Cisco Unified Workforce Optimization

Workforce Management Installation Guide 10.0

First Published: November 30, 2013
Last Modified: May 9, 2014

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

Workforce Management Installation Guide

Contents

Contents

Contents

Contents

Overview

1

Introduction

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

Table 1. Workforce Management Installation Components

Installation	Components
Capture Services	• WFM Capture service
Compile Services	• WFM Compile service
Process Services	• WFM Request service • WFM Schedule service
Transaction Services	• WFM Real Time Engine (RTE) service • WFM Adherence Conformance Calculator (ACC) service • WFM Jetty service • WFM Mana service • WFM Product Adapter service • WFM Sync service • WFM Tomcat service

These components are installed on a single server. See "Server Configurations" on page 20 for more information.

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

For information about configuring WFM, see the *Workforce Management Administrator User Guide* and the *Monitoring and Recording Services Administrator User Guide*.

What's New in This Version

WFM 10.1 includes the following new features.

WFM 10.0(1)

- Administrators can configure shrinkage percentages in the Application Management application in Workforce Optimization and apply them when generating a schedule
- Administrators can configure service queue groups in the Application Management application in Workforce Optimization
- Administrators and supervisors can now configure reports to run on a scheduled, recurring basis and be sent to specified email addresses as attachments
- Supervisors can now run reports from the WFM legacy application
- Schedule exceptions can now be saved to the agent's scheduled exception list so that if the schedule is rerun, the exception is not lost and will appear in the agent's schedule
- The Coverage drawer in the Agent Schedules application has been expanded to include three new views: Coverage: Reforecast, Coverage: Shrinkage, and Intraday: Data.
- The Capture service has been improved for better data accuracy

WFM 10.0(1) SR1

- Bug fixes

WFM 10.0(1) SR2

- Bug fixes

WFM 10.0(1) SR3

- The interface and the Help have been localized in Danish, Dutch, German, French, Italian, Portuguese (Brazilian), Spanish, and Swedish
- Bug fixes

WFM Documentation

The following documents contain additional information about WFM. They are available online on the Cisco website (www.cisco.com/en/US/products/ps8293/tsd_products_support_series_home.html).

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

Workforce Management Services

Workforce Management ACC Service

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

Workforce Management Capture Service

The Workforce Management Capture service manages the import of historical data from the Cisco ACD database.

When the Capture service detects new data, it sends a compilation request to the Compile service.

Workforce Management Compile Service

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

Workforce Management Jetty Service

The Jetty service is a webserver that supports the Workforce Optimization user interface and notification data from the Mana service.

Workforce Management Mana Service

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

Workforce Management Product Adapter Service

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

Workforce Management Real Time Engine Service

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

Workforce Management Request Service

The Workforce Management Request service generates distributions and forecasts.

Workforce Management Schedule Service

The Workforce Management Schedule service manages schedule requests.

Workforce Management Sync Service

The Workforce Management Sync service connects to the Unified CCX database using the SQL connection. The Sync service retrieves and processes configuration data such as contact service queue (CSQ) configurations, team configurations, and agent configurations.

Workforce Management Tomcat Service

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

Port Usage

Table 2 lists the ports used by WFM and its components.

NOTE: The port numbers are defaults and can be changed as needed.

Table 2. WFM Port Usage

Server application	Destination port (listening)	Client application
CTI server*	TCP 12028 Side A TCP 12028 Side B	WFM Sync Service WFM RTE Service
Unified CCX instance of Informix		WFM Capture Service
WFM instance of SQL Server	TCP 1433 TCP 1434	WFM ACC Service WFM Capture Service WFM Compile Service WFM Mana Service WFM Product Adapter Service WFM RTE Service WFM Request Service WFM Schedule Service WFM Sync Service WFM Tomcat
WFM Jetty Service	TCP 59103 (surrogate) TCP 443 (HTTPS) TCP 80 (HTTP)	WFM Product Adapter Web browser Web browser
WFM Sync Service	TCP 59011	unused
WFM Tomcat	TCP 8087 (c3) TCP 8017 TCP 8007	HTTP AJP 1.3 Shutdown port

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

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 WFM Transaction server that uses these ports or the Jetty service might fail. Examples include Microsoft SQL Server 2008 Reporting Services and Microsoft Internet Information Services (IIS).

The SQL Server 2008 Reporting Services is a tool that provides a web-based GUI to present SQL performance information. You can configure this tool to use another port and so not interfere with the Jetty service.

To change the port used by Reporting Services:

1. On the WFM Transaction server, launch Reporting Services Configuration Manager (Start > Microsoft SQL Server 2008 > Configuration Tools > Reporting Services Configuration Manager).
2. Connect to the report server instance.
3. In the left pane, click Web Service URL. In the right pane, under Report Server Web Service Site Identification, change the TCP port from 80 to another port (for example, 8080).
4. In the left pane, click Report Manager URL. In the right pane, click Advanced and in the resulting window change the TCP port from 80 to another port (for example, 8080).
5. Click Apply, then exit the Configuration Manager.

System Requirements

2

Overview

This chapter covers the following subjects:

System Requirements

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

Workforce Management Environment

WFM 10.0 is compatible with Cisco Quality Management 10.0.

System Environment

WFM has been verified in the following environments:

- Cisco Unified Contact Center Express 8.5, 9.0, and 10.0

Operating Environment

Server Operating Systems

The supported operating systems for WFM servers are the following.

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

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

Hardware Requirements and Capacity

Table 3 displays the minimum hardware requirements and capacity for WFM servers in the supported configurations.

NOTE: The capacity numbers shown in Table 3 are estimates. The actual numbers might vary.

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

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

Users are defined as follows.

- Configured users—Any scheduled plus all other users (for example, supervisors, managers, and schedulers).
- Concurrent users—The users who are logged into WFM at any given time.

Table 3. WFM server capacities

	Single Server Configurations		
Server Type	Physical	Physical	Cisco UCS OVA
Processor Cores	2	4	2 x Nehalem class CPU
Memory (GB)	8	8	8
System Storage (GB)	250	250	250
Max Number Named Users	450	900	900
Max Number Concurrent Users	150	300	300

WFM in a Cisco Unified Computing System Environment

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

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

WFM in a Virtual Server Environment

A virtual server environment requires hardware resources equivalent to those required for a physical server for a given number of users (see "Hardware Requirements and Capacity" on page 16).

NOTE: WFM systems hosted on a VMware ESX server have been tested for functionality only, not for scalability. Due to the many possible virtual server configurations, and the possible impact on WFM of additional hosted virtual servers, the actual server performance in a VMware environment is the responsibility of the customer. Cisco support for performance and scalability issues is limited to server-based deployments. If a problem occurs in a VMware deployment, the customer might be required to shut down other

sessions or reproduce the problem in a non-VMware configuration to assist in isolating the issue.

