select Destination Location window.
5. The default installation folder is C:\Program Files\Cisco. If you want to change the default folder, click Change and follow the prompts.

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

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

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

IMPORTANT: Be sure to preserve your WFM database. Do not delete it after uninstalling a previous version of WFM.

Note: After any installation or upgrade, clear your browser cache in order to be sure of viewing the latest version of WFM.

Because WFM 11.5 is a 64-bit application, and all previous versions of WFM were 32-bit applications, no over-the-top upgrades are possible. If you are upgrading from a previous version of WFM, you must first uninstall that version and then perform a fresh install of WFM 11.5 (see [Installing a Base Release](#) for instructions).

WFM 11.5 supports upgrades from the following versions:

- WFM 10.5
- WFM 11.0

To install an upgrade:

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. 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. When the installation is complete, WFM Configuration Setup (Postinstall) is launched.
8. Configure WFM. For instructions, see [Configuring WFM](#)
9. If present on the server, restart your security software.
10. Log into WFM and test your WFM system to ensure it is working properly.

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 an Update

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

Note: After any installation or upgrade, clear your browser cache in order to be sure of viewing the latest version of WFM.

WFM is updated periodically. The update 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 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 [Installing a Base Release](#).

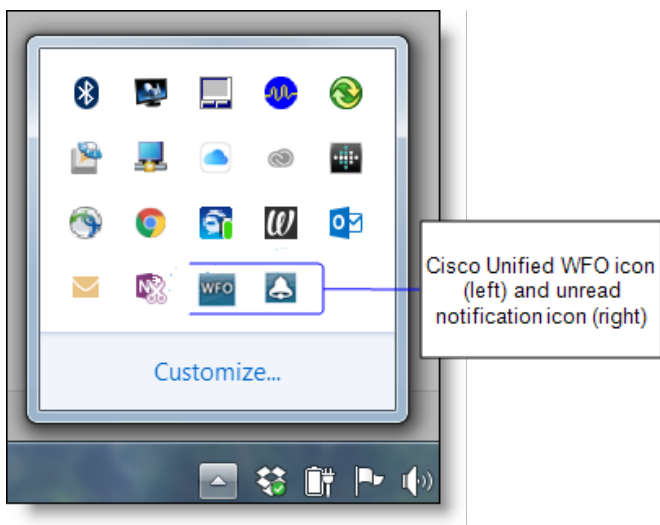
Installing the Unified Workforce Optimization Notification Client

The Unified Workforce Optimization Notification client can be used in systems that use Active Directory logins to access Unified Workforce Optimization. This feature is not available in systems that do not use Active Directory logins.

When this client is installed on the user's desktop, any notifications and alerts that the user receives via the Alerts bubble on the Unified Workforce Optimization menu bar are also displayed as toaster

popups on the desktop. An icon for Unified Workforce Optimization is present in the system tray, as well as an icon that appears whenever an unread notification is present.

Alerts and notifications are displayed whether or not the user is logged into Unified Workforce Optimization. See the *Workforce Management User Guide* for more information on using the system tray icons.



The Notification client can be installed manually on each user's PC, or automatically by a system-wide push. The installation file is accessed from a web page located on the WFM Transaction Services server.

Manual Installation

To install the Notification client manually, follow these steps.

1. On the PC where you want to install the Notification client, start the browser.
2. Navigate to this URL:

```
http://<Transaction Services server IP  
address>/TUP/WFM/Notification.htm
```

Note: In a combined system with both QM and WFM, use the URL `http://<Base Services server IP address>/TUP/QM/Notification.htm`.

3. Follow the instructions on the page.

Note: You must have Administrator privileges on the PC in order to download and install the Notification client. If User Account Control (UAC) is off, you will not be able to download and install the client. If UAC is on, you will be asked to provide the Administrator credentials and then you can proceed with the installation. Alternatively, an administrator can configure the elevated privileges policy so that users with limited privileges can install a desktop application. See *Elevating User Privileges* below.

