



GroupWise 18 Installation Guide

May 2023

Legal Notices

© Copyright 1993 - 2023 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide	11
Part I GroupWise Product Overview	13
1 GroupWise Features and Benefits	15
Essential Communication and Collaboration Services	15
Available Anytime	16
Accessible Anywhere	16
Always Secure	17
Competitive Performance	17
Evaluation Version Available	17
2 GroupWise Components	19
3 GroupWise System Architecture	21
Agent Architecture	21
Administration Service Architecture	22
WebAccess Architecture	23
Calendar Publishing Host Architecture	23
Monitor Architecture	24
Part II GroupWise System Requirements	25
4 GroupWise Server Requirements	27
Hardware and Operating System Requirements	27
Directory Requirements	31
Web Browser Requirements - Administrators	31
Internet Agent Functional Requirements	32
Sample Agent Memory Requirements	32
Sample POA Memory Requirements Based on Post Office Size	33
Sample Memory Requirements for Other GroupWise Agents and Applications	33
5 GroupWise User Requirements	35
GroupWise Client User Requirements	35
GroupWise Web User Requirements	37
GroupWise Web Mobile User Requirements	37
GroupWise WebAccess User Requirements	37
GroupWise WebAccess Mobile User Requirements	37

6	Supported Environments	39
	IPv6 Support	39
	Clustering Support	39
	Virtualization Support.....	39
	Citrix Support	39
	Domain Services for Windows Support.....	40
	File System Support	40
Part III	GroupWise System Creation	41
7	GroupWise System Overview	43
	Simple GroupWise System	43
	Typical GroupWise System.....	44
	GroupWise Users	44
	GroupWise Agents	45
8	Planning Your GroupWise System	47
	Planning GroupWise System Information.....	47
	GroupWise System Name	48
	GroupWise Internet Domain Name	48
	Planning a Domain	48
	Domain Server	49
	Domain Name	49
	Domain Folder	49
	Domain Language	50
	Domain Time Zone.....	50
	Domain Link (Secondary Domain Only)	50
	Agents for the Domain	50
	Administrator Access for Domain Creation	52
	Planning a Post Office.....	53
	Post Office Server	53
	Post Office Name	54
	Post Office Folder.....	54
	Post Office Language.....	54
	Post Office Time Zone	55
	Agents in the Post Office.....	55
	Administrator Access for Post Office Creation	56
	Planning Users.....	57
	Manually Created Users	57
	Imported Users	57
	GroupWise System Worksheets.....	58
	Simple GroupWise System Worksheet.....	58
	Primary Domain Worksheet	61
	Secondary Domain Worksheet.....	62
	Post Office Worksheet.....	63
9	Installing the GroupWise Server Software	65
	Linux: Installing the GroupWise Server Software.....	65
	Preparing the Linux Server for Your GroupWise System	65

Running the Linux GroupWise Installation Wizard	65
Windows: Installing the GroupWise Server Software	66
Preparing the Windows Server	66
Running the Windows GroupWise Installation Wizard	67
10 Creating a Simple GroupWise System	69
11 Creating a Typical GroupWise System	71
Creating the Primary Domain	71
Adding a Secondary Domain	72
Adding a Post Office	73
Handling an Installation Timeout	75
Changing the Authentication Mode for the Installation Console	75
12 Adding Users to Your GroupWise System	77
Manually Adding Users to the Internal GroupWise Directory	77
Importing Users from an LDAP Directory	77
Providing LDAP Directory Information	77
Importing Users	78
Testing the Users	78
13 Working with the GroupWise Administration Console	79
Accessing the Admin Console	79
Making the Most of the System Overview	80
Finding Objects in Object Lists	80
Finding Frequently Used Objects Quickly	81
Working with Objects and Object Properties	81
Using System Tools	81
14 Working with the GroupWise Agents	83
Linux: Managing the GroupWise Agents	83
Manually Starting and Stopping the Linux GroupWise Agents	83
Running the Linux GroupWise Agents as a Non-root User	85
Automatically Restarting the Linux GroupWise Agents with the GroupWise High Availability Service	89
Using the Linux GroupWise Agent Log Files	95
Windows: Managing the GroupWise Agents	96
Manually Starting and Stopping the Windows GroupWise Agents	96
Using the Windows GroupWise Agent Log Files	98
Uninstalling the Windows GroupWise Agents and Applications	98
Monitoring the Agents from Your Web Browser	99

15 What's Next	101
Part IV GroupWise Component Installation and Setup	103
16 Setting Up GroupWise Web	105
GroupWise Web System Requirements	105
Planning Your GroupWise Web Install	105
Installing Docker	106
Installing Docker on SLES 12/15	106
Installing Docker Community on Windows	107
Downloading and Running the Web Configuration Utility	107
Option 1 - Using the Docker Image	107
Option 2 - Using the Micro Focus Download	108
Downloading and Running the GroupWise Web Image	109
Option 1 - Using a Docker Run Command	109
Option 2 - Using the Micro Focus Download Site	110
Upgrading the GroupWise Web Image	111
Securing GroupWise Web with TLS Connections	112
Securing GroupWise Web using a Commercial Certificate	112
Updating POA/DVA Certificates while GroupWise Web is Running	112
Securing GroupWise Web using Certificate Verification	113
17 Setting Up GroupWise WebAccess (Legacy)	115
GroupWise WebAccess Overview	115
GroupWise WebAccess Functionality	115
GroupWise WebAccess Components	116
WebAccess Security Requirements	116
GroupWise WebAccess System Requirements	118
Server Requirements	118
GroupWise Requirements	118
User Requirements	119
Planning GroupWise WebAccess	119
Selecting the WebAccess Application Platform	119
Gathering Web Server Information	120
Determining the WebAccess Application's Configuration	120
Connecting the WebAccess Application with Supporting Agents	121
Installing the GroupWise WebAccess Software	121
Linux: Installing the GroupWise WebAccess Software	121
Windows: Installing the GroupWise WebAccess Software	122
Testing GroupWise WebAccess	124
Testing WebAccess on a Workstation	124
Testing WebAccess on a Tablet Device	124
Testing the WebAccess Basic Interface on a Mobile Device	125
Assisting Users with Login Problems	125
Monitoring the WebAccess Application	125
What's Next	126
GroupWise WebAccess Installation Worksheet	126
18 Setting Up the GroupWise Calendar Publishing Host	127
GroupWise Calendar Publishing Host Overview	127

GroupWise Calendar Publishing Host Functionality	127
GroupWise Calendar Publishing Host Components	128
GroupWise Calendar Publishing Host Security Requirements	128
GroupWise Calendar Publishing Host System Requirements	130
Server Requirements	130
Web Browser Requirements	131
Planning a GroupWise Calendar Publishing Host	131
Selecting the Calendar Publishing Host Application Platform	131
Gathering Web Server Information	132
Choosing the Calendar Publishing Host Name	132
Determining the URL of the Calendar Publishing Host	133
Selecting a Calendar Publishing Host Administrator	133
Connecting the Calendar Publishing Host to a POA	134
Designing Your Calendar Browse List	134
Selecting Calendar Publishing Settings	135
Installing the GroupWise Calendar Publishing Host	135
Linux: Installing the Calendar Publishing Host Software	135
Windows: Installing the Calendar Publishing Host Software	137
Configuring GroupWise to Support the Calendar Publishing Host	138
Configuring the Calendar Publishing Host in the GroupWise Admin Console	138
Enabling Calendar Publishing	139
Configuring a POA for Calendar Publishing	139
Setting Up Calendar Publishing Administration	140
Using the Published Calendar Browse List	141
Testing GroupWise Calendar Publishing	141
Publishing a Personal Calendar	141
Displaying the Browse List of Calendars	142
Publishing Free/Busy Information	142
What's Next	142
GroupWise Calendar Publishing Host Worksheets	142
Calendar Publishing Host Installation Worksheet	143
Calendar Publishing Host Configuration Worksheet	144

19 Setting Up GroupWise Monitor 145

GroupWise Monitor Overview	145
GroupWise Monitor Functionality	145
GroupWise Monitor Components	146
One Monitor Server versus Two	146
Monitor Security Requirements	147
Monitor and the GroupWise High Availability Service on Linux	148
GroupWise Monitor System Requirements	148
Server Requirements	149
Web Browser Requirements	149
Planning GroupWise Monitor	150
Deciding Where to Install the GroupWise Monitor Components	150
Determining the Monitor Agent's Configuration	151
Determining the Monitor Application's Configuration	153
Installing the GroupWise Monitor Software	153
Linux: Installing the GroupWise Monitor Software	153
Windows: Installing the GroupWise Monitor Software	156
Testing GroupWise Monitor	158
Using the Monitor Web Console	158
Using the Monitor Agent Console	158

Using the Windows Monitor Agent Server Console	159
GroupWise Monitor Installation Worksheets	159
GroupWise Monitor Agent Installation Worksheet	159
GroupWise Monitor Application Installation Worksheet	160
20 Setting Up GroupWise Calendar Server	163
GroupWise Calendar Server Overview	163
GroupWise Calendar Server System Requirements	163
Server Requirements	163
Configuration Requirements	164
Planning GroupWise Calendar Server	164
Gathering the Primary Domain Information	164
Gathering the Server Information	164
Specifying the Application Admin	165
Gathering SOAP Information	165
Gathering the Novell Push Notification Certificate	165
Installing the Calendar Server Software	166
Configuring Auto-Discovery of the GroupWise Calendar Server	167
Testing the GroupWise Calendar Server	167
Calendar Server Service Name	167
Testing Calendar Server on a Workstation	167
Troubleshooting Calendar Server Configuration Errors	167
Resolving an Untrusted CA	168
GroupWise Calendar Server Worksheet	169
21 Installing the GroupWise Client	171
GroupWise Client Overview	171
GroupWise Client Workstation Requirements	171
Installing the GroupWise Client	172
Installing the GroupWise Client	172
Implementing System-Wide GroupWise Client Rollouts	173
Starting the Groupwise Client	174
What's Next	174
22 Using Other Micro Focus Products with GroupWise	175
Using the GroupWise Mobility Service to Synchronize GroupWise Data to Mobile Devices	175
Using GroupWise Messenger to Provide Secure Instant Messaging for GroupWise Users	175
Using Micro Focus Vibe to Provide Team Workspaces for GroupWise Users	176
Using GroupWise Teamworks to Provide Team Workspaces for GroupWise Users	176
Part V GroupWise System Upgrade	177
23 What's New in GroupWise 18	179
24 Understanding the Upgrade Process	181
Domain and Post Office Upgrades	182
Agent Upgrades	183

Monitor Upgrades	183
WebAccess Upgrades	184
Calendar Publishing Host Upgrades	184
GroupWise Client Upgrades	184
Obsolete eDirectory Schema Extensions	184
Obsolete Software Distribution Directories	185
Obsolete GroupWise Gateways	185
NetWare Compatibility	185
 25 Preparing Your Existing GroupWise System for the Upgrade	 187
 26 Installing the GroupWise 18 Software	 189
Linux: Installing the GroupWise 18 Software	189
Windows: Installing the GroupWise 18 Software	190
 27 Upgrading the Primary Domain Server	 193
 28 Upgrading a Secondary Domain Server	 197
 29 Upgrading a Post Office Server	 201
 30 Upgrading GroupWise Agents and Applications	 203
Upgrading the Document Viewer Agent	203
Upgrading GroupWise WebAccess	203
Preparing to Upgrade the WebAccess Application	204
Installing the GroupWise 18 WebAccess Application	204
Clearing User Browser Caches to Display GroupWise 18 WebAccess Correctly	205
Upgrading the Calendar Publishing Host	205
Installing the GroupWise 18 Calendar Publishing Host Application	205
Clearing User Browser Caches to Display Published Calendars Correctly	206
Upgrading GroupWise Monitor	206
Preparing to Upgrade GroupWise Monitor	206
Installing the Monitor Software	206
Clearing Browser Caches to Display GroupWise 18 Monitor Correctly	207
Reconfiguring the GroupWise High Availability Service	207
Implementing TLS Encryption	207
 31 Upgrading Users' GroupWise Client Software	 209
 32 Transitioning from ConsoleOne	 211
 Part VI Appendixes	 213
 A GroupWise Version Compatibility	 215
GroupWise 18 with Earlier GroupWise Versions	215
Compatibility with GroupWise 2012	215