The supported versions of VMware virtual server are the following:

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

Desktop Requirements

WFM is operating system-independent. The only requirement is that the OS can run the supported web browsers (see "Third Party Software" on page 18).

Third Party Software

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

Table 4. Required third party software

Application	Where Installed	Use
Any of the following: Microsoft SQL Server 2005 32-bit Standard and Enterprise Editions, including the latest service pack Microsoft SQL Server 2008 32-bit and 64-bit Standard and Enterprise Editions, including the latest service pack Microsoft SQL Server 2008 R2 32-bit and 64-bit Standard and Enterprise Editions, including the latest service pack	WFM database server	Database
Adobe Acrobat Reader 6.0 or later	Client desktop	PDF-based reports and WFM user documentation
Either of the following: Microsoft Internet Explorer 8 (32-bit) Microsoft Internet Explorer 9 (32-bit)	Agent and supervisor desktops	WFM desktop widgets and HTML-based reports
	Scheduler and Administrator client desktop	WFM administrative interface, WFM desktop widgets, and HTML-based reports

Microsoft Internet Explorer Requirements

Popup Blockers

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

> **NOTE:** You can try other browsers (for example, Firefox or Chrome) if you want to improve performance. However, these browsers were not tested and are not supported by Calabrio. If problems are found while using an unsupported browser, you will be asked to recreate the problem while using a supported browser.

Server Configurations

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

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.

Table 5. SQL Native Client version to be used in multiple SQL Server version systems

ACD Database	WFM Database	SQL Native Client
SQL Server 2008	SQL Server 2008	2008
SQL Server 2008	SQL Server 2005	2008
SQL Server 2005	SQL Server 2008	2008
SQL Server 2005	SQL Server 2005	2005, 2008*

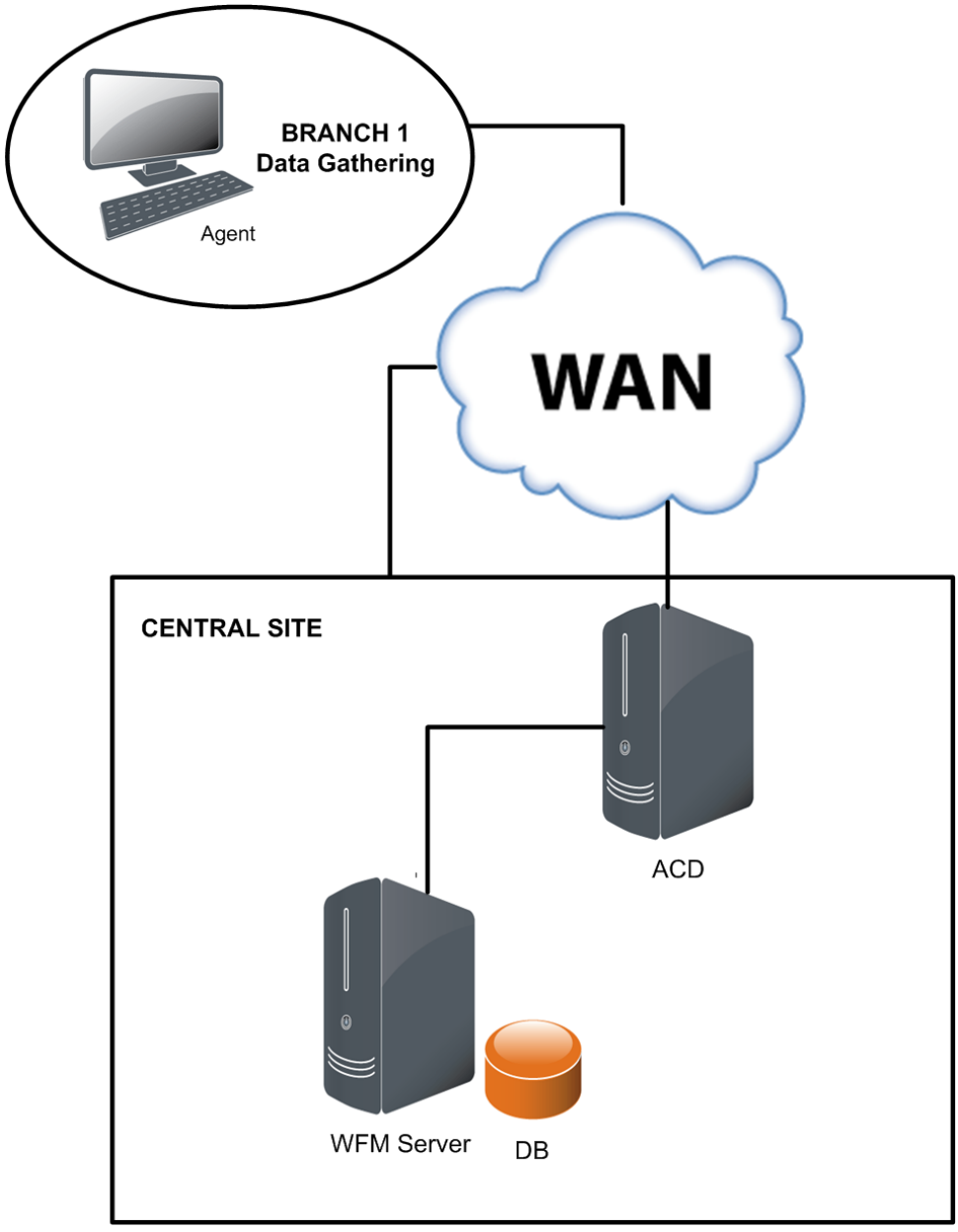
* SQL Native Client is backward compatible, so version 2008 will work in a SQL Server 2005 environment.

Single Server Configuration

A single server configuration has one ACD cluster with all Workforce Management services located on a single server (Figure 1 on page 21). The single server configuration supports 150 concurrent users and 450 configured users.