Elevating User Privileges

To allow users with limited privileges install a desktop application on a PV you must enable the Windows policy “Always Install with Elevated Privileges” for both the User Configuration and the Computer Configuration.

To elevate user privileges, follow these steps:

1. Start the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in.
2. Right-click the appropriate organizational unit (OU) and select Properties from the popup menu.
3. On the Group Policy tab, select the Group Policy object (GPO) and click Edit.
4. Expand Computer Configuration > Administrative Templates > Windows Components > Windows Installer.
5. Double-click Always install with elevated privileges.
6. Choose Set to Enabled, and then click OK.
7. Expand User Configuration > Administrative Templates > Windows Components > Windows Installer.
8. Double-click Always install with elevated privileges.
9. Choose Set to Enabled, and then click OK.

Automated Installation

The Notification client MSI-based installation can be deployed (“pushed”) via a third-party automated package distribution tool that makes use of the Microsoft Windows Installer service.

Requirements

Support of automated package distribution depends on compliance with the following requirements.

- Installations must be executed on the target machine. Deployment methods that capture a snapshot of an installation and redistribute that image are not supported.
- Installations must be deployed on a per-machine basis. Per-user installations are not supported.

Recommended Deployment Preparation Model

Use the following deployment preparation model before you deploy the client installation in a production environment.

1. Use a lab environment to model the pending deployment.
2. Verify that the required hardware and software are installed on the desktop clients.
3. Install the Transaction services server to obtain a valid client installation package (see *Configuring the Notification Client Installation File* below).
4. Manually deploy the client installation package to ensure that the installation is compatible with your environment and to isolate product installation vs. automated deployment issues.
5. Create the deployment package in accordance with the requirements listed above. It is recommended that you create both installation and uninstallation deployment packages.
6. Test the deployment packages.
7. At deployment time, replace the client installation package from the lab environment with one from the production server.

Configuring the Notification Client Installation File

Run the Notification Client Configuration tool (ConfigureNotificationClient.exe) to create the installation file for the Notification client.

1. Create a virtual drive and load the WFM installation ISO on that drive.
2. Copy the Clients folder and all its contents from the WFM installation ISO to a desktop.
3. On the desktop, open a command window and navigate to the Clients folder.
4. Run ConfigureNotificationClient.exe as an administrator.
5. After the tool starts, follow the prompts. Enter the IP address or host name of the Surrogate Host (the location of Unified Workforce Optimization) and press Enter.

The utility creates the Notification Client installation file.

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.

SNMP Integration

WFM includes SNMP integration for the Monitoring and Notification (MANA) service.

MANA is responsible for sending notifications to administrators or supervisors when it detects events that might negatively affect the functioning of the software or system.

This topic covers SNMP integration and how to take advantage of this method of notification when you install WFM.

Definitions

The following table defines terms used in this topic.

Term	Definition
MIB	Management Information Base. A defined hierarchy of data values managed by a single SNMP Agent application.
OID	Object Identifier. A unique string of digits representing a value defined in an MIB.
SNMP	Simple Network Management Protocol. A common network protocol that describes messages passed between SNMP-enabled applications.
SNMP Agent	An SNMP-enabled application that acts as a client to an SNMP management application by providing data values for registered OIDs.
SNMP GET	An SNMP message used to get a value for a particular OID.
SNMP Management Application	An SNMP-enabled application that can get or set information from a local or remote SNMP Agent application.
SNMP SET	An SNMP message used to set a value for a particular OID.
Trap	An unsolicited SNMP message sent from an SNMP agent to an SNMP management application.

SNMP Implementation

The MANA service already has methods to alert administrators of potential problems with WFM. WFM extends this functionality to SNMP so that hardware/software management is provided for customers who already use SNMP management software.

The MANA service provides unsolicited alerts when it detects problem events. The alert contains the details of the problem, which enables action to be taken to prevent loss of software functionality. The

SNMP trap message contains the same information and can be sent out to multiple SNMP management stations.