Compatibility with GroupWise 8	217
GroupWise 18 in a Cross-Platform Environment	218
GroupWise 18 Administrative Components and Databases	219
GroupWise 18 Agents on Linux and Windows	219
B Attributes, Operators, and Values for Object Filters	221
Attributes	221
Logical Operators	222
Grouping Operators	223
Wildcard Characters	223
Literal Values	223
Date Specifications	224
C Invalid Characters in GroupWise Object Names and Email Addresses	225
Invalid Characters in GroupWise Object Names	225
Invalid Characters in Internet Email Addresses	225
D Cross-Platform Connections	227
Setting up Samba on OES	227
Configuring NetWare Core Protocol (NCP)	227
Installing Samba	228
Logging In to iManager	228
Creating a User to Manage the Samba Share	228
Configuring the eDirectory Universal Password for Samba	229
Setting the eDirectory Universal Password for the Samba Administrator User	229
Creating a Samba Share	229
Setting the eDirectory Rights for the Samba Share	230
Testing Samba on the OES Server	230
Mapping a Drive to a Samba Share on an OES Server	230
Setting Up Samba on SLES	231
Preparing Your Firewall to Allow Samba Connections	231
Configuring the Samba Server	231
Configuring the Samba Web Administration Tool (SWAT)	232
Accessing SWAT	232
Setting the Samba User Name and Password	232
Creating a Samba Share	233
Mapping a Drive to a Samba Share on a SLES Server	233

About This Guide

The *GroupWise 18 Installation Guide* helps you install a new GroupWise system or upgrade an existing GroupWise 8 or 2012 system to GroupWise 18.

Latest Version

For the latest version of the GroupWise installation guide, see [GroupWise 23.4 Installation Guide](#).

The following resources provide additional information about using GroupWise 18:

- ♦ [Micro Focus Support and Knowledge Base](#)
- ♦ [GroupWise Support Community](#)

Audience

This guide is intended for network administrators who install and administer GroupWise.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation.

Additional Documentation

For additional GroupWise documentation, see the [Micro Focus GroupWise 18 Documentation website](#).

GroupWise Product Overview

Micro Focus GroupWise is an enterprise collaboration system that provides the following secure services:

- ♦ Email
- ♦ Calendaring
- ♦ Scheduling
- ♦ Task management
- ♦ Contact management
- ♦ Document management
- ♦ Additional productivity tools

Companion products provide additional capabilities:

- ♦ **GroupWise Mobility Service:** Synchronization of GroupWise data to mobile devices
- ♦ **GroupWise Messenger:** Secure instant messaging
- ♦ **Micro Focus Vibe:** Team workspaces, document management, and other collaboration tools

GroupWise 18 can be used in a variety of environments:

- ♦ **Your Windows Desktop:** Windows 10 and Windows 11
- ♦ **Web Browsers:** Mozilla Firefox, Google Chrome, and Microsoft Internet Explorer
- ♦ **Tablets:** Apple, Android, Kindle, and RIM
- ♦ **Mobile Devices:** Apple, Android, BlackBerry, and Windows

The following sections include more details about the benefits that GroupWise provides and the steps you need to perform to set up your GroupWise system to best meet your users' needs.

- ♦ [Chapter 1, "GroupWise Features and Benefits," on page 15](#)
- ♦ [Chapter 2, "GroupWise Components," on page 19](#)
- ♦ [Chapter 3, "GroupWise System Architecture," on page 21](#)

1 GroupWise Features and Benefits

GroupWise provides communication and collaboration services that are secure, highly available, and easily accessible:

- ♦ [“Essential Communication and Collaboration Services” on page 15](#)
- ♦ [“Available Anytime” on page 16](#)
- ♦ [“Accessible Anywhere” on page 16](#)
- ♦ [“Always Secure” on page 17](#)
- ♦ [“Competitive Performance” on page 17](#)
- ♦ [“Evaluation Version Available” on page 17](#)

Essential Communication and Collaboration Services

GroupWise provides a variety of tools to enable users to work together and to work smarter:

- ♦ **Messaging:** Send and receive mail messages, phone messages, and reminder notes. A mail message is for general correspondence. A phone message is for those who take phone messages for others. A reminder note includes a start date and, when accepted by the recipient, is posted to the recipient’s Calendar.
- ♦ **Scheduling:** Schedule both appointments and tasks. When you schedule an appointment, you can search other users’ Calendars to find free times for the appointment. When you schedule a task, you can assign a priority and due date to the task. If the recipient accepts an appointment or task, it is automatically added to his or her Calendar.
- ♦ **Calendaring:** View and manage your appointments, tasks, and reminder notes in a Calendar view. You can create multiple calendars. You can create multi-user calendars. You can also publish calendars and free/busy status to the web so that non-GroupWise users can conveniently schedule meetings with you.
- ♦ **Task Management:** Create and schedule tasks for others. Accept or decline the tasks you receive, and track accepted tasks through to completion. You can turn any message into a task. You can also organize, schedule, and monitor tasks in your Tasklist folder.
- ♦ **Contact Management:** Manage information for your contacts, groups, resources, and organizations, including being able to view, update, delete, and add information to the contacts in your personal address books and Contacts folders. In addition, you can view a history of messages sent to and received from individual contacts, and compile notes on interactions with contacts.
- ♦ **Document Management:** Store documents in GroupWise libraries. In a library, documents, are compressed to save disk space and encrypted to maintain security. With document management, you can check in, check out, share, and create multiple versions of documents.
- ♦ **Mobile Device Synchronization:** Receive and respond to GroupWise messages, appointments, tasks, and notes on your mobile device. You can also send new items of all types and manage contacts on your mobile device.

- ♦ **Instant Messaging:** Communicate in real time with other GroupWise users through GroupWise Messenger. Messenger lets you know when other users are online, busy, or away from their desks and displays this status in the GroupWise client. Messenger also enables you to save conversations.
- ♦ **Teaming:** Collaborate on a Micro Focus Vibe website where personal, team, and global workspaces can include discussion folders, shared calendars, shared documents, blogs, wikis, surveys, and more. Powerful search capabilities make finding information quick and easy. GroupWise includes integration with Vibe, so you can access a Vibe site from the GroupWise client.

Available Anytime

GroupWise ensures that your essential communication tools are always available:

- ♦ **Caching:** The GroupWise client includes a Caching mode that allows you to cache GroupWise information to your local drive and continue to work even when you are not logged in to your Online mailbox.
- ♦ **LDAP Pooling:** If you are using LDAP authentication for GroupWise mailbox authentication, LDAP pooling ensures that there is always an LDAP server through which authentication can be performed.
- ♦ **Clustering:** To ensure that GroupWise data is always available and GroupWise components are always running, you can install GroupWise in a cluster on Linux or Windows.

Accessible Anywhere

GroupWise lets you communicate and collaborate with other people by using the device that is most convenient:

- ♦ **Personal Computers:** To access your GroupWise mailbox with the most robust functionality, you can run the GroupWise client on any workstation that uses Windows 10 or 11.
- ♦ **Web Browsers:** When you are away from your office, or when you prefer a platform other than Windows, you can access your GroupWise mailbox from a variety of desktop web browsers by using GroupWise WebAccess.
- ♦ **Tablet Computers:** For those who prefer a more mobile computer, you can access your GroupWise mailbox from a tablet computer by using GroupWise WebAccess Mobile.
- ♦ **Mobile Devices:** If you want to access email messages, calendar items, tasks, and so on from a handheld mobile device such as your cell phone, you have several options:
 - ♦ **GroupWise Mobility Service:** The GroupWise Mobility Service, available free of charge to GroupWise customers with maintenance contracts, synchronizes GroupWise data to most popular mobile devices.
 - ♦ **BlackBerry Enterprise Server for GroupWise:** This solution from Research in Motion provides synchronization of GroupWise data for BlackBerry users with devices that are older than the BlackBerry Z10. Newer BlackBerry devices are fully supported by the GroupWise Mobility Service.
 - ♦ **GroupWise WebAccess Basic Template:** GroupWise WebAccess includes a basic template customized for use on the small display available on a typical mobile device.

NOTE: GroupWise WebAccess Mobile is intended for use on tablets, not on smaller mobile devices such as cell phones.

- ♦ **Other Email Clients:** GroupWise enables you to access your mailbox with any POP3, IMAP4, or SOAP email client.

Always Secure

GroupWise provides extensive security measures to protect your information:

- ♦ **Native GroupWise Encryption:** To protect your information as it is stored in the various GroupWise databases and moved across the network, GroupWise automatically encrypts the information. Each piece of information is encrypted differently through the use of randomly generated encryption keys.
- ♦ **Open Security Standards:** To further ensure that your information is secure while moving across your internal network and across the Internet, GroupWise supports open security standards such as Secure Sockets Layer (TLS), Secure Multipurpose Internet Mail Extension (S/MIME), Public Key Infrastructure (PKI), and Transport Layer Security (TLS).
- ♦ **Spam Protection:** To protect you from seeing unwanted messages, the GroupWise client includes a Junk Mail Handling feature that lets you control unwanted Internet email messages. In addition, you can configure the GroupWise Internet Agent (GWIA) to reject messages from known open relay hosts and spam hosts. GroupWise also works with partner products that provide additional anti-spam solutions.
- ♦ **Virus Protection:** GroupWise works with partner products to provide solutions that detect and eliminate viruses.

For information about additional security solutions available for GroupWise through GroupWise partners, see the [Micro Focus Partner Product Guide \(http://www.novell.com/partnerguides/\)](http://www.novell.com/partnerguides/).

Competitive Performance

GroupWise functionality compares very favorably with popular email solutions. For more information, see <https://www.microfocus.com/products/groupwise/features/>.

Evaluation Version Available

An evaluation version of GroupWise is available on the [Micro Focus Downloads website \(https://www.novell.com/products/groupwise/download/\)](https://www.novell.com/products/groupwise/download/). With the evaluation version of GroupWise, you can create a GroupWise system that includes any number of domains, post offices, and users. The evaluation version expires after 60 days. If you want to use GroupWise past the evaluation period, you must configure a GroupWise license. For more information about licensing, see “[Licensing](#)” in the *GroupWise 18 Administration Guide*.

2 GroupWise Components

GroupWise includes multiple components that you need to install to realize the full benefits of GroupWise. However, some components might not be necessary, depending on your needs. The following table outlines the components, what they provide, and where to find instructions for installing them.