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

Figure 1. Single server configuration



Single Server Configuration With Offboard SQL Server

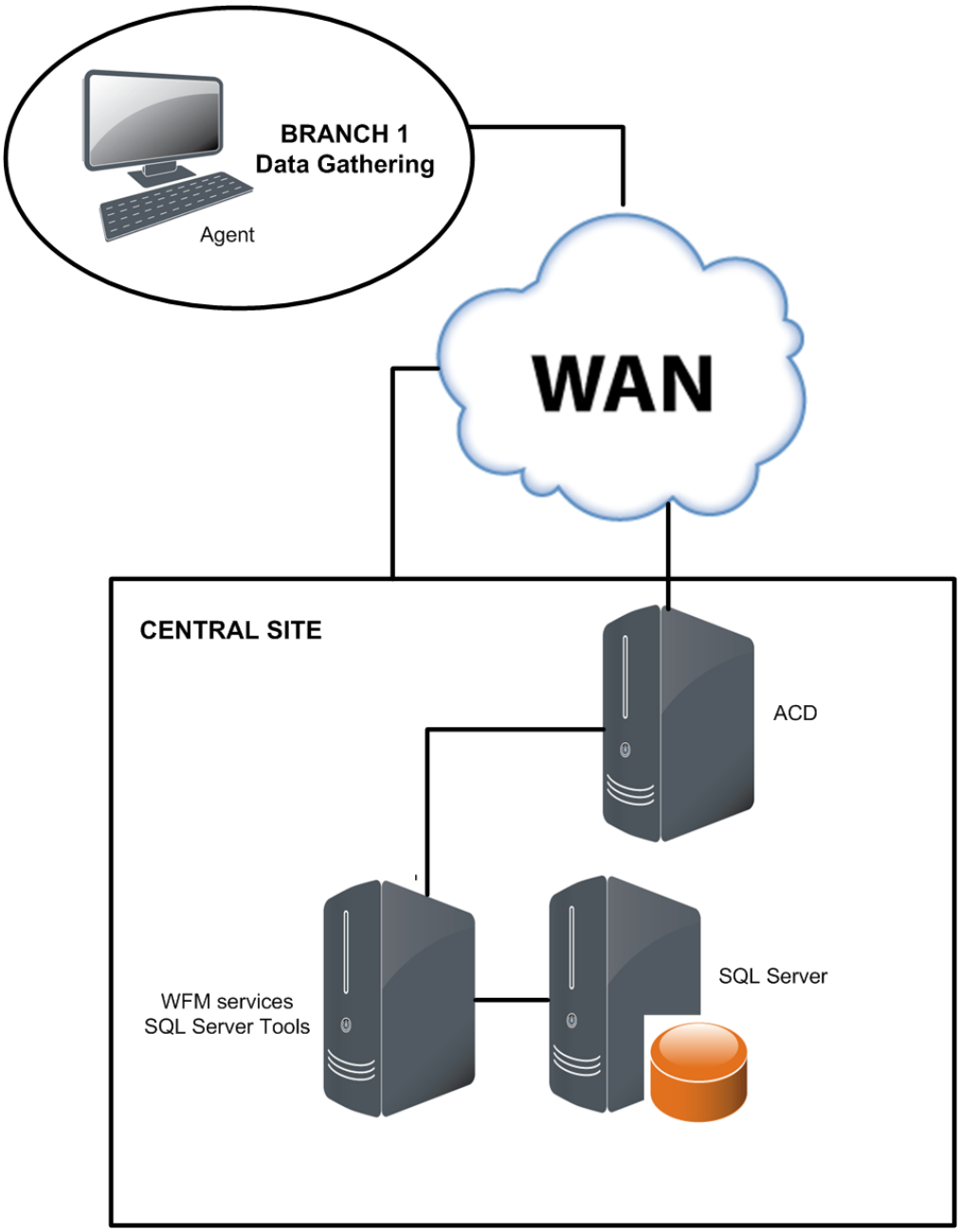
If you choose to use an offboard SQL server (Figure 2 on page 23), the installation follows the same configuration as for the single server, except that you must install the SQL Server Tools on the WFM server before WFM is installed. SQL Native Client, which is part of the SQL Server Tools, is required to maintain system configuration data. This configuration supports 300 concurrent users and 900 configured users.

Table 6 shows how components must be installed on the two servers.

Table 6. Single server with offboard SQL server component locations

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

Figure 2. Single server configuration with offboard SQL Server



Configuration Data

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

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

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

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

Before You Install WFM

3

Overview

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

- Installing Microsoft SQL Server (page 26)
- Creating a SQL Server Login for WFM (page 28)
- Installing Microsoft SQL Server Tools (page 29)
- Configuring Regional Settings (page 30)
- Verifying Prerequisites (page 33)

Installing Microsoft SQL Server

NOTE: You must install Microsoft SQL Server 2005 or 2008 on the WFM server. 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 information about how to install Microsoft SQL Server, see the Microsoft SQL Server installation documentation.

Complete the Microsoft SQL Server Setup utility windows as shown in Table 7.

Table 7. Microsoft SQL Server Setup utility entries

Window	Complete as follows:
Registration Information	Enter your name, company, and product key.
Components to Install	Select check boxes for: • SQL Server Database Services • Workstation Components • Any other desired components **NOTE**: If you install the SQL Server 2008 Reporting Services tool, you must configure it so that it does not use TCP port 80 (if it uses port 80, it interferes with the WFM Jetty service). For more information, see "WFM Jetty Service Ports" on page 12.
Instance Name	Select one of the following options: • Default Instance • Named Instance. If you select this option, specify the named instance.
Service Account	Select Use the Built-In System Account, then select Local System from the drop-down list. Under Start Services at the End of Setup, highlight SQL Server, SQL Server Agent, and SQL Browser.
Authentication Mode	Select Mixed Mode. Enter a password for the SQL Server System Administrator (sa) logon.

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

Window	Complete as follows:
Collation Settings	Under SQL Collations, select the following option: Dictionary order, case-insensitive, for use with 1252 Character Set **NOTE**: The SQL collation name is SQL_Latin1_General_CP1_CI_AS. See http://msdn2.microsoft.com/en-us/library/ms180175.aspx for more information about SQL Server collation settings.

Creating a SQL Server Login for WFM

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

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

To create a SQL Server login for WFM:

1. On the SQL Server computer, start Microsoft SQL Server Management Studio and log in.
2. In the Object Explorer pane, expand the SQL Server instance. Choose Security > Logins.
3. Right-click Logins and choose New Login.
4. The Login–New window appears.
5. On the General page, enter the login you want WFM services to use to connect to SQL Server. Select SQL Server Authentication, enter a password, and clear the Enforce password policy check box so that the WFM user account does not expire.
6. On the Server Roles page, select dbcreator and sysadmin from the list of server roles.

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

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

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

Installing Microsoft SQL Server Tools

These steps apply if your system includes an off-board SQL Server.

After you install Microsoft SQL Server on the WFM server that hosts the WFM transaction services, you must install SQL Native Client on the remaining servers. SQL Native Client is automatically installed when you run the setup for Microsoft Server Tools.

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

To install the Microsoft SQL Server Tools:

- Run the setup.exe located in the Tools directory of the Microsoft SQL Server CD and follow the prompts.

  NOTE: For more information about SQL Native Client settings, see http://msdn2.microsoft.com/en-us/library/ms131321.aspx.

8.

-

Configuring Regional Settings

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

To change the regional settings in the Windows registry:

1. Open the Windows registry on the Capture services server.
2. Navigate to the following registry key:

   HKEY_USERS\.DEFAULT\Control Panel\International\
3. Ensure that the registry settings under the International key are as listed in Table 8.