MIBs

Two MIBs are used to define the trap messages sent by WFM:

- The CISCO-SMI MIB contains definitions of frequently-used objects
- The CISCO-GENERIC-TRAP MIB file defines the trap message format

Whereas most MIBs are very specific in their use and definitions, the Generic Trap MIB was designed to define a generic message that can be sent by any Cisco application. The data values contained in the trap are used to decode the trap's contents.

For example, these OIDs are used to specify a particular Cisco product:

- 1.3.6.1.4.1.29988.1.1.1—used only for Cisco Quality Management
- 1.3.6.1.4.1.29988.1.1.2—used only for Cisco Agent Desktop
- 1.3.6.1.4.1.29988.1.1.3—used only for Cisco Workforce Management

Rather than use these very specific OIDs, the Generic Trap MIB uses this single OID:

- 1.3.6.1.4.1.29988.1.2—uses a variable that maps to the appropriate product name

Using MIBs

How to configure WFM to enable the sending of SNMP traps is described in the topic, [Monitoring and Notification Step](#). Once configured, MANA will send the SNMP trap messages to all the IP addresses configured. These IP addresses represent machines that are running some type of SNMP management software.

The MIB files are used in order for the management software to display the information from a Ciscogeneric trap in a readable format, or to allow decision code running on the management station to interpret these traps.

The two Cisco MIBs describe the layout of information found in the Cisco trap in a language that SNMP management stations understand. The MIB files need to be placed on a drive accessible to the SNMP management software. Once there, the administrator configures the management station to load the MIB files. How this is done varies, based on the SNMP management station software provider.

The SNMP error codes are the same as the MANA error codes. These error codes are documented in the *Error Code Dictionary*.

Generic Trap

The trap message defined in the CISCO-GENERIC-TRAP MIB is a set of string and numeric values that define the event. The OIDs, field names, and field descriptions are shown in the table below.

OID	Field	Description
1.3.6.1.4.1.29988.1.1	cigtTimestamp	Numeric. The date and time the event was generated. Number of seconds since 1/1/1970.
1.3.6.1.4.1.29988.1.2	cigtProduct	String. The name of the product sending the trap.
1.3.6.1.4.1.29988.1.3	cigtVersion	String. The version of WFM that is installed.
1.3.6.1.4.1.29988.1.4	cigtModule	String. The WFM module reporting the event. Currently, this is MANA. In the future, other modules might be used in addition to MANA.
1.3.6.1.4.1.29988.1.5	cigtSeverity	Numeric. The severity of the event. <ul style="list-style-type: none">■ 1 = Informational. Normal processing messages.■ 2 = Warning. Abnormal event that does not affect product functionality.■ 3 = Error. Error that affects some product functionality.■ 4 = Fatal. Serious error that causes loss of basic functionality.
1.3.6.1.4.1.29988.1.6	cigtEventCode	String. An alphanumeric error code representing the event. This code is used to look up additional information in the <i>Error Code Dictionary</i> .
1.3.6.1.4.1.29988.1.7	cigtEventText	String. A readable string describing the event.

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 Transaction 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](#)

- [Enterprise Settings Step](#)
- Jetty Configuration (action only; this step configures Jetty)
- 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	<p>The host name or IP address of the server that hosts the WFM database.</p> <div style="background-color: #e0f0e0; padding: 5px; border: 1px solid #ccc;"> <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> </div>

Field	Description
Use default instance/ Use named instance	<p>Select the type of database instance you are using for the WFM database.</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>
Instance Port	<p>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.</p>
Instance Name	<p>The name of the database named instance. This field appears only if you select the “Use named instance” option.</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 for WFM).</p> <p>Note: The default language for this user must be set to US English.</p>
Password	<p>The SQL Server user's password.</p>

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 (1-3650)

Forecasts
Schedules
Agent Requests Months (12-120)
Assigned Exceptions

Historical Service Data Months (6-120)
Agent Productivity Data Months (6-120)

GIS Agent
Productivity/Service Days (1-3650)
Historical Data files
Vacation Report files Days (1-3650)