Component	What it does	Go to
GroupWise Server: <ul style="list-style-type: none">♦ Administration Service♦ Message Transfer Agent♦ Post Office Agent♦ Internet Agent♦ Document Viewer Agent	Required for any GroupWise system. These components must be installed before any other components.	Creating a Simple GroupWise System Creating a Typical GroupWise System
WebAccess WebAccess Mobile	Provides access to mailboxes through desktop web browsers, tablet computers, and mobile devices.	Setting Up GroupWise WebAccess (Legacy)
Calendar Publishing Host	Provides web-based public access to GroupWise calendars and free/busy availability to Internet users.	Setting Up the GroupWise Calendar Publishing Host
Monitor	Provides administrative monitoring of the GroupWise agents.	Setting Up GroupWise Monitor
GroupWise Client	Provides access to mailboxes from the Windows desktop; can be easily rolled out to all GroupWise users on a convenient schedule.	Installing the GroupWise Client

In addition to the sections referenced in the above table, this *Installation Guide* includes the following supplemental sections:

- ♦ [Using the GroupWise Mobility Service to Synchronize GroupWise Data to Mobile Devices](#)
- ♦ [Using GroupWise Messenger to Provide Secure Instant Messaging for GroupWise Users](#)
- ♦ [Using Micro Focus Vibe to Provide Team Workspaces for GroupWise Users](#)

The information in these sections is provided as a reference for installing additional products after you have created your GroupWise system.

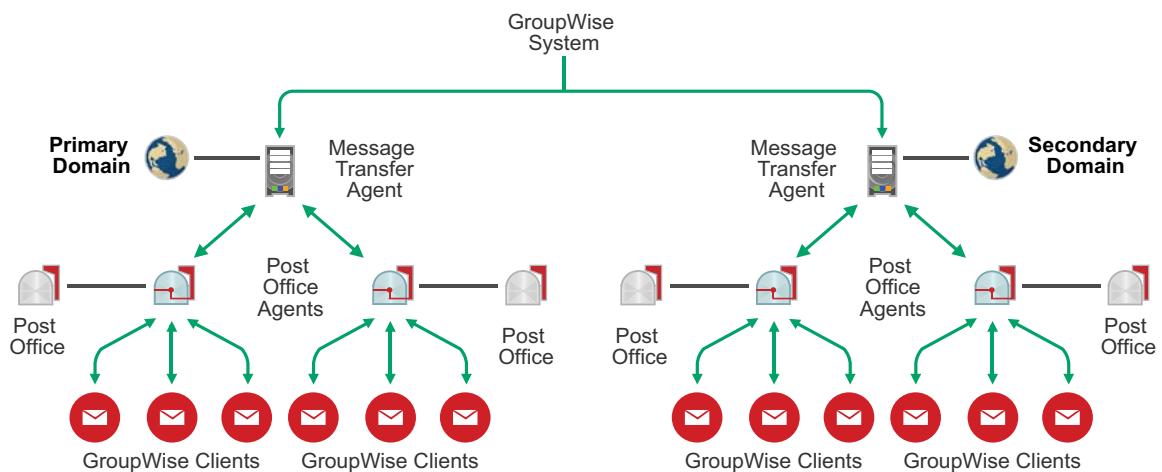
3 GroupWise System Architecture

Your GroupWise system consists of multiple components. The better you understand each component, the more effectively you can manage your GroupWise system.

- ♦ [“Agent Architecture” on page 21](#)
- ♦ [“Administration Service Architecture” on page 22](#)
- ♦ [“WebAccess Architecture” on page 23](#)
- ♦ [“Calendar Publishing Host Architecture” on page 23](#)
- ♦ [“Monitor Architecture” on page 24](#)

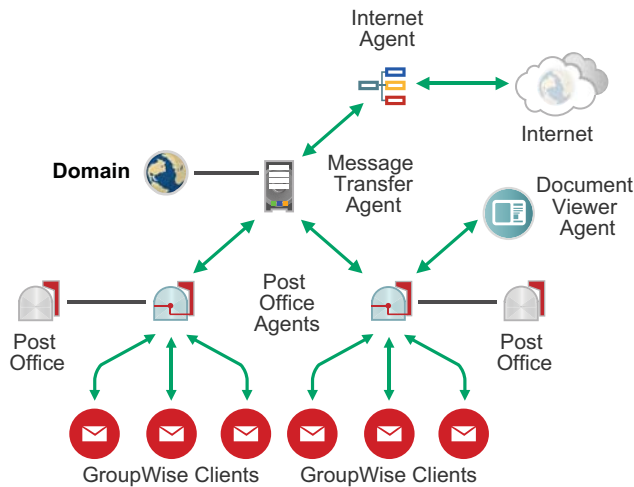
Agent Architecture

The GroupWise agents move email throughout your GroupWise system, as well as to and from the Internet.



The Post Office Agent (POA) runs for each post office. The POA delivers email to users' mailboxes. The Message Transfer Agent (MTA) runs for each domain. The MTA transfers email between post offices and other domains.

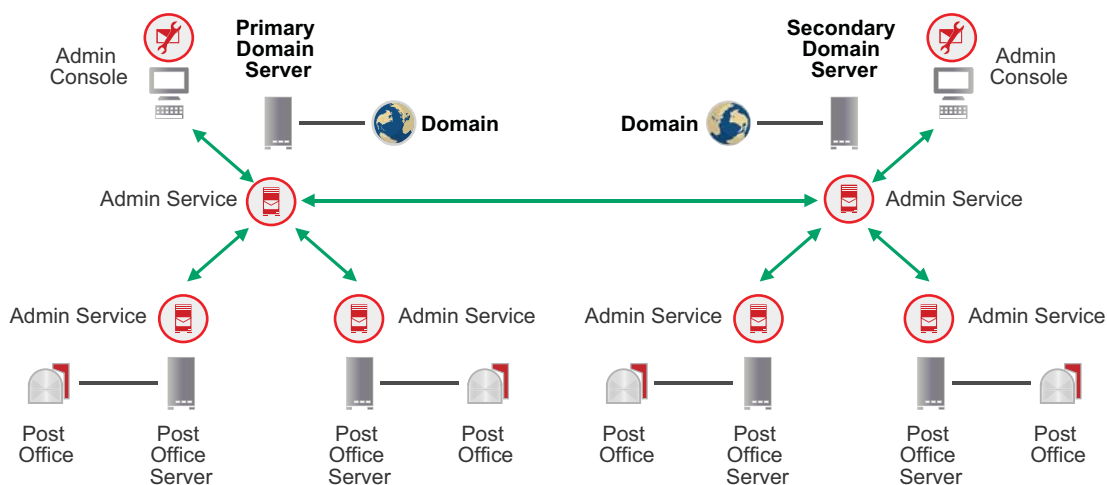
The Internet Agent (GWIA) runs for at least one domain in your GroupWise system. The GWIA communicates with SMTP hosts across the Internet, sending and receiving email for users who are not part of your GroupWise system.



The Document Viewer Agent (DVA) runs for at least one post office. The DVA converts attached document files from a wide variety of formats into HTML format for indexing by the POA and for viewing in GroupWise WebAccess.

Administration Service Architecture

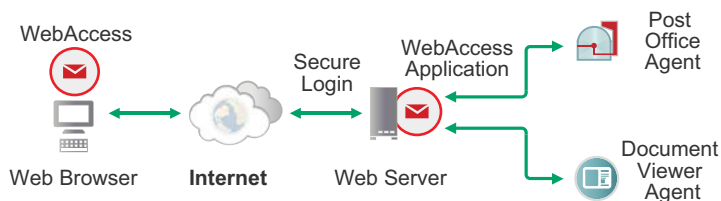
The GroupWise Administration Service provides the GroupWise Administration console in your web browser. The Admin console provides the global view of your GroupWise system. It enables you to configure and customize all GroupWise objects (Domain, Post Office, User, MTA, POA, GWIA, DVA, and so on). It also provide a number of administrative tools for managing your GroupWise system.



The Admin Service runs on each domain server and post office server. The Admin Service communicates with Admin Services on other GroupWise servers and with the agents that run on its local server. You can access the Admin console on any domain server. For post office access, you access the Admin console for the domain that owns the post office.

WebAccess Architecture

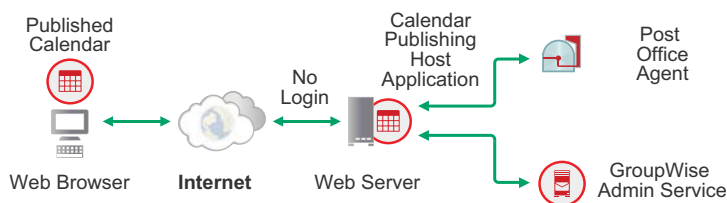
WebAccess enables GroupWise users to access their mailboxes from their web browser.



Externally, the WebAccess Application, which integrates with your web server, communicates with the user's web browser across the Internet. Internally, the WebAccess Application communicates with the Post Office Agent (POA) to request mailbox data and with the Document Viewer Agent (DVA) for conversion of attached documents into HTML for viewing.

Calendar Publishing Host Architecture

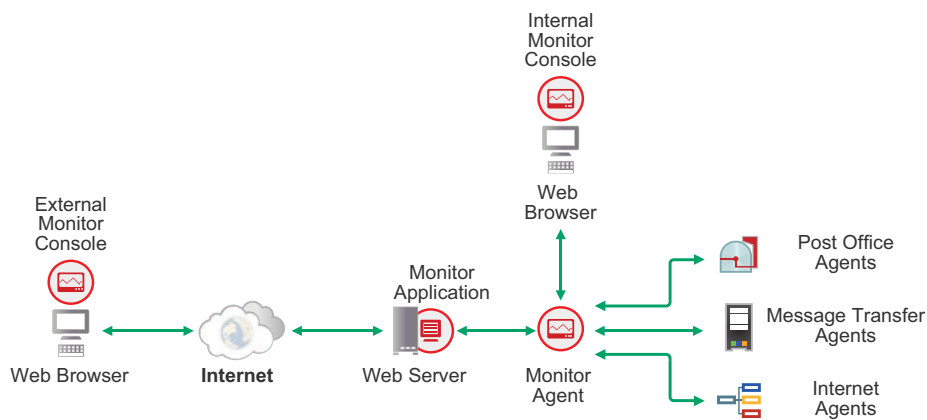
The Calendar Publishing (CalPub) Host enables GroupWise users and non-GroupWise users to view GroupWise users' calendars from their web browser.



Externally, the CalPub Host Application, which integrates with your web server, communicates with the user's web browser across the Internet. Internally, the CalPub Host Application communicates with the Post Office Agent (POA) to request calendar data from the user's mailbox. The CalPub Host requires access to an LDAP server such as NetIQ eDirectory or Microsoft Active Directory for administrator authentication to the CalPub Admin console.

Monitor Architecture

Monitor enables you to monitor the GroupWise agents from your web browser when you are not working behind your firewall.



Internally, the Monitor Agent gathers status information from GroupWise agents. Externally, the Monitor Application, which integrates with your web server, communicates with your web browser across the Internet to provide a Monitor console that is available outside your firewall. The Monitor Agent also provides its own internal Monitor console independent of your web server, which is available inside your firewall.



GroupWise System Requirements

You, as a GroupWise administrator, must ensure that your system meets GroupWise system requirements, so your GroupWise system can be set up successfully. After your GroupWise system is set up, you must ensure that users' workstations meet GroupWise client requirements, so users can run the GroupWise clients successfully.

- ♦ [Chapter 4, "GroupWise Server Requirements," on page 27](#)
- ♦ [Chapter 5, "GroupWise User Requirements," on page 35](#)
- ♦ [Chapter 6, "Supported Environments," on page 39](#)

4 GroupWise Server Requirements

Refer to these sections for server related requirements.