Table 8. Regional settings

Value	Type	Data
iCalendarType	string	1
iCountry	string	1
iCurrDigits	string	2
iCurrency	string	0
iDate	string	0
iDigits	string	2
iFirstDayOfWeek	string	6
iFirstWeekOfYear	string	0
iLZero	string	1
iMeasure	string	1
iNegCurr	string	0
iNegNumber	string	1
iTime	string	0
iTimePrefix	string	0
iTLZero	string	0
Locale	string	00000409
NumShape	string	1
s1159	string	AM

Table 8. Regional settings (cont'd)

Value	Type	Data
s2359	string	PM
sCountry	string	United States
sCurrency	string	$
sDate	string	/
sDecimal	string	.
sGrouping	string	3;0
sLanguage	string	ENU
sList	string	,
sLongDate	string	dddd, MMMM dd, yyyy
sMonDecimalSep	string	.
sMonGrouping	string	3;0
sMonThousandSep	string	,
sNativeDigits	string	0123456789
sNegativeSign	string	-
sPositiveSign	string	
sShortDate	string	mm-dd-yyyy
sThousand	string	,
sTime	string	;
sTimeFormat	string	h:mm:ss tt

Configuring Firewall Port Exceptions

If Microsoft Windows Firewall is enabled when WFM is installed, the installation process opens the necessary firewall ports. See "Port Usage" on page 12 for a list of the ports used by WFM.

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

Verifying Prerequisites

Active Directory Prerequisites

You need the following information:

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

Unified CCX Prerequisites

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

- Cisco Unified Contact Center Express (Unified CCX)
- Cisco Unified Communications Manager (Unified CM)
- IP address and port number of the server that hosts the CTI service (see "Port Usage" on page 12)
- Cisco Monitoring and Recording Services server IP address (if you use Monitoring and Recording Services)
- Unified CCX server IP address:
  - Single node environment: use the primary server IP address
  - High Availability (two node) environment: use the secondary server IP address

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

WFM Prerequisites

To install WFM, you need the following information.

- WFM server IP address
- WFM SQL Server database username and password you used in "Creating a SQL Server Login for WFM" on page 28
- SQL Server instance name you used in "Installing Microsoft SQL Server" on page 26 (if you did not use the default instance)

Installing and Configuring WFM

4

Overview

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

- Pre-Installation Considerations (page 36)
- Installing WFM (page 38)
- Configuring WFM (page 43)

Pre-Installation Considerations

For All Types of Installs

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

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

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

For Upgrades

Before you install a WFM upgrade, do the following:

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

  NOTE: Do not remove the old SQL Server WFM database. The old SQL Server WFM database is required during the upgrade process. Backing up your database is recommended in case a problem occurs during the upgrade.

- Uninstall any service releases (SRs) applied to the old version of WFM. For instructions, see "Rolling Back to a Previous State" on page 66. Removing an SR takes approximately 10 minutes, followed by a server reboot.
- Uninstall the old version of WFM. For instructions, see "Removing WFM Services" on page 67. Removing a WFM base release takes approximately 10 minutes. The system does not reboot.

  NOTE: When you uninstall WFM, the WFM SQL Server database instance remains.

Upgrading Systems with Pending Requests

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

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

For Patches

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

- Because installing a WFM patch requires bringing down a WFM system, schedule installation for a maintenance period when your WFM system is out of production.
- Run WFM Configuration Setup and note the settings used. Not all WFM settings are maintained when a patch is installed, and you might need to enter them again.
- Back up the SQL Server WFM database using SQL Server backup tools.

Installing WFM

Follow these steps to install or upgrade WFM.

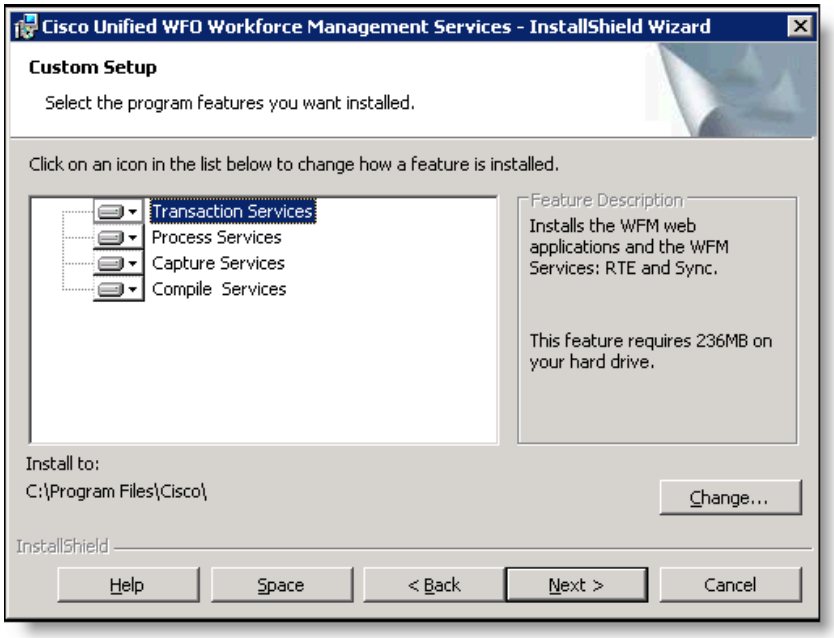
Installing a Base Release

Install the WFM services according to the supported system configuration as described in "Server Configurations" on page 20.

To install WFM:

1. On the WFM server, log in as a local administrator.
2. Shut down any security software that might be running.
3. On the installation CD, double-click setup_WFM_<version>.exe to start the InstallShield Wizard.
4. Click Next to display the Custom Setup window (Figure 3).

Figure 3. Custom Setup window



5. The default installation folder is C:\Program Files\Cisco (or C:\Program Files (x86)\Cisco on a 64-bit system). 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 continue. Follow the InstallShield Wizard prompts until the installation is finished.

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

7. After the installation is complete and the InstallShield Wizard closes, WFM Configuration Setup starts. See "Configuring WFM" on page 43 for instructions on how to configure the services you just installed.
8. After you have completed WFM Configuration Setup, restart your security software (if present on the server).

Installing an Upgrade

NOTE: Review "Pre-Installation Considerations" on page 36 before installing upgrades.

WFM 10.0 supports direct upgrades from the following versions:

- WFM 8.5(2)
- WFM 9.0(1)

Upgrades from all other versions are indirect as per the upgrade paths shown in Table 9.

Table 9. Upgrade paths to WFM 10.0

From version	Instructions
8.5(2), 9.0(1)	Follow the instructions on page 40.
8.3(3), 8.3(4), 8.5(1),	Upgrade to version 8.5(2). Follow the upgrade instructions in the *WFM Installation Guide* for version 8.5(2).

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

NOTE: Installing the upgrade, including running WFM Configuration Setup, takes approximately 30–40 minutes.