Audit Trail Days (7-3650)

Schedule History Days (0-365)

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 1-3650 days (10 years). Default = 15 days.</p> <p>Agent adherence detail information is the agent state data needed to calculate adherence.</p> <div style="border: 1px solid black; 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. A longer the retention period requires greater server storage space. See Deployment Capacity and Sizing for more information.</p> </div>
Forecasts Schedules Agent Requests Assigned Exceptions	<p>Value from 12-120 months (10 years). Default = 13 months.</p> <p>This information is forecast data, agent schedules, agent requests displayed in the Messaging application, and the exceptions assigned to agents.</p>
Historical Service Data	<p>Value from 6-120 months (10 years). Default = 25 months.</p> <p>This information is all the ACD contact data gathered for each service queue.</p>
Agent Productivity Data	<p>Value from 6-120 months (10 years). Default = 25 months.</p> <p>This information is the ACD data gathered for each agent that measures agent productivity.</p>
GIS Agent Pro- ductivity/Service His- torical Data files	<p>Value from 1-3650 days (10 years). Default = 30 days.</p> <p>These are the historical data files imported into WFM by the GIS Connector Tool.</p>
Vacation Report files	<p>Value from 1-3650 days (10 years). Default = 30 days.</p> <p>These are the files containing agent vacation hours data imported from the HRMS.</p>
Audit Trail	<p>Value from 7-3650 days (10 years). Default = 30 days.</p> <p>This determines how long audit trail information is retained. The information is viewed in the Audit Trail Report.</p>

Field	Description
Schedule History	<p>Value from 0-365 days (1 year). Default = 0 days.</p> <p>This determines how much schedule history is kept, to allow an agent's schedule to revert to an earlier version.</p>
Time to purge the retention period data	<p>Default = 04:00 (24-hour format)</p> <p>Set the time of day that data that is beyond the configured retention period is purged from the database.</p>


- 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.
- If Schedule History is set to 0 (zero days), no schedule history is kept, and agent's schedules cannot be reverted to previous versions.
- 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 Transaction Server Step

The WFM Transaction Server step configures the host name or IP address of the server where the WFM services or iCalendar service are installed.

Note: The name of this step is “WFM iCalendar Server” if Postinstall is run on a server that hosts the iCalendar service and is separate from the WFM Transaction Services server.

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



The screenshot shows a dialog box titled "WFM Transaction Server". Inside the dialog, there is a text prompt: "Select the IP address or host name of the WFM Transaction Services Server from the drop-down list, or enter a new one." Below this prompt, there is a label "Host Name or IP Address" followed by a drop-down menu. The menu is currently displaying the IP address "10.192.246.15".

ACD Connection Step

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

Cisco Unified CCX ACD

ACD Connection

Select ACD Cisco Unified CC Express

Select Language English

Enable sync to associate agents with the NewAgents (system) team

Use GIS to capture ACD historical data manually

Use GIS to capture ACD real-time agent state data

Primary IP Address or Host Name 10.192.246.18

Primary Instance Name wfm18_uccx

Secondary IP Address or Host Name 10.192.246.18

Secondary Instance Name wfm18_uccx

User Name uccxhtruser

Password *****

Client Locale en_US.CP1252

Server Locale en_US.57372

	IP Address or Host Name	Port
CTI Servers	10.192.246.18	12028

Add
Remove
Edit

Capture Settings...

PREVIOUS
NEXT

Field	Description
Select ACD	Select Cisco Unified CC Express from the drop-down list.
Select Language	Select the language used in the contact center. This field appears only if a localized version of WFM has been installed.