- ♦ [“Hardware and Operating System Requirements” on page 27](#)
- ♦ [“Directory Requirements” on page 31](#)
- ♦ [“Web Browser Requirements - Administrators” on page 31](#)
- ♦ [“Internet Agent Functional Requirements” on page 32](#)
- ♦ [“Sample Agent Memory Requirements” on page 32](#)

Hardware and Operating System Requirements

The requirements listed below are the base server requirements for the GroupWise Domain and agents (Post Office Agent, Message Transfer Agent, Document Viewer Agent, Internet Agent, and Monitor Agent). Other agents might have additional requirements. See [GroupWise Component Installation and Setup](#) for these additional agent requirements.

- ❑ x86-64 bit processor
- ❑ Use the following OS support matrix to know what OS is supported for your version of GroupWise:

GroupWise Version	Supported Operating Systems	Added in this Version	Removed in this Version
GW 18.0	<ul style="list-style-type: none">♦ SLES 11, 12, or 15 with the latest support pack♦ OES 11, 2015, or 2018 with the latest support pack♦ Windows Server 2012 R2 or Windows Server 2016 with the latest support pack		
GW 18.1	<ul style="list-style-type: none">♦ SLES 11, 12, or 15 with the latest support pack♦ OES 2015 or 2018 with the latest support pack♦ Windows Server 2012 R2 or Windows Server 2016 with the latest support pack		<ul style="list-style-type: none">♦ OES 11

GroupWise Version	Supported Operating Systems	Added in this Version	Removed in this Version
GW 18.1.1	<ul style="list-style-type: none"> ◆ SLES 11, 12, or 15 with the latest support pack ◆ OES 2015 or 2018 with the latest support pack ◆ Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 with the latest support pack 	<ul style="list-style-type: none"> ◆ OES 2018 SP1 ◆ Windows Server 2019 	
GW 18.2	<ul style="list-style-type: none"> ◆ SLES 12 or 15 with the latest support pack ◆ OES 2018 with the latest support pack ◆ Windows Server 2016 or Windows Server 2019 with the latest support pack 		<ul style="list-style-type: none"> ◆ SLES 11 ◆ OES 2015 ◆ Windows Server 2012 R2
GW 18.3	<ul style="list-style-type: none"> ◆ SLES 12 or 15 with the latest support pack ◆ OES 2018 with the latest support pack ◆ Windows Server 2016 or Windows Server 2019 with the latest support pack 		
GW 18.4	<ul style="list-style-type: none"> ◆ SLES 12 or 15 with the latest support pack ◆ OES 2018 with the latest support pack ◆ Windows Server 2016, Windows Server 2019 with the latest support pack, or Windows Server 2022 	<ul style="list-style-type: none"> ◆ Windows Server 2022 	

GroupWise Version	Supported Operating Systems	Added in this Version	Removed in this Version
GW 18.4.1	<ul style="list-style-type: none"> ◆ SLES 12 SP5 or SLES 15 SP4 ◆ OES 2018 with the latest support pack ◆ Windows Server 2016, Windows Server 2019 with the latest support pack, or Windows Server 2022 		
GW 18.4.2	<ul style="list-style-type: none"> ◆ SLES 12 SP5 or SLES 15 SP4 ◆ OES 2018 SP3 or 2023 <p>IMPORTANT: If Calendar Server is not starting, check to see if it has a port conflict with another service. You may have to change the default port of 443.</p> <p>For information, see Changing the Default Port on GroupWise Calendar Server.</p> <ul style="list-style-type: none"> ◆ Windows Server 2016, 2019, or 2022 	<ul style="list-style-type: none"> ◆ OES 2023 	

GroupWise Version	Supported Operating Systems	Added in this Version	Removed in this Version
GW 18.5	<ul style="list-style-type: none"> ♦ SLES 12 SP5 or SLES 15 SP4 ♦ OES 2018 SP3 or 2023 <p>IMPORTANT: If Calendar Server is not starting, check to see if it has a port conflict with another service. You may have to change the default port of 443.</p> <p>For information, see Changing the Default Port on GroupWise Calendar Server.</p> <ul style="list-style-type: none"> ♦ Windows Server 2016, 2019, or 2022 		

NOTE: By default, the GroupWise Linux agents run as services without user interfaces. Running Linux agents with a user interface is not supported.

IMPORTANT: When installing on SLES 15, the following modules and extensions must be installed before installing GroupWise:

- ♦ Base system
- ♦ Desktop Applications
- ♦ Legacy
- ♦ Server Applications
- ♦ Web & Scripting (for WebAccess, CalPub, Monitor, and CalServer)

For more information on modules and extensions on SLES 15, see SUSE documentation, [Modules & Extensions Quick Start](#).

- ☐ Adequate server memory as required by the operating system

Depending on the anticipated load on the GroupWise agents, additional memory might be required. For details, see [Sample Agent Memory Requirements](#).

- ☐ Adequate server disk space as required by each GroupWise component:

- ♦ **Domain Folder:** 100-200 MB for the domain database, plus 1 GB or more for message queues when links are down
- ♦ **Post Office Folder:** 5 MB per user (minimum); 100 MB or more per user (recommended); plus 100-300 MB for the post office database; plus 500 MB or more for message queues when links are down

- ♦ **GroupWise Server Installation:** Approximately 885 MB (GroupWise Administration Service, Message Transfer Agent, Post Office Agent, Internet Agent, and Document Viewer Agent combined; varies by platform)
For additional Internet Agent requirements, including Internet connectivity requirements, see [Internet Agent Functional Requirements](#).
- ♦ **WebAccess Installation:** Approximately 525 MB (shared with the Calendar Publishing Host Application and the Monitor Application when they are installed on the same web server; varies by platform)
- ♦ **Calendar Publishing Host Installation:** Approximately 525 MB (shared with the WebAccess Application and the Monitor Application when they are installed on the same web server; varies by platform), plus 50 KB per published calendar and 50 KB per user for free/busy searching
- ♦ **Monitor Installation:** Approximately 40 MB for the Monitor Agent (varies by platform); approximately 525 MB for the Monitor Application (shared with the WebAccess Application and the Calendar Publishing Host Application when they are installed on the same web server; varies by platform)

Directory Requirements

One or more of the following directories:

- ☐ Micro Focus eDirectory 9.1 or later, with LDAP enabled (optional)

You can download eDirectory from the [Micro Focus Downloads site \(http://download.novell.com\)](http://download.novell.com).

- ☐ Microsoft Active Directory (optional)
- ☐ Native GroupWise directory (internal; required)

Web Browser Requirements - Administrators

Any of the following web browsers for the GroupWise Administration console and agent consoles:

- ☐ Linux: Mozilla Firefox; Google Chrome
- ☐ Windows: Mozilla Firefox; Microsoft Edge with Chromium Edge; Google Chrome
- ☐ Macintosh: Mozilla Firefox; Google Chrome; Safari

NOTE: The web browser requirements for GroupWise WebAccess are different from the web browser requirements for the Admin and agent consoles. For those user requirements, see [GroupWise WebAccess User Requirements](#).

The Admin and agent consoles are not supported on tablet devices. For those user requirements, see [GroupWise WebAccess Mobile User Requirements](#).

Internet Agent Functional Requirements

The following additional requirements apply when you install the Internet Agent:

The GroupWise system in which you install the Internet Agent (GWIA) must meet the following requirements:

- ☐ The domain's version must be equal to or later than the GWIA's version. The domain's version is determined by the Message Transfer Agent (MTA) version running for it.
- ☐ The versions of any post offices that the GWIA accesses on behalf of POP3 or IMAP4 clients must be equal to or later than the GWIA's version. A post office's version is determined by the Post Office Agent (POA) version running for it.
- ☐ The POA and MTA need to be accessible to the GWIA for IMAP, POP, and ICAL.

Before you install the Internet Agent (GWIA), ensure that your network is configured for Internet connectivity.

- ☐ **Internet Connection:** You can connect to the Internet by using a direct connection over a leased line or a standard switched telephone line.
- ☐ **Internet Domain Name:** You must have an Internet domain name. The domain name must be defined by an MX RR (mail exchanger resource record) in DNS.
- ☐ **DNS Server Access or Relay Host Access:** If you want the GWIA to send messages directly to other SMTP hosts, it requires access to a DNS server for address resolution. Otherwise, it requires access to a relay host that can perform the address resolution and message routing. Ensure the server where you plan to install the GWIA is configured to access a DNS server or can access your relay host. For specific details, refer to your server documentation.
- ☐ **IP Address:** The GWIA's server requires a static IP address and a fully qualified DNS hostname.

Sample Agent Memory Requirements

The sections below have memory requirements for Post Office and other GroupWise agents.

- ♦ [“Sample POA Memory Requirements Based on Post Office Size” on page 33](#)
- ♦ [“Sample Memory Requirements for Other GroupWise Agents and Applications” on page 33](#)

Sample POA Memory Requirements Based on Post Office Size

The amount of memory used by the POA depends on the number of active users, as illustrated by the table below. The POA typically performs best with abundant cache memory available. Be aware that these are just recommendations. Several different environment and enterprise variables can affect memory requirements

Concurrent Users	Minimum Memory Required	Recommended Memory for Best Performance
100 active users (100-250 users in post office)	4 GB	12 GB
250 active users (250-500 users in post office)	6 GB	16 GB
500 active users (500-1000 users in post office)	8 GB	32 GB
1000 active users (1000 - 1500 users in post office)	12 GB	48 GB
1500 active users (1500 - 3000 users in post office)	16 GB	64 GB

Sample Memory Requirements for Other GroupWise Agents and Applications

Agent/Application	Minimum Memory Required	Recommended Memory for Best Performance
Routing MTA	4 GB	12 GB
DVA	2 GB	4 GB
GWIA and its MTA	4 GB	16 GB
Monitor	2 GB	8 GB
WebAccess Application	400 MB	4 GB
Calendar Publishing Host Application	2 GB	4 GB
Calendar Server (CalDAV and CardDAV)	4 GB	12 GB or higher

5 GroupWise User Requirements

GroupWise client and web requirements are in these sections.

- ♦ “GroupWise Client User Requirements” on page 35
- ♦ “GroupWise Web User Requirements” on page 37
- ♦ “GroupWise Web Mobile User Requirements” on page 37
- ♦ “GroupWise WebAccess User Requirements” on page 37
- ♦ “GroupWise WebAccess Mobile User Requirements” on page 37

GroupWise Client User Requirements

Generally, the following points apply:

- ❑ x86-32 processor or x86-64 processor
 - On a 64-bit processor, GroupWise still runs as a 32-bit application.
- ❑ Any of the following desktop operating systems for the GroupWise client:
 - ♦ Windows 7 on a 1 GHz or higher workstation with at least 1 GB of RAM
 - ♦ Windows 8 or Windows 8.1 on a 1 GHz or higher workstation with at least 1 GB of RAM
 - ♦ Windows 10 on a 1 GHz or higher workstation with at least 1 GB of RAM
 - ♦ Windows 11 on a 1 GHz or higher workstation with at least 1 GB of RAM
- ❑ Microsoft Internet Explorer 9 or later
- ❑ Approximately 200 MB of free disk space on each user’s workstation to install the GroupWise client.

The following is a summary of release-specific details.