To upgrade to WFM 10.0:

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

   NOTE: Do not uninstall the WFM database, but rather just the WFM application itself.

5. Double-click setup_WFM_<Version>.exe, where <Version> is the version number associated with this release (for example, setup_WFM_1001.exe), to start the installation wizard.

6. Follow the instructions in the InstallShield wizard.
7. Configure WFM. For instructions, see "Configuring WFM" on page 43.
8. If present on the server, restart your security software.
9. After installation and configuration, log into WFM as an administrator and test your WFM system to ensure that it is working properly. From the WFM interface, choose Agents > Agents. If the right pane displays a list of agents, the synchronization was successful.

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

Installing Patches

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

Engineering Test

An ET is an 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 an installable component that addresses a specific bug fix needed by a customer. An ES is cumulative. If multiple ESs are issued against a base release, the latest ES contains all the fixes provided in the ESs previously issued.

ESs are installed separately, and each ES appears in the Windows Programs and Features (Add/Remove Programs) utility in Control Panel. This enables each ES to be uninstalled so that it is possible to roll back to a previous state.

Service Release

An SR contains all patches for all bugs found and fixed since the base release of the product. An SR is cumulative. If multiple SRs are issued, the latest SR contains all the fixes in the SRs previously issued.

SRs are installed separately, and each SR appears in the Windows Programs and Features (Add/Remove Programs) utility in Control Panel. This enables each SR to be uninstalled so that it is possible to roll back to a previous state.

Guidelines for Installing a Patch

Consider these guidelines when installing a patch:

- Uninstall an ET before installing an ES or SR. Only one ET can exist on a system at one time. You cannot install an ES or SR until the ET is removed.
- When you install a major, minor, or maintenance upgrade, ETs, ESs, and SRs are automatically removed.

- All but the latest ES and SR can be removed; the Remove button is disabled for all older ESs and SRs.

To install an engineering special or service release:

NOTE: Review "Pre-Installation Considerations" on page 36 before installing an engineering test, engineering special, or service release.

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

Configuring WFM

WFM Configuration Setup Utility

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

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

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

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

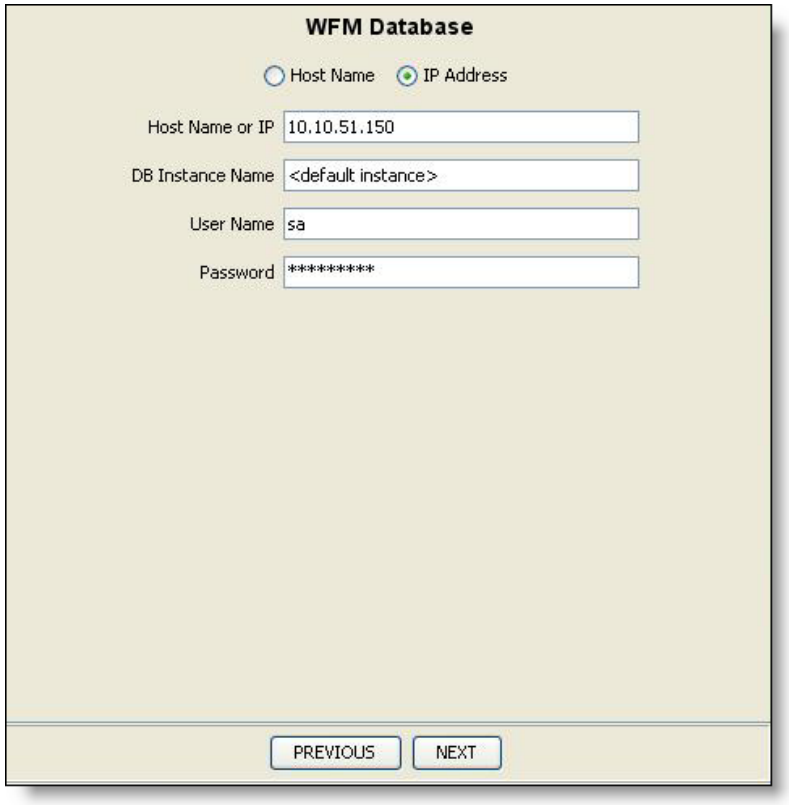
NOTE: Some steps trigger actions and do not display windows that contain fields to be completed.

- WFM Database Step (page 44)
- Create WFM DB—action only. This step creates the WFM database.
- WFM Server Step (page 46)
- Data Retention Step (page 47)
- ACD Connection Step (page 49)
- QM Connection Step (page 51)
- Administrator Password Step (page 52)
- WFM Authentication Step (page 53)
- Email Distribution Step (page 57)
- Monitoring and Notification Step (page 58)
- Start Services—action only. This step starts all the WFM service.
- Finish Configuration—action only. This step configures the WFM Windows registry settings.

WFM Database Step

The WFM Database step (Figure 4) configures access to the WFM database.

Figure 4. WFM Database step



Complete the fields listed in Table 10.

Table 10. WFM Database step fields

Field	Description
Host Name or IP Address	Indicate which format is used for the server name in the Host Name or IP field.
Host Name or IP	The host name or IP address of the server that hosts the WFM database. **NOTE:** You cannot change this setting in Update Mode. If the host name or IP address changes after WFM is configured, you must reinstall WFM.

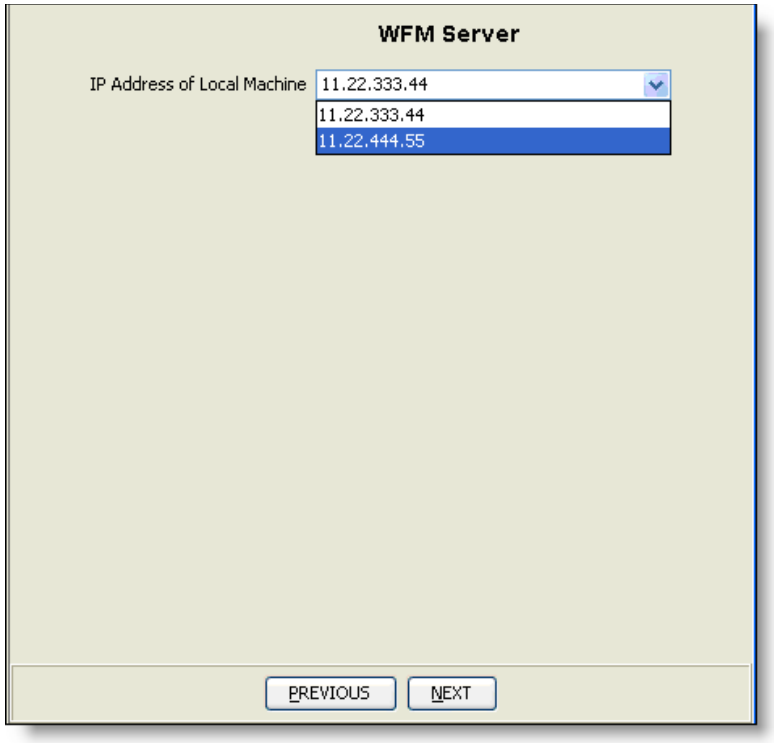
Table 10. WFM Database step fields (cont'd)

Field	Description
DB Instance Name	The WFM database instance name. If this is a new installation of WFM, this field is prepopulated with <default instance>. Use the default value, the named instance, or leave the field blank. Leaving the field blank is the same as using the default instance. **NOTE:** You cannot change this setting in Update Mode. If the WFM database instance name changes after WFM is configured, you must reinstall WFM.
User Name	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" on page 28.
Password	SQL Server user's password.