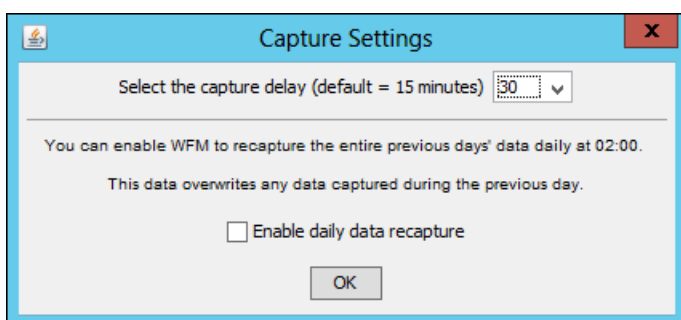
Field	Description
Sync new agents to the NewAgents (system) team	<p>Select this check box if you want all new agents automatically added to the NewAgent (system) team. The check box is selected by default. When cleared, agents are associated only with the team defined for them in the ACD. The ACD team is the agents' Main Team whether or not the check box is selected.</p> <div data-bbox="597 510 1377 674" style="border: 1px solid black; background-color: #e1f5fe; padding: 5px;"> <p>Note: Administrators will continue to be able to associate agents with additional teams that are not linked to the agent in the ACD.</p> </div>
Use GIS to capture ACD historical data manually	Select the check box if you want to use the GIS API to capture ACD historical data rather than using the default of capturing historical data automatically.
Use GIS to capture ACD real-time agent state data	Select the check box if you want to use the GIS API to capture ACD real-time agent state data rather than using the default ACD real-time data source. Use this option if you want to collect real-time data for both interactive and non-interactive service queues. Real-time data is not available for non-interactive service queues from the default ACD real-time data source.
Primary IP Address or Host Name	The ACD's primary IP address or host name.
Primary Instance Name	<p>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 _uccx to complete the instance name <div data-bbox="597 1556 1377 1686" style="border: 1px solid black; background-color: #e1f5fe; padding: 5px;"> <p>Example: If your host name is 80-ABC, your instance name will be i80_abc_uccx.</p> </div>
Secondary IP Address or Host Name	If this is a redundant system, enter the ACD's secondary IP address or host name.

Field	Description
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.
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 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.

WFM Authentication

Authentication With Other Cisco Products

Share Login Fields

Unified Workforce Optimization Container (IP Address or Host Name)

Active Directory

Use Active Directory

User must have read access to the given domain.

Base DN	Search Base	Domain Name	IP Address ...	Port	User Displa...	Use														
<div style="border: 1px solid gray; padding: 5px;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 15%;">Base DN</th> <th style="width: 15%;">Search Base</th> <th style="width: 15%;">Domain Name</th> <th style="width: 15%;">IP Address ...</th> <th style="width: 10%;">Port</th> <th style="width: 15%;">User Displa...</th> <th style="width: 10%;">Use</th> </tr> </thead> <tbody> <tr> <td colspan="7" style="height: 80px;"> <div style="border: 1px solid gray; height: 70px; width: 100%;"></div> </td> </tr> </tbody> </table> </div>							Base DN	Search Base	Domain Name	IP Address ...	Port	User Displa...	Use	<div style="border: 1px solid gray; height: 70px; width: 100%;"></div>						
Base DN	Search Base	Domain Name	IP Address ...	Port	User Displa...	Use														
<div style="border: 1px solid gray; height: 70px; width: 100%;"></div>																				

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.

Field	Description
Unified Workforce Optimization Container	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 host name or IP address of the Cisco Quality Management base services server.
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.

Best Practice: If you are using multiple Unified Workforce Optimization products, you should configure your Jetty web server to use 1024 MB of RAM for each product.

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.

The 'Enter Data' dialog box contains the following fields and options:

- Base DN:** dc=p1,dc=rd,dc=ld
- Domain Name:** p1.rd.ld
- IP Address or Host Name:** 10.192.252.11
- Port:** 636
- User Display Name:** wfmaduser1 wfmaduser1
- User Password:** (masked with dots)
- User Search Base:** u=R&D,ou=Users By Department,ou=User Accounts
- Use SSL:**
- Certificate File Names (separated by semicolon):** C:\Certs\rdcert2.cer;C:\Certs\cert2.cer
- Admin Group:** SG-DL-WFM_DE

Buttons: Yes, No

Field	Description
Base DN	<p>The location in the directory server tree under which all Active Directory users are located.</p> <div data-bbox="597 365 1377 533" style="border: 1px solid black; background-color: #e6f2e6; padding: 5px;"> <p>Note: Be sure to narrow your base DN as much as possible to ensure that logins complete in a reasonable amount of time.</p> </div>
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="597 865 1377 1033" style="border: 1px solid black; background-color: #e6f2e6; padding: 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 Distinguished Name of the user that WFM uses for authentication. 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.