GroupWise Version	Workstation Requirements	Added in this Version	Removed in this Version
GW 18.0	<ul style="list-style-type: none">♦ Windows 7, 8.1, and 10 contingent on Microsoft support♦ 1 GHz or higher x86-32 or x86-64 processor (32-bit application only)♦ 1 GB RAM♦ 200 MB free disk space		

GroupWise Version	Workstation Requirements	Added in this Version	Removed in this Version
GW 18.1	<ul style="list-style-type: none"> ♦ Windows 7, 8.1, and 10 contingent on Microsoft support ♦ 1 GHz or higher x86-32 or x86-64 processor (32-bit application only) ♦ 1 GB RAM ♦ 200 MB free disk space 		
GW 18.2	<ul style="list-style-type: none"> ♦ Windows 8.1 and 10 contingent on Microsoft support ♦ 1 GHz or higher x86-32 or x86-64 processor (32-bit application only) ♦ 1 GB RAM ♦ 200 MB free disk space 		♦ Windows 7
GW 18.3	<ul style="list-style-type: none"> ♦ Windows 10 contingent on Microsoft support ♦ 1 GHz or higher x86-32 or x86-64 processor (32-bit application only) ♦ 1 GB RAM ♦ 200 MB free disk space 		♦ Windows 8.1
GW 18.4	<ul style="list-style-type: none"> ♦ Windows 10 contingent on Microsoft support ♦ Windows 11 ♦ 1 GHz or higher x86-32 or x86-64 processor (32-bit application only) ♦ 1 GB RAM ♦ 200 MB free disk space 	♦ Windows 11	
GW 18.5	<ul style="list-style-type: none"> ♦ Windows 10 contingent on Microsoft support ♦ Windows 11 ♦ 1 GHz or higher x86-32 or x86-64 processor (32-bit application only) ♦ 1 GB RAM ♦ 200 MB free disk space 		

GroupWise Web User Requirements

Any of the following web browsers are supported, but may not all be officially tested:

- ☐ **Linux:** Mozilla Firefox; Google Chrome
- ☐ **Windows:** Mozilla Firefox; Google Chrome; Microsoft Edge with Chromium Edge
- ☐ **Macintosh:** The latest version of Safari for your version of Mac OS; Mozilla Firefox; Google Chrome

GroupWise Web Mobile User Requirements

Any of the following mobile operating systems and devices:

- ☐ Android 8.x or later, with Google Chrome, on any Android device
- ☐ Apple iOS 16.x and iPadOS 16.x or later, with Apple Safari and the latest updates

GroupWise WebAccess User Requirements

- ☐ Any of the following web browsers:
 - ♦ **Linux:** Mozilla Firefox; Google Chrome
 - ♦ **Windows:** Microsoft Internet Explorer 11 or later; Mozilla Firefox; Google Chrome; Microsoft Edge
 - ♦ **Macintosh:** The latest version of Safari for your version of Mac OS; Mozilla Firefox; Google Chrome
- ☐ Any mobile device that supports Wireless Access Protocol (WAP) and has a microbrowser that supports Hypertext Markup Language (HTML) 4.0 or later

GroupWise WebAccess Mobile User Requirements

Any of the following tablet operating systems and tablets:

- ☐ Android 4.1, 5.0, or later, with Google Chrome, on any Android device
- ☐ Apple iOS 7.x, 8.x, 9.x, 10.x, 11.x or later, with Apple Safari
- ☐ Kindle Fire, with Amazon Silk
- ☐ Windows Mobile 8.0 or later Pro, with Microsoft Internet Explorer, on any Windows device (full WebAccess, no template)

6 Supported Environments

Information about supported environments is provided in the sections below.

- ♦ [“IPv6 Support” on page 39](#)
- ♦ [“Clustering Support” on page 39](#)
- ♦ [“Virtualization Support” on page 39](#)
- ♦ [“Citrix Support” on page 39](#)
- ♦ [“Domain Services for Windows Support” on page 40](#)
- ♦ [“File System Support” on page 40](#)

IPv6 Support

The Post Office Agent, the Message Transfer Agent, the Internet Agent, and the Monitor Agent support the IPv6 protocol when it is available on the server. If IPv6 is available, the agent detects it and supports it by default, along with IPv4. The Document Viewer Agent does not support IPv6.

As you configure your GroupWise system and specify the network address of an IPv6 server in the GroupWise Administration console, you must specify its DNS hostname. **IP Address** fields in the Admin console do not accommodate IPv6 address format.

Clustering Support

You can set up your GroupWise system in the following clustering environments:

- ♦ OES Cluster Services (NCP) on Linux
- ♦ Microsoft Clustering on Windows

If you are using one of these clustering environments, see [“Setting up a GroupWise Cluster”](#) in the *GroupWise 18 Interoperability Guide* before using the installation instructions in this guide.

Virtualization Support

You can install components of your GroupWise system in virtual environments. If your Virtual Machine supports a supported operating system, you can run GroupWise on that Virtual Machine.

Citrix Support

Any version of the GroupWise client runs successfully on any version of Citrix terminal services.

The GroupWise agents run successfully on Citrix XenServer.

For more information, see the [Citrix website \(http://www.citrix.com\)](http://www.citrix.com).

Domain Services for Windows Support

GroupWise can be used with Domain Services for Windows (DSfW) in your NetIQ eDirectory tree. GroupWise accounts can be added to User objects in the DSfW partition.

IMPORTANT: Do not install GroupWise on the same server with DSfW.

File System Support

GroupWise is supported on any file system supported by the server operating system. However, not all file systems are tested, including BTRFS.

Using an NFS mount to the file system where the GroupWise system is located is not supported.

NOTE: If you choose to use the NSS file system, turn off Salvage for best performance. For more information, see the [Open Enterprise Server Documentation](#).



GroupWise System Creation

Refer to these section for an overview of the GroupWise system and comprehensive information for planning, installing, configuring, and working with GroupWise components.

- ♦ [Chapter 7, “GroupWise System Overview,” on page 43](#)
- ♦ [Chapter 8, “Planning Your GroupWise System,” on page 47](#)
- ♦ [Chapter 9, “Installing the GroupWise Server Software,” on page 65](#)
- ♦ [Chapter 10, “Creating a Simple GroupWise System,” on page 69](#)
- ♦ [Chapter 11, “Creating a Typical GroupWise System,” on page 71](#)
- ♦ [Chapter 12, “Adding Users to Your GroupWise System,” on page 77](#)
- ♦ [Chapter 13, “Working with the GroupWise Administration Console,” on page 79](#)
- ♦ [Chapter 14, “Working with the GroupWise Agents,” on page 83](#)
- ♦ [Chapter 15, “What’s Next,” on page 101](#)

7 GroupWise System Overview

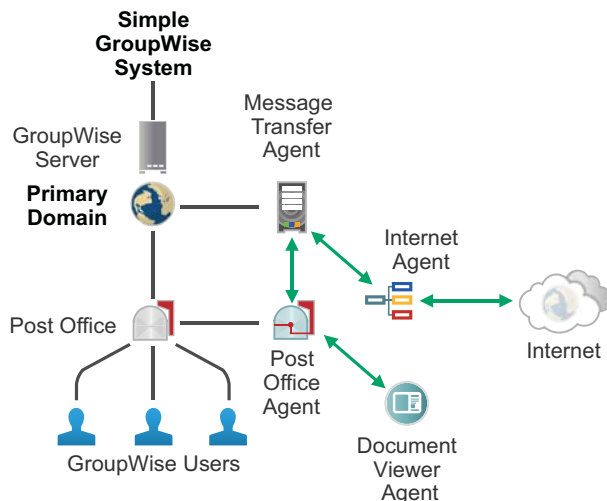
Your GroupWise system can be structured in a variety of ways. Some decisions must be made in the beginning. Other decisions can be made as your GroupWise system grows.

- ♦ [“Simple GroupWise System” on page 43](#)
- ♦ [“Typical GroupWise System” on page 44](#)
- ♦ [“GroupWise Users” on page 44](#)
- ♦ [“GroupWise Agents” on page 45](#)

Simple GroupWise System

A simple GroupWise system is installed on a single server. A simple GroupWise system would be appropriate only for a very small number of users working in a single geographic location or for temporary use in a lab environment.

A simple GroupWise system consists of a single domain (the primary domain) with one post office, and several users, as shown below:



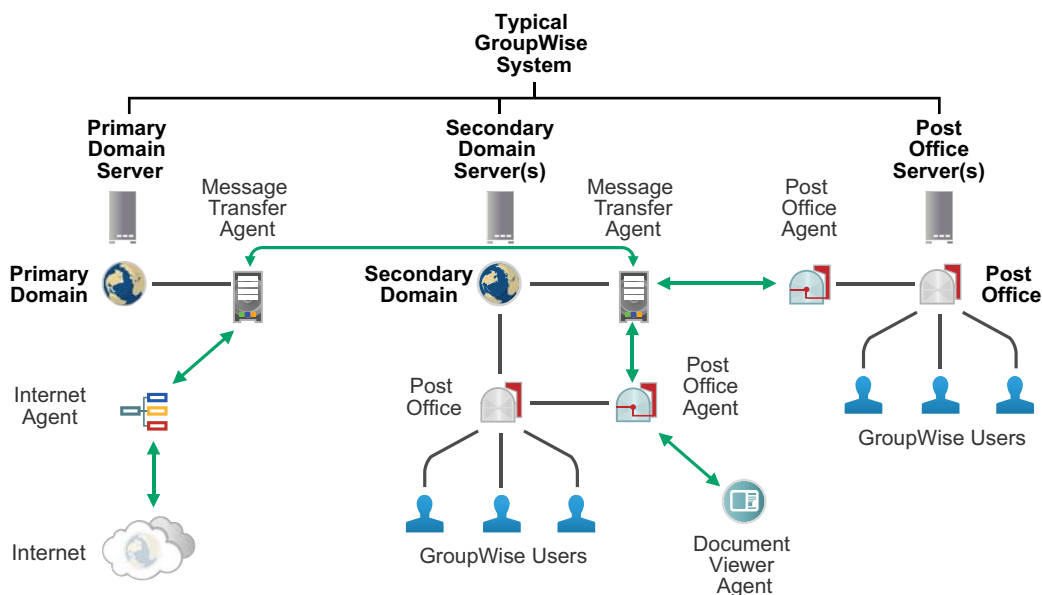
A domain organizes post offices into a logical grouping for administration and routing purposes in your GroupWise system. Messages are transferred between post offices and domains by the Message Transfer Agent (MTA). Messages are transferred to and from your GroupWise system by the Internet Agent (GWIA).

A post office serves as an administrative unit for a group of users and mailboxes. Messages are delivered to mailboxes by the Post Office Agent (POA).

Typical GroupWise System

In contrast to a simple GroupWise system, a typical GroupWise system is installed on multiple servers, perhaps across multiple geographic locations.

- ♦ **Primary Domain:** The primary domain would be created on its own server and would not own post offices.
- ♦ **Secondary Domains:** Secondary domains would each be created on their own servers and would own multiple post offices.
- ♦ **Post Offices:** Depending on server capacity, post offices could be created on domain servers or could be created on their own servers.
- ♦ **Internet Agents:** One or more Internet Agents would be set up for the GroupWise system. An Internet Agent could be set up in a domain that owns post offices, or a separate domain could be created specifically to house one or more Internet Agents.



GroupWise Users

You can add users to your GroupWise system in two different ways:

- ♦ Manually create users in the internal GroupWise directory
- ♦ Import users from an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory

Each GroupWise user has a mailbox in the post office. Users can access their mailboxes in several ways:

- ♦ GroupWise client on a Windows desktop
- ♦ GroupWise WebAccess in a supported web browser
- ♦ GroupWise WebAccess Mobile on a supported tablet

Users can also synchronize mailbox data with mobile devices using the GroupWise Mobility Service.