WFM Server Step

The WFM Server step (Figure 5) configures the IP address of the server where WFM is installed. It appears only if Configuration Setup detects that there is more than one network interface card (NIC) on the server. Select the appropriate public IP address from the drop-down list.

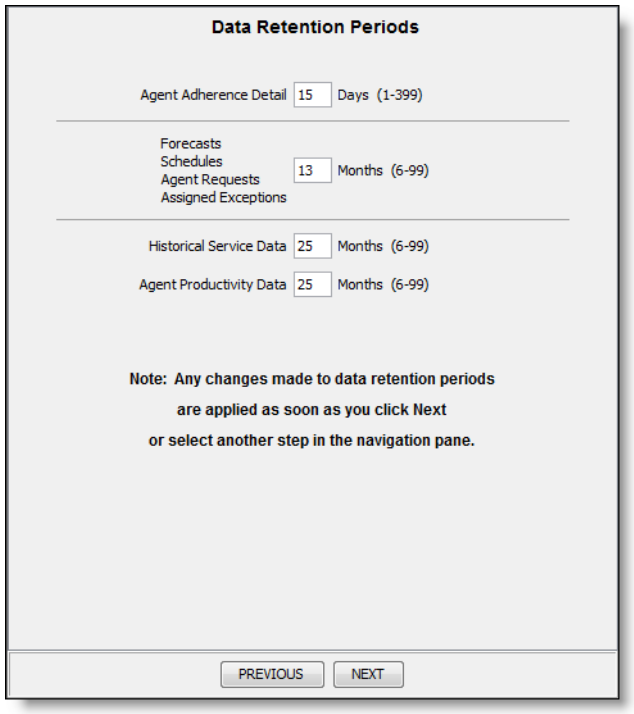
Figure 5. WFM Server step



Data Retention Step

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

Figure 6. Retention Times step



Complete the fields listed in Table 11.

Table 11. Data Retention step fields

Field	Description
Agent Adherence Detail	Value from 1–399 days, with a default of 15 days. Agent adherence detail information is agent state data. **NOTE:** Agent adherence detail data includes every phone state every agent goes into for every day. As a result, the amount of data stored can quickly become very large. The longer the retention period you configure here, the more server space is required to store the data.

Table 11. Data Retention step fields (cont'd)

Field	Description
Forecasts Schedules Agent Requests Assigned Exceptions	Value from 6–99 months, with a default of 13 months. This information is the forecast data, the agent scheduled activity data, the agent requests that are shown in the Messaging application, and the assigned exceptions that are in the Agent Detail Exceptions tab.
Historical Service Data	Value from 6–99 months, with a default of 25 months. This information is all the ACD call data gathered for each contact service queue.
Agent Productivity Data	Value from 6–99 months, with a default of 25 months. This information is the ACD data gathered for each agent.

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 after the ACC service calculates adherence and conformance statistics, which occurs between 04:00 and 04:30.) If the retention period is shortened, all data that exceeds the new retention period is deleted at the next purge. Likewise, if the retention period is extended, no data is purged until the new retention period is exceeded.

- Agent adherence detail data is retained in full days. For example, if the current date is June 15, 2012 and the retention setting is 10 days, then data older than June 5, 2012 will be purged.

  Note that there can be a short time when more than 10 days' worth of data is available. Consider agent adherence detail data that was available as of 01:00 on June 15, 2012. At that time the purge process has not yet run. The last purge was sometime after 04:00 on June 14, so data back to June 4 is still available. Once the June 15 purge runs, the data from June 4 is gone and data is retained from June 5 to the present.

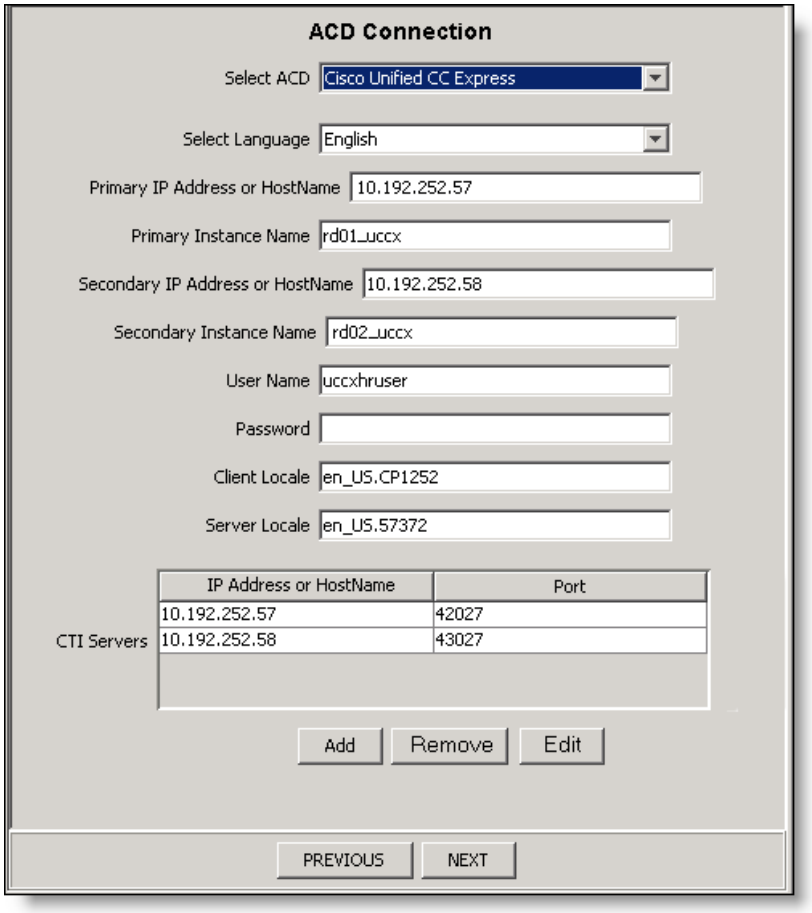
- Agent productivity and historical service data is retained in full months. For example, if the current date is June 15, 2012 and the retention setting is 25 months, then data older than May 1, 2010 will be purged.