Field	Description
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="597 474 1377 569" style="background-color: #e1f5fe; padding: 5px; border: 1px solid #ccc;"> <p>Note: Certificates must be base-64 encoded.</p> </div>
Admin Group	<p>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.</p>

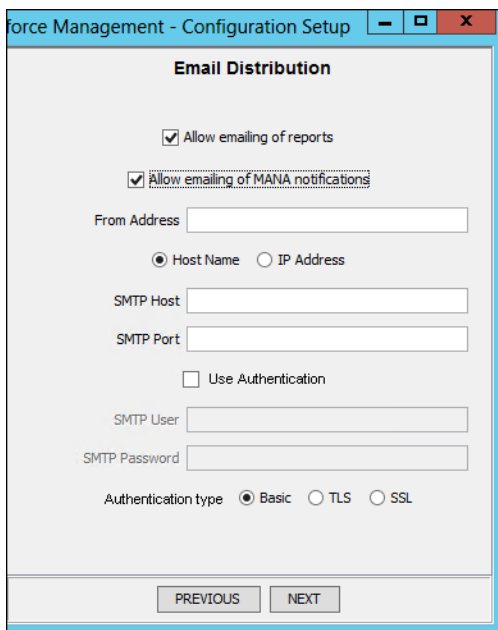
Managing Active Directory Domains

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.
SMTP User	The username required to gain access to the SMTP server.

Field	Description
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/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.
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.

Note: For more information on SNMP, see [SNMP Integration](#).

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:

- 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

Enterprise Settings

HRMS

Enable HRMS integration

Time to export user vacation data (default = 05:00)

Report Logo

Security Mode

Use HTTPS to communicate among WFO components

Adherence Calculation Settings

Number of days in the past to recalculate adherence

Time to run adherence calculations ▼

Reports Folder Location

SSRS Configuration

Field	Description
<p>Enable HRMS Integration</p>	<p>Select this check box to enable a connection between WFM and your HRMS (Human Resources Management System).</p> <p>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 <i>Historical and Real-Time Data Import Reference Guide</i>.</p>

Field	Description
Time to export user vacation hours	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 <i>Configuring the Report Logo</i> below for 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 ACC service will perform adherence and conformance calculations. Default is 5 days, and valid entries are 1-90 days.
Time to run adherence calculations	The time of day you want adherence and conformance to be calculated. Default time is 04:00. Note: If you change the time that adherence calculations are run it is possible to conflict with the daily data recapture, which will cause adherence data to be unavailable the next day. Best practice is to use the default time.
Reports Folder Location	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 <i>WFM Historical and Real-Time Data Import Reference Guide</i> for more information.

Configuring the Report Logo

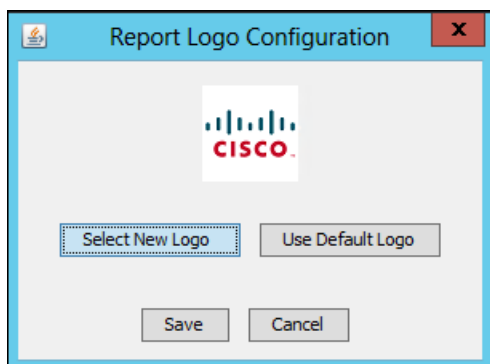
You can customize the logo that appears on WFM reports by replacing the default logo with one of your own.