GroupWise Agents

Domains, post offices, and mailboxes are supported by four GroupWise agents:

- ♦ **POA:** The Post Office Agent (POA) responds to GroupWise client requests for mailbox data and delivers messages between users' mailboxes in a post office. The POA also communicates with the MTA to route messages to and from the post office. In addition, the POA performs a variety of maintenance tasks in the post office.
- ♦ **MTA:** The Message Transfer Agent (MTA) transfers messages between post offices and domains, and performs a variety of other functions in the domain.
- ♦ **GWIA:** The Internet Agent (GWIA) converts GroupWise messages into SMTP format and transfers them to the Internet SMTP hosts where recipients are located. In reverse, it receives SMTP messages from Internet SMTP hosts and converts them into GroupWise format. The GWIA can also provide access for POP3 and IMAP4 clients to access GroupWise mailboxes.
- ♦ **DVA:** The Document Viewer Agent (DVA) converts attached document files from a wide variety of formats into HTML format for indexing by the POA and for viewing in GroupWise WebAccess. You can run up to three DVAs to service conversion requests for a single instance of the POA. Each DVA must be installed on a different server.

8 Planning Your GroupWise System

The GroupWise Installation Wizard helps you install the GroupWise software on GroupWise servers. The GroupWise Installation console helps you create domains and post offices and configure the GroupWise agents.

Print the following worksheets and fill them out as you plan your GroupWise system:

- ☐ Simple GroupWise system

[Simple GroupWise System Worksheet](#)

- ☐ Typical, multiple-server GroupWise system

[Primary Domain Worksheet](#)

[Secondary Domain Worksheet](#) (one for each secondary domain)

[Post Office Worksheet](#) (one for each post office)

The topics in this section present the required information in a convenient planning sequence. The worksheets organize the information in the order in which you need it during installation and setup. As you review the planning information, record the specific details for your GroupWise system on the appropriate worksheet.

- ♦ [“Planning GroupWise System Information” on page 47](#)
- ♦ [“Planning a Domain” on page 48](#)
- ♦ [“Planning a Post Office” on page 53](#)
- ♦ [“Planning Users” on page 57](#)
- ♦ [“GroupWise System Worksheets” on page 58](#)

Planning GroupWise System Information

To identify your GroupWise system as a whole, the Installation console prompts you for the following information:

- ♦ [GroupWise System Name](#)
- ♦ [GroupWise Internet Domain Name](#)

GroupWise System Name

You must provide a name for your GroupWise system. The system name can be your company name (for example, Micro Focus), GroupWise, or anything else that fits the naming scheme you want to use. The system name is displayed only in the Admin console, so any characters can be used. You cannot change the name after your GroupWise system is created.

WORKSHEET

Under **System Settings**, specify the name for your GroupWise system.

GroupWise Internet Domain Name

Your GroupWise system also needs an Internet domain name. The Internet domain name is used after the @ sign in GroupWise users' email addresses. You should already have obtained an Internet domain name from your Internet service provider (ISP).

WORKSHEET

Under **GroupWise System Settings**, specify the Internet domain name.

Under **Create Internet Agent**, specify the host name of the GWIA server as it appears in its DNS record.

Planning a Domain

The primary domain functions as the main administration unit for your GroupWise system. Domains are the routing and administration units for GroupWise. You should plan your domains around working needs instead of necessarily a geographic location, although that can be used as well.

In a simple GroupWise system, the primary domain owns one or more post offices and a GWIA with a secondary domain that serves as a backup for the primary. In a typical GroupWise system, the primary domain can function as a hub for the secondary domains where post offices and GWIAs are located, or it can own post offices that are located on other servers.

As you create a domain, the Installation console prompts you for the following information about the domain:

- ♦ [Domain Server](#)
- ♦ [Domain Name](#)
- ♦ [Domain Folder](#)
- ♦ [Domain Language](#)
- ♦ [Domain Time Zone](#)
- ♦ [Domain Link \(Secondary Domain Only\)](#)
- ♦ [Agents for the Domain](#)
- ♦ [Administrator Access for Domain Creation](#)

Domain Server

You can create a domain on Linux or Windows. Your GroupWise system can include both Linux servers and Windows servers.

WORKSHEET

Under **Platform**, mark the operating system (Linux or Windows) that you plan to use for the domain.

Under **Host**, specify the IP address or DNS hostname of the server where you plan to create the domain.

Domain Name

The name of the primary domain might reflect a company name (such as Micro Focus). The name of a secondary domain might reflect a location (such as Provo), a department (such as Engineering), or some other element that makes sense for your organization. The name is used as the Domain object's name in the Admin console.

The name should consist of a single string. Do not use any of the characters listed in [Invalid Characters in GroupWise Object Names](#).

WORKSHEET

Under **Domain Settings**, specify the domain name.

Domain Folder

The domain requires a folder structure in which to store database files and temporary files that are created during message routing. If you want, the folder name can reflect the domain name you chose.

You must specify an empty folder. If the folder does not already exist, it is automatically created. The installation process can proceed more smoothly if you create the folder in advance.

Use the following platform-specific naming conventions for the folder name:

Linux: Use only lowercase characters.

Windows: No limitations.

WORKSHEET

Under **Domain Settings**, specify the full path for the domain folder.

Domain Language

The domain language determines the sort order for object lists in the Admin console. The primary domain language becomes the default language for secondary domains. The owning domain language becomes the default language for the domain's post offices.

WORKSHEET

Under **Primary Domain Settings**, specify the language for the domain.

NOTE: The languages listed for selection in the Installation console includes more languages than GroupWise supports. See "[Multilingual GroupWise Systems](#)" in the *GroupWise 18 Administration Guide* for a list of valid languages.

Domain Time Zone

When a message is sent from a user in one time zone to a user in another time zone, GroupWise adjusts the message's time so that it is correct for the recipient's time zone. For example, if a user in New York (GMT -05:00, Eastern Time) schedules a user in Los Angeles (GMT -08:00, Pacific Time) for a conference call at 4:00 p.m. Eastern Time, the appointment is scheduled in the Los Angeles user's calendar at 1:00 p.m. Pacific Time.

The primary domain time zone becomes the default time zone for secondary domains. The owning domain time zone becomes the default time zone for the domain's post offices.

WORKSHEET

Under **Domain Settings**, specify the time zone for the domain.

Domain Link (Secondary Domain Only)

When you add a new domain to your GroupWise system, links define how messages are routed from one domain to another. When you add the first secondary domain, the links between the primary and secondary domains are very simple. As the number of domains grows, the links among them can become quite complex. For more information, see "[Managing the Links between Domains and Post Offices](#)" in the *GroupWise 18 Administration Guide*.

SECONDARY DOMAIN WORKSHEET

Under **Domain Settings**, specify the domain that you want to link the new secondary domain to.

Agents for the Domain

Two agents run for a domain. As you configure the agents for the domain, the Installation console prompts you for the following information:

- ♦ [MTA Configuration](#)
- ♦ [GWIA Configuration](#)

The agent consoles are automatically available in the GroupWise Admin console. The agents are configured to start automatically when the server restarts.

MTA Configuration

The Message Transfer Agent (MTA) transfers messages between post offices and domains, and performs a variety of other functions in the domain.

The MTA requires a TCP/IP connection with POAs in the domain and with MTAs in other domains. In order to configure the MTA, you need to plan the following port numbers:

- ♦ **Message Transfer Protocol Port:** Used to communicate with the POA. The default MTP port for the MTA is 7100.
- ♦ **HTTP Port:** Used to communicate with your web browser to provide the MTA console. The default HTTP port for the MTA is 7180.

Use the default port number unless it is already in use on the server.

WORKSHEET

Under **MTA Settings**, specify the required port numbers.

For a complete list of default port numbers used by the GroupWise agents, see “[GroupWise Port Numbers](#)” in the *GroupWise 18 Administration Guide*.

GWIA Configuration

The Internet Agent (GWIA) converts GroupWise messages into SMTP format and transfers them to the Internet SMTP hosts where recipients are located. In reverse, it receives SMTP messages from Internet SMTP hosts and converts them into GroupWise format. The GWIA can also provide access for POP3 and IMAP4 clients to access GroupWise mailboxes.

The GWIA requires that you provide the fully qualified Internet hostname of the server where the GWIA runs, such as `gwia.example.com`, or the name of the "A record" in your DNS table that associates the hostname with the server's IP address.

WORKSHEET

Under **Create Internet Agent**, specify the hostname of the GWIA server as it appears in its DNS record if you want to run the GWIA for this domain.

As your GroupWise system grows, you might want to set up a standalone GWIA in a domain that does not own post offices.

Administrator Access for Domain Creation

The GroupWise Administration Service provides the GroupWise Administration console for managing your GroupWise system. For background information, see [Administration Service Architecture](#).

As you configure the domain, the Installation console prompts you for the following information:

- ♦ [Domain Admin Port](#)
- ♦ [Primary Domain: Super Admin Creation](#)
- ♦ [Secondary Domain: Primary Domain Access](#)

Domain Admin Port

An instance of the Admin Service runs on each GroupWise domain server so that you can access the Admin console at the following URL:

```
https://domain_server_address:9710/gwadmin-console
```

Replace *domain_server_address* with the IP address or DNS hostname of the domain server. The default Admin port for a domain is 9710.

The Admin Service also uses the Admin port to communicate with the MTA for the domain.

WORKSHEET

Under **MTA Settings**, specify the Admin port for the domain.

Use the default port number unless it is already in use on the server.

Primary Domain: Super Admin Creation

When you create the primary domain of a new GroupWise system, you create a GroupWise Super Admin user. The Super Admin has all administrative rights throughout your GroupWise system. The Super Admin can designate other Admin users with lesser rights, perhaps for specific domains or post offices. For more information, see “[GroupWise Administrators](#)” in the *GroupWise 18 Administration Guide*.

WORKSHEET

Under **Credential Settings**, specify the name for the GroupWise Super Admin user and the accompanying password.

If you need to reset the Super Admin password at a later time, you can use the GroupWise Administration utility (GWAdminUtil). For more information, see “[Using the GroupWise Administration Utility](#)” in the *GroupWise 18 Administration Guide*.

Secondary Domain: Primary Domain Access

When you create a secondary domain, you must be the GroupWise Super Admin or a GroupWise system administrator, and know the associated password. For more information, see “[GroupWise Administrators](#)” in the *GroupWise 18 Administration Guide*.

WORKSHEET

Under **System Settings**, specify the administrator user name and password that provide access to the primary domain in the Admin console.

You also need to know the network address of the primary domain server and the Admin port number for the domain. You must be connected to the primary domain in order to create a secondary domain.

WORKSHEET

Under **System Settings**, specify the IP address or DNS hostname of the primary domain server and the Admin port.

Planning a Post Office

A post office contains users’ mailboxes. Like a domain, a post office requires a name and has a folder structure. Post offices should be created around users with common needs and similar settings. This enables you to create post office level settings without having to change settings for smaller groups or users.

As you create the post office, the Installation console prompts you for the following information:

- ♦ [Post Office Server](#)
- ♦ [Post Office Name](#)
- ♦ [Post Office Folder](#)
- ♦ [Post Office Language](#)
- ♦ [Post Office Time Zone](#)
- ♦ [Agents in the Post Office](#)
- ♦ [Administrator Access for Post Office Creation](#)

Post Office Server

You can create a post office on Linux or Windows. Your GroupWise system can include both Linux servers and Windows servers.

WORKSHEET

Under **Platform**, mark the operating system (Linux or Windows) that you plan to use for the post office.

Under **Host**, specify the IP address or DNS hostname of the server where you plan to create the post office.