- Scheduling and forecasting data is retained in full months, plus any additional days necessary to preserve the schedule week. For example, if the current date is Friday, June 15, 2012, the starting day of the schedule week is configured as Sunday, and the retention time setting is 13 months, then data older than Sunday, April 25, 2011 will be purged, This is because May 1, 2012 is a Saturday, so data is retained for the rest of that schedule week (back through Sunday, April 25, 2011).

ACD Connection Step

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

Figure 7. ACD Connection step



Complete the fields listed in Table 12.

Table 12. ACD Connection step fields

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

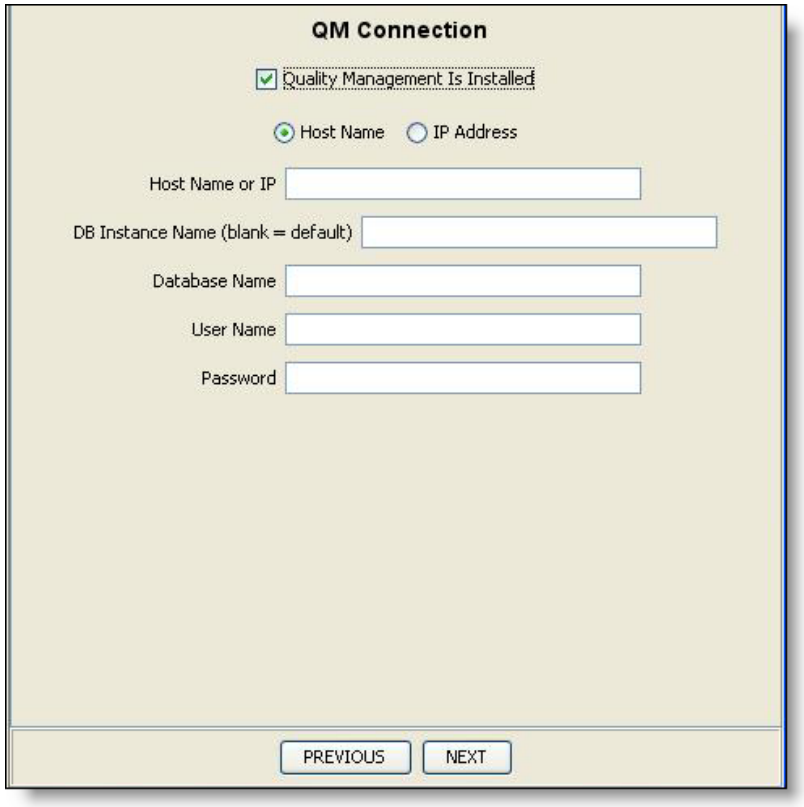
Table 12. ACD Connection step fields (cont'd)

Field	Description
Primary Instance Name	Enter the primary Unified CCX database instance name. This is typically the primary Unified CCX server name (not IP address) followed by "_uccx".
Secondary IP Address or HostName	Enter the ACD's secondary IP address or host name, if this is a redundant system.
Secondary Instance Name	Enter the secondary Unified CCX database instance name. This is typically the secondary Unified CCX server name (not IP address) followed by "_uccx".
User Name	Enter the Unified CCX database user name.
Password	Enter the Unified CCX database user's password.
Client Locale	The client locale that is configured in Unified CCX. The locale for US English appears by default in this field. If the client locale is changed in Unified CCX, then it must also be manually changed in Configuration Setup.
Server Locale	The server locale that is configured in Unified CCX. The locale for US English appears by default in this field. If the server locale is changed in Unified CCX, then it must also be manually changed in Configuration Setup.
CTI Servers	The CTI server(s) and port(s) associated with your system. To add a CTI server to the list, click Add and enter the CTI server hostname or IP address and port, then click OK. You can also edit or delete an existing CTI server and port.

QM Connection Step

NOTE: The QM Connection step (Figure 8) is used if you are using the Quality Management part of the Workforce Optimization suite..

Figure 8. QM Connection step



Complete the fields listed in Table 13.

Table 13. QM Connection step fields

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

Table 13. QM Connection step fields (cont'd)

Field	Description
DB Instance Name	The QM database instance name. Leave this field blank if using the default instance name.
Database Name	The name of the QM database.
User Name	User name with access to the QM database.
Password	User's password.

Administrator Password Step

The Administrator Password step (Figure 9) creates the password used by the WFM administrator to access the application. This step appears only in Initial Mode.

Figure 9. Administrator Password step

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

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

WFM Authentication Step

The WFM Authentication step (Figure 10) configures the shared login with other Workforce Optimization products, the IP address of the Workforce Optimization container, and Active Directory domains, if used in your system.

Figure 10. WFM Authentication step

Complete the fields listed in Table 14.

Table 14. WFM Authentication step fields

Field	Description
Share Login Fields	Select this check box is you want to share login fields in the Workforce Optimization container with other Workforce Optimization products.

Table 14. WFM Authentication step fields (cont'd)

Field	Description
Calabrio One Container	The hostname or IP address of the **WFM 10.0(1) SR1** ■ Bug fixes container. If you are sharing login fields with Monitoring and Recording Services, this must be the Monitoring and Recording Services hostname or IP address.
Use Active Directory	Select this check box if you will be using Active Directory. **NOTE:** You cannot change this setting in Update Mode. If you want to enable or disable Active Directory after WFM is configured, you must reinstall WFM.

Configuring Active Directory Domains

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

To add a domain, click Add to display the Enter Data window (Figure 11).

Figure 11. Enter Data window

Complete the fields listed in Table 15.

Table 15. Active Directory domain Enter Data window fields

Field	Description
Domain Name	The name of the Active Directory domain. This is usually the first part of the Base DN.
IP Address	The IP address of the Active Directory server.
Port	The port used to access the Active Directory server. If you have selected the Use SSL check box, use 636. If you have not selected the Use SSL check box, use 389. **NOTE:** The WFM Transaction services server must be able to access the Active Directory server for user authentication using this port number.
Base DN	The location in the directory server tree under which all Active Directory users are located.

Table 15. Active Directory domain Enter Data window fields (cont'd)

Field	Description
User Base	The path to organizational units (OU) for user records. The path must be specified from the most specific to the least specific (from left to right in the path statement). For example: ou=Users,ou=Minneapolis,ou=Minnesota,ou=US
User Name	The display name as configured in Active Directory of a user with read access to the Active Directory database.
Password	The user's password.
Use SSL	Select this check box if you want to use a Secure Socket Layer (SSL) for the Active Directory.
Certificate File Name	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. **NOTE:** WFM has been tested with certificate files with the extension CER. If the certificate file is not available in the file path specified, WFM AD authentication will fail.

NOTE: The WFM Transaction services server must be able to access the Active Directory server for user authentication using the port number specified in the Enter Data window.