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\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 than 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 [Port Usage](#) 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 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. However, a WFM certificate is required for WFM reports because the reports point directly at the WFM base server.

Note: If you have a Certificate Authority (CA)-signed certificate with a weak signaling algorithm, WFM Configuration Setup will ask if you want to keep the CA-signed certificate or regenerate a new self-signed certificate with a stronger signaling algorithm. This self-signed certificate will then need to be signed by a Certificate Authority.

If you already have a self-signed certificate, WFM Configuration Setup will automatically replace the certificate if necessary with another self-signed certificate that has a stronger signaling algorithm.

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 VeriSign 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\cisco\WFO_WFM\Java\bin\keytool.exe" -keystore  
"C:\Program Files\Common Files\WFM\config\keystore" -storepass  
Sp@nllnk -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\cisco\WFO_WFM\Java\bin\keytool.exe" -  
keystore "C:\Program Files\Calabrio\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\cisco\WFO_WFM\Java\bin\keytool.exe" -  
keystore "C:\Program Files\Common Files\WFM\config\keystore"  
-storepass Sp@nllnk -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\cisco\WFO_WFM\Java\bin\keytool.exe" -keystore  
"C:\Program Files\Common Files\WFM\config\keystore" -storepass  
Sp@nllnk -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\cisco\WFO_WFM\Java\bin\keytool.exe" -keystore  
"C:\Program Files\Common Files\WFM\config\keystore" -storepass  
Sp@nllnk -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 already 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](#).

Generating Certificates with Active Directory

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

Follow these steps to generate certificates using 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

For more information, see the Microsoft Knowledge Base article 555252, "How to export Root Certification Authority Certificate" at

<http://support.microsoft.com/kb/555252>

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 using SHA2.

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\cisco\WFO_WFM\Java\bin\keytool.exe" -keystore  
"C:\Program Files\Common Files\WFM\config\keystore" -storepass  
Sp@nllnk -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\cisco\WFO_WFM\Java\bin\keytool.exe" -keystore  
"C:\Program Files\Common Files\WFM\config\keystore" -storepass  
Sp@nllnk -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.

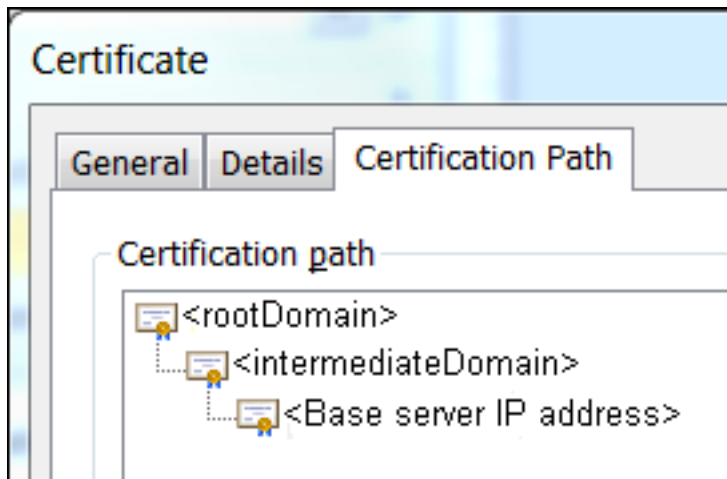
3. Click Request a certificate.

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_webserver.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\cisco\WFO_WFM\Java\bin\keytool.exe" -  
keystore "C:\Program Files\Calabrio\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\cisco\WFO_WFM\Java\bin\keytool.exe" -  
keystore "C:\Program Files\Common Files\WFM\config\keystore"  
-storepass Sp@nllnk -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\cisco\WFO_WFM\Java\bin\keytool.exe" -keystore  
"C:\Program Files\Common Files\WFM\config\keystore" -storepass  
Sp@nllnk -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\cisco\WFO_WFM\Java\bin\keytool.exe" -keystore  
"C:\Program Files\Common Files\WFM\config\keystore" -storepass  
Sp@n1lnk -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 already 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 uninstillation process.