Post Office Name

A post office, like a domain, requires a unique name. The name can reflect any element that makes sense for your organization. For example, you could use a location (such as Provo) or a department (such as Engineering).

The name is used as the Post Office object's name in the Admin console. It can appear in the GroupWise Address Book.

The name should consist of a single string. Do not use any of the characters listed in [“Invalid Characters in GroupWise Object Names” on page 225](#).

WORKSHEET

Under **Post Office Settings**, specify the post office name.

Post Office Folder

A post office requires a folder structure in which to store database files and temporary files that are created during message routing and delivery. If you want, the folder name can reflect the post office name you chose.

You must specify an empty folder. If the folder does not already exist, it is automatically created. The installation process can proceed more smoothly if you create the folder in advance.

Use the following platform-specific naming conventions for the folder name:

Linux: Use only lowercase characters.

Windows: No limitations.

WORKSHEET

Under **Post Office Settings**, specify the full path for the post office folder.

Post Office Language

The post office language determines the sort order for items in the GroupWise Address Book.

The post office assumes the same language as its domain unless you specify otherwise. For example, if you set the domain and post office language to English, the GroupWise Address Book items are sorted according to English sort order rules. This is true even if some users in the post office are running non-English GroupWise clients such as German or Japanese. Their client interface and help files are in German or Japanese, but the sort order in the GroupWise Address Book is according to English standards. Time, date, and number formats for the non-English clients default to the workstation language.

WORKSHEET

Under **Post Office Settings**, specify the language for the post office.

NOTE: The languages listed for selection in the Installation console includes more languages than GroupWise supports. See “[Multilingual GroupWise Systems](#)” in the *GroupWise 18 Administration Guide* for a list of valid languages.

Post Office Time Zone

When a message is sent from a user in one time zone to a user in another time zone, GroupWise adjusts the message’s time so that it is correct for the recipient’s time zone. For example, if a user in New York (GMT -05:00, Eastern Time) schedules a user in Los Angeles (GMT -08:00, Pacific Time) for a conference call at 4:00 p.m. Eastern Time, the appointment is scheduled in the Los Angeles user’s calendar at 1:00 p.m. Pacific Time.

In a simple, single-server GroupWise system, the post office is automatically created with the same time zone as the primary domain. In a typical, multiple-server GroupWise system, the post office time zone defaults to the domain time zone, but you can change it as you create the post office.

WORKSHEET

Under **Post Office Settings**, specify the time zone where the post office is located.

Agents in the Post Office

Two agents run for a post office. As you configure the agents for the post office, the Installation console prompts you for the following information:

- ♦ [POA Configuration](#)
- ♦ [DVA Configuration](#)

The agent consoles are automatically available in the GroupWise Admin console. The agents are configured to start automatically when the server restarts.

POA Configuration

The Post Office Agent (POA) responds to GroupWise client requests for mailbox data and delivers messages between users’ mailboxes in a post office. The POA also communicates with the MTA to route messages to and from the post office. In addition, the POA performs a variety of maintenance tasks in the post office.

The POA requires a TCP/IP connection with the domain’s MTA. It also requires TCP/IP connections with GroupWise clients. In order to configure the POA, you need to plan the following port numbers:

- ♦ **Client/Server Port:** Used to communicate with GroupWise clients. The default client/server port is 1677.
- ♦ **Message Transfer Port:** Used to communicate with the MTA. The default MTP port for the POA is 7101.
- ♦ **HTTP Port:** Used to communicate with your web browser to provide the POA console. The default HTTP port for the POA is 7181.
- ♦ **SOAP Port:** Used to communicate with SOAP clients such as WebAccess and the GroupWise Mobility Service. The default SOAP port for the POA is 7191.

Use the default port number unless it is already in use on the server.

WORKSHEET

Under **POA Settings**, specify the required port numbers.

For a complete list of default port numbers used by the GroupWise agents, see “[GroupWise Port Numbers](#)” in the *GroupWise 18 Administration Guide*.

DVA Configuration

The Document Viewer Agent (DVA) converts attached document files from a wide variety of formats into HTML format for indexing by the POA and for viewing in GroupWise WebAccess. You can run up to three DVAs to service conversion requests for a single instance of the POA. Each DVA must be installed on a different server.

The DVA requires a TCP/IP connection with a POA. The default DVA port is 8301. Typically, the DVA is set up along with a post office.

WORKSHEET

Under **Create Document Viewer Agent**, mark **Yes** or **No**.

If you need to create a DVA on a server that does not have a post office and POA on it, see “[Scaling Your DVA Installation](#)” in the *GroupWise 18 Administration Guide*.

Administrator Access for Post Office Creation

In order to create a new post office, you need access to the owning domain.

- ♦ “[Owning Domain Access](#)” on page 56
- ♦ “[Post Office Admin Port](#)” on page 57

Owning Domain Access

When you create a post office, you must be the GroupWise Super Admin, a GroupWise system administrator, or a domain administrator for the owning domain, and you must know the associated password. For more information, see “[GroupWise Administrators](#)” in the *GroupWise 18 Administration Guide*.

WORKSHEET

Under **System Settings**, specify the administrator user name and password that provide access to the owning domain in the Admin console.

You also need to know the network address of the primary domain server or the owning domain server, and the Admin port number for the domain.

WORKSHEET

Under **System Settings**, specify the IP address or DNS hostname of the domain server and the Admin port for the domain.

Post Office Admin Port

An instance of the Admin Service runs on each GroupWise post office server. You never use this port when you connect to the Admin console, but the Admin Service uses it to communicate with the POA for the post office. The default Admin port for a post office is 9711.

WORKSHEET

Under **POA Settings**, specify the Admin port for the post office.

Use the default port number unless it is already in use on the server.

Planning Users

When you create a new GroupWise system, you can manually add a few users in order to test your new system. When you see that everything is working smoothly, you can add all of the users to your GroupWise system.

For a simple, single-server GroupWise system, you might want to add the users to the internal GroupWise directory. For a larger number of users, you can import them from an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory.

Manually Created Users

You manually create GroupWise users in the Admin console. You can manually create users specifically for testing a new GroupWise system, or you can initially create users in the internal GroupWise directory and then later associate them with users in an LDAP directory.

WORKSHEET

Under **Users**, list any users that you want to create for testing purposes in your new GroupWise system.

Imported Users

In order to import users from an LDAP directory into GroupWise, you need to gather the following information about the LDAP directory so that GroupWise agents can access it:

- ♦ **Type:** NetIQ eDirectory or Microsoft Active Directory.
- ♦ **Address:** The IP address or DNS hostname of the LDAP server.
- ♦ **Port:** 636 if the LDAP server requires TLS; 389 if TLS is not required.
- ♦ **TLS Certificate:** The location of the LDAP root certificate file on the LDAP server.

- ♦ **LDAP User:** The user name for accessing the LDAP directory.

The user must have sufficient rights to read the LDAP User and Group objects that you plan to import. Specify the information in the format used by the LDAP server. For example:

```
cn=user_name,ou=org_unit,o=organization|
cn=user_name,ou=users,dc=server_name,dc=company_name,dc=com
```

- ♦ **Password:** The password for the LDAP user.
- ♦ **Base DN:** (Optional) The LDAP context under which User and Group objects are located.

You must also establish a name for the LDAP directory to be known in your GroupWise system. The name should be clear and easy to remember, especially if you plan to have multiple GroupWise administrators.

WORKSHEET

Under **LDAP Directory Information**, specify the name for the LDAP directory and list the required information for connecting to the LDAP server.

GroupWise System Worksheets

The following worksheets are provided in this section:

- ♦ [“Simple GroupWise System Worksheet” on page 58](#)
- ♦ [“Primary Domain Worksheet” on page 61](#)
- ♦ [“Secondary Domain Worksheet” on page 62](#)
- ♦ [“Post Office Worksheet” on page 63](#)

Simple GroupWise System Worksheet

Installation Console Field	Value for Your Simple GroupWise System	Explanation
Platform		Domain Server
<ul style="list-style-type: none"> ♦ Linux ♦ Windows 		
Folders		Domain Folder
<ul style="list-style-type: none"> ♦ Domain folder ♦ Post office folder 		Post Office Folder

Installation Console Field	Value for Your Simple GroupWise System	Explanation
System Settings		GroupWise System Name
♦ System Name		GroupWise Internet Domain Name
♦ Internet Domain Name		Domain Server
♦ Host		
♦ IP address		
♦ DNS hostname		
Primary Domain Settings		Planning a Domain
♦ GroupWise Domain Name		
♦ Domain Folder		
♦ Language		
♦ Time zone		
MTA Settings		MTA Configuration
♦ MTP Port		Domain Admin Port
(default 7100)		
♦ HTTP Port		
(default 7180)		
♦ Admin Port		
(default 9710)		
Create Internet Agent		GWIA Configuration
♦ Hostname/DNS “A Record” Name		
Create Post Office		Planning a Post Office
♦ Post Office Name		
♦ Post Office Folder		
Create Document Viewer Agent		DVA Configuration
♦ Yes		
♦ No		

Installation Console Field	Value for Your Simple GroupWise System	Explanation
POA Settings		POA Configuration
<ul style="list-style-type: none"> ♦ Client/Server Port (default 1677) ♦ MTP Port (default 7101) ♦ HTTP Port (default 7181) ♦ SOAP Port (default 7191) ♦ Admin Port (default 9711) 		Post Office Admin Port
Credential Settings		Primary Domain: Super Admin Creation
<ul style="list-style-type: none"> ♦ Admin Name ♦ Password 		
Users		Planning Users
<ul style="list-style-type: none"> ♦ GroupWise Directory <ul style="list-style-type: none"> ♦ User Name ♦ User Name ♦ LDAP Directory <ul style="list-style-type: none"> ♦ eDirectory ♦ Active Directory 		
LDAP Directory Information		Imported Users
<ul style="list-style-type: none"> ♦ Name ♦ Type <ul style="list-style-type: none"> ♦ eDirectory ♦ Active Directory ♦ Address ♦ Port ♦ Use TLS <ul style="list-style-type: none"> ♦ No ♦ Yes TLS Certificate ♦ LDAP User ♦ LDAP User Password 		

Primary Domain Worksheet

Installation Console Field	Value for the Primary Domain	Explanation
Primary Domain Platform <ul style="list-style-type: none"> ♦ Linux ♦ Windows 		Domain Server
Primary Domain Folder <ul style="list-style-type: none"> ♦ Folder Name 		Domain Folder
System Settings <ul style="list-style-type: none"> ♦ System Name ♦ Internet Domain Name ♦ Host <ul style="list-style-type: none"> ♦ IP address ♦ DNS hostname 		GroupWise System Name GroupWise Internet Domain Name Domain Server
Domain Settings <ul style="list-style-type: none"> ♦ GroupWise Domain Name ♦ Domain Folder ♦ Language ♦ Time zone 		Planning a Domain
MTA Settings <ul style="list-style-type: none"> ♦ MTP Port (default 7100) ♦ HTTP Port (default 7180) ♦ Admin Port (default 9710) 		MTA Configuration Domain Admin Port
Credential Settings <ul style="list-style-type: none"> ♦ Admin Name ♦ Password 		Primary Domain: Super Admin Creation

Secondary Domain Worksheet

Installation Console Field	Value for the Secondary Domain	Explanation
Domain Platform		Domain Server
<ul style="list-style-type: none"> ♦ Linux ♦ Windows 		
Domain Folder		Domain Folder
<ul style="list-style-type: none"> ♦ Folder Name 		
System Settings		Secondary Domain: Primary Domain Access
<ul style="list-style-type: none"> ♦ Primary Domain Host ♦ Primary Domain Admin Port ♦ Admin Name ♦ Password 		
Domain Settings		Planning a Domain
<ul style="list-style-type: none"> ♦ GroupWise Domain Name ♦ Domain Folder ♦ Host ♦ Link to Domain ♦ Language ♦ Time zone 		
MTA Settings		MTA Configuration
<ul style="list-style-type: none"> ♦ MTP Port (default 7100) ♦ HTTP Port (default 7180) ♦ Admin Port (default 9710) 		Domain Admin Port
Create Internet Agent		GWIA Configuration
<ul style="list-style-type: none"> ♦ Hostname/DNS “A Record” Name 		

Post Office Worksheet

Installation Console Field	Value for the Post Office	Explanation
Post Office Platform		Post Office Server
<ul style="list-style-type: none"> ♦ Linux ♦ Windows 		
Post Office Folder		Post Office Folder
<ul style="list-style-type: none"> ♦ Folder Name 		
System Settings		Owning Domain Access
<ul style="list-style-type: none"> ♦ Owning Domain Host ♦ Owning Domain Admin Port ♦ Admin Name ♦ Password 		
Post Office Settings		Planning a Post Office
<ul style="list-style-type: none"> ♦ Post Office Name ♦ Host ♦ Post Office Folder ♦ Language ♦ Time zone 		
Create Document Viewer Agent		DVA Configuration
<ul style="list-style-type: none"> ♦ Yes ♦ No 		
POA Settings		POA Configuration
<ul style="list-style-type: none"> ♦ Client/Server Port (default 1677) ♦ MTP Port (default 7101) ♦ HTTP Port (default 7181) ♦ SOAP Port (default 7191) ♦ Admin Port (default 9711) 	Post Office Admin Port	

Installation Console Field	Value for the Post Office	Explanation
Users		Planning Users
<ul style="list-style-type: none"> ◆ GroupWise Directory <ul style="list-style-type: none"> ◆ User Name ◆ User Name ◆ LDAP Directory <ul style="list-style-type: none"> ◆ eDirectory ◆ Active Directory 		
LDAP Directory Information		Imported Users
<ul style="list-style-type: none"> ◆ Name ◆ Type <ul style="list-style-type: none"> ◆ eDirectory ◆ Active Directory ◆ Address ◆ Port ◆ Use TLS <ul style="list-style-type: none"> ◆ No ◆ Yes ◆ TLS Certificate ◆ LDAP User ◆ LDAP User Password 		

9 Installing the GroupWise Server Software

You should have already reviewed [Planning Your GroupWise System](#) and filled out the appropriate [GroupWise System Worksheets](#). The following sections step you through using the GroupWise Installation Wizard to install the GroupWise Server software.

- ♦ “Linux: Installing the GroupWise Server Software” on page 65
- ♦ “Windows: Installing the GroupWise Server Software” on page 66

Linux: Installing the GroupWise Server Software

Reference these sections for information on preparing and installing GroupWise Server software.

Preparing the Linux Server for Your GroupWise System

To prepare the Linux server for your GroupWise system:

- 1 Ensure that the server for your GroupWise system meets the system requirements listed in [GroupWise Server Requirements](#).
- 2 Ensure that the Linux operating system media is available, either physically or in a repository, in case the Installation Wizard needs to install supporting packages on the Linux server.
- 3 Ensure that the server has a static IP address.
- 4 (Optional) Ensure that the folders exist where you want to create your domain and post office folder structures, as described in [Domain Folder](#) and [Post Office Folder](#).
- 5 Continue with [Running the Linux GroupWise Installation Wizard](#).

Running the Linux GroupWise Installation Wizard

To install GroupWise on a Linux server:

- 1 Download and extract the GroupWise 18 software to a temporary location on your server.
- 2 In a terminal window, become `root` by entering `su -` and the `root` password.
- 3 Browse to the location of the extracted software, and run the following command to start the install:


```
./install.sh
```
- 4 Type the number for the language in which you want to run the GroupWise Installation Wizard, and press Enter to select **OK**.
- 5 (Optional) Type 1 for **Documentation**, and then press Enter to review the Readme, Quick Start, and Installation Guide to better prepare yourself for the installation.
- 6 Type 2 for **Installation** and press Enter.

- 7 Enter **a** to accept the License Agreement and to display the Software list.
- 8 Enter **1** for **GroupWise Server** and to display the Actions list.
- 9 Enter **1** for **Install** and to install the GroupWise Server component.

The packages for the GroupWise Server component (Admin Service and agents) are installed on the server. If any supporting packages are not available on the server, the Installation Wizard automatically installs them from the operating system media.
- 10 When the installation is finished, press any key to return to the Installation Options list.

All of the GroupWise agents are installed on every GroupWise server. The MTA and, optionally, the GWIA are configured to run on a domain server. The POA and the DVA are configured to run on a post office server.
- 11 Enter **2** for **Configure** to start the GroupWise Admin Service and display instructions for accessing the Installation console to create a new GroupWise system.
- 12 Right-click the URL under **To install or configure a new GroupWise server**, and then click **Open Link** to open your web browser.

If your web browser does not offer this functionality, open your web browser and copy the URL into it.
- 13 Accept the GroupWise CA signed certificate that the Installation Wizard automatically provides for accessing the Installation console.

The browser session will then authorize you for the next hour to perform installation console tasks. If the browser does not automatically authorize the session, you must manually authorize it by running in a terminal the **gwadmin-ipc authorize** command specified in your web browser.
- 14 Continue with the instructions for the type of GroupWise system that you want to create:
 - ♦ [Creating a Simple GroupWise System](#)
 - ♦ [Creating a Typical GroupWise System](#)

Windows: Installing the GroupWise Server Software

You should have already reviewed [Chapter 8, “Planning Your GroupWise System,” on page 47](#) and filled out the appropriate [GroupWise System Worksheets](#). The following sections step you through using the GroupWise Installation Wizard to install the GroupWise Server software.

Preparing the Windows Server

To prepare the Windows Server for GroupWise installation:

- 1 Ensure that the server for your GroupWise system meets the system requirements listed in [Chapter 4, “GroupWise Server Requirements,” on page 27](#).
- 2 Ensure that the server has a static IP address.
- 3 Ensure that the firewall on the server has the ports open that are used by the GroupWise agents.

For assistance, see [“GroupWise Port Numbers”](#) in the *GroupWise 18 Administration Guide*.

- 4 (Optional) Ensure that the folders exist where you want to create your domain and post office folder structures, as described in [“Domain Folder” on page 49](#) and [“Post Office Folder” on page 54](#).
- 5 Continue with [Running the Windows GroupWise Installation Wizard](#).

Running the Windows GroupWise Installation Wizard

- 1 Log in to Windows as an Administrator-equivalent user.
- 2 Download and extract the contents of the GroupWise 18 software to a temporary location on your server.
- 3 Run `setup.exe` at the root of the extracted GroupWise software to start the GroupWise Installation Wizard.
- 4 (Optional) Review the Readme, Quick Start, and Installation Guide to better prepare yourself for the installation.
- 5 Click **GroupWise Server** to install the GroupWise Server component.
- 6 Select the language in which you want to perform the installation, and then click **OK** to start the GroupWise Server Setup Wizard.
- 7 Click **Next** to continue.
- 8 Accept the **License Agreement** and click **Next** to display the Custom Setup page.

The following components are available for installation:

- ♦ **GroupWise Server:** (Required) Consists of the Admin Service, the POA, the MTA, the GWIA, and the DVA.

All of the GroupWise agents are installed on every GroupWise server. The MTA and, optionally, the GWIA are configured to run on a domain server. The POA and the DVA are configured to run on a post office server.

- ♦ **Client Auto-Update Repository:** (Optional) Helps you distribute the GroupWise client software to users' Windows workstations.

For usage instructions, see [“Using Client Auto-Update to Distribute the GroupWise Client Software”](#) in the *GroupWise 18 Administration Guide*.

- 9 (Optional) Click **Browse** to change the default location where the GroupWise software is installed.
- 10 Click **Next** to continue, and then click **Install** to install the GroupWise software.
- 11 When the GroupWise software is installed, click **Finish** to return to the main page of the Installation Wizard, and then close the Installation Wizard.

You should see two new icons on your Windows desktop.
- 12 On your Windows desktop, double-click **GroupWise Install** to open your web browser and to access the Installation console.

This starts the GroupWise Admin Service and launches the GroupWise Installation console in your web browser.

After installation, use **GroupWise Admin Console** to access the Admin console for ongoing GroupWise system administration.
- 13 Accept the GroupWise CA signed certificate that the Installation Wizard provides for accessing the Installation console.

The browser session will then authorize you for the next hour to perform installation console tasks. If the browser does not automatically authorize the session, you must manually authorize it by running in a command prompt the `gadmin-ipc authorize` command specified in your web browser.

14 Continue with the instructions for the type of GroupWise system that you want to create:

- ♦ [Chapter 10, “Creating a Simple GroupWise System,” on page 69](#)
- ♦ [Chapter 11, “Creating a Typical GroupWise System,” on page 71](#)

10 Creating a Simple GroupWise System

Before you create your simple GroupWise system, you should have reviewed the following sections and completed the associated tasks:

- ❑ [“GroupWise System Overview” on page 43](#)
- ❑ [“Planning Your GroupWise System” on page 47](#)
- ❑ [“Simple GroupWise System Worksheet” on page 58](#)
- ❑ [“Installing the GroupWise Server Software” on page 65](#)

You are ready to use the Installation console to create your simple GroupWise system.

IMPORTANT: As a security feature, the Installation console times out after one hour. For instructions to renew the session, see [Handling an Installation Timeout](#).

- 1 In the GroupWise Installation console, click **Create a New GroupWise System** to display the System Settings page.
- 2 Fill in the following fields from the [Simple GroupWise System Worksheet](#):

[System Name](#)

[Internet Domain Name](#)

[Host](#)

[GroupWise Domain Name](#)

[Domain Folder](#)

[Language](#)

[Time Zone](#)

MTA Settings

[MTA MTP Port](#)

[MTA HTTP Port](#)

[Admin Port](#)

Internet Agent Settings

[Create Internet Agent](#)

[Hostname/DNS “A Record” Name](#)

Post Office Settings

[Create Post Office](#)

[Post Office Name](#)

[Post Office Folder](#)

[Create Document Viewer Agent](#)

[POA Client/Server Port](#)

[POA HTTP Port](#)

[POA MTP Port](#)

[Admin Port](#)

You can click **Help** for more information about the fields.

- 3 Click **Next** to display the Credential Settings page:
- 4 Fill in the following fields from the [Simple GroupWise System Worksheet](#):

[Admin Name](#)

[Password](#)

You can click **Help** for more information about the fields.

- 5 Click **Next** to display the Licensing page. Enter in your Micro Focus customer center credentials to verify your GroupWise License. If you do not enter your credentials, GroupWise will run in evaluation mode for 60 days.

If your GroupWise server does not have access to the Internet, select **Do not install a license at this time** and follow the steps found in [Manually Configure License](#) to install your license manually.

- 6 Click **Next** to display the Summary page.
- 7 Review the information that you have provided and click **Finish** to create your simple GroupWise system.
- 8 Click **GroupWise Administration Console** to log in to the GroupWise Admin console.
- 9 Specify the GroupWise Super Admin user name and password, and then click **Login**.
- 10 Continue with [Adding Users to Your GroupWise System](#).

11 Creating a Typical GroupWise System

Before you create your GroupWise system, you should have reviewed the following sections and