Editing and Deleting Active Directory Domains

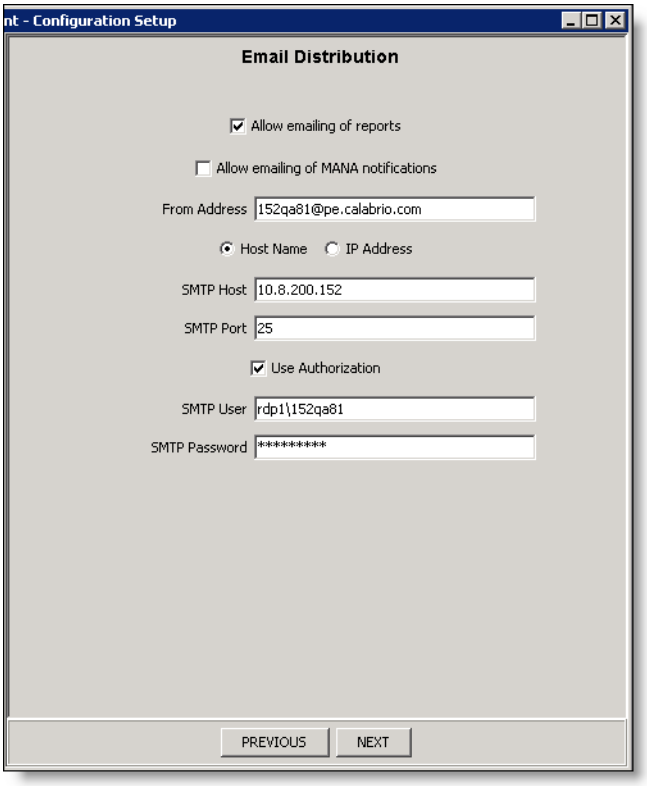
Active Directory domains that have already been added are listed in a table in the WFM Authentication step window. You can edit the information for an existing domain by double-clicking any of the cells in the table and entering new information. When you finish editing the information, click another 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 (Figure 12) configures whether the system uses email to distribute reports and MANA notifications, and the SMTP server settings needed to generate the emails.

Figure 12. Email Distribution step



Complete the fields listed in Table 14.

Table 16. Email Distribution step fields

Field	Description
Allow emailing of reports	Select this check box to use email for sending out reports.
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.

Table 16. Email Distribution step fields (cont'd)

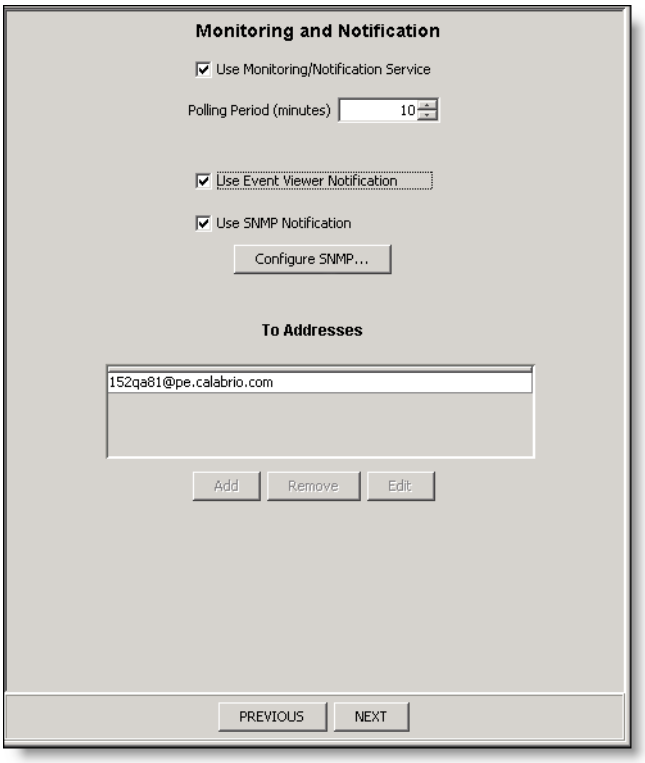
Field	Description
SMTP Host	The host name or IP address of the SMTP server.
SMTP Port	The port used to communicate with the SMTP server.
Use Authorization	Select this check box if authentication is needed to access the SMTP server.
SMTP User	Username required to gain access to the SMTP server.
SMTP Password	Password required to gain access to the SMTP server.

Monitoring and Notification Step

The Monitoring and Notification step (Figure 13) is used to enable the monitoring and notification feature, and to configure the following:

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

Figure 13. Monitoring and Notification step



Complete the fields listed in Table 17.

Table 17. Monitoring and Notification step fields

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

Table 17. Monitoring and Notification step fields (cont'd)

Field	Description
Configure SNMP	Click this button to add an SNMP trap destination. See "Configuring SNMP Notification" on page 60 for more information.
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 base services server.

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

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

To add a trap destination for SNMP notification:

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

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

Verifying the Database Connection to the Unified CCX Database

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

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

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

NOTE: The website address is case sensitive.

The Workforce Management login window appears.

2. Enter `administrator` in the username field and the password that you specified in WFM Configuration Setup (see "Administrator Password Step" on page 52), then click GO or press the Enter key. The Workforce Management window appears.
3. Choose Agents > Agents. If the right pane displays a list of agents, the synchronization was successful.
4. Navigate to C:\Program Files\Cisco\WFO_WFM\log. Open the Capture Service log file. Verify that the log file does not contain any error messages. If there are error messages, correct the errors before proceeding.

Capturing Historical Data

5

Overview

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

> **IMPORTANT:** Your ACD must be configured to capture data at 30-minute intervals just as the Capture service does. If this is not the case, some data is not captured. For example, if your ACD processes data at 15-minute intervals, WFM will capture only half of your data (the data processed every 30 minutes).

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

Capturing Unified CCX Historical Data

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

Removing WFM

6

Overview

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

1. Remove all service releases (see "Rolling Back to a Previous State" on page 66)
2. Remove WFM (see "Removing WFM Services" on page 67)

Rolling Back to a Previous State

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

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

To remove a Workforce Management patch:

1. Log into the WFM server as the local machine administrator.
2. Start the Add or Remove Programs utility in Control Panel.
3. Select the Cisco Unified WFO Workforce Management patch, click Remove Me First, and follow the prompts.

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

NOTE: A reboot might be required when you uninstall an ET, ES, or SR. If you are prompted to reboot, click No. This reboot prematurely terminates background removal activities. You can manually reboot the machine after the removal process is completed..

After the service release is removed, your system is back to its base level software state.

Removing WFM Services

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

> **NOTE:** If there is a service release installed on the Workforce Management server and you want to remove WFM, you must remove the service release before you can remove WFM. See "Rolling Back to a Previous State" on page 66 for more information.

To remove Workforce Management services:

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

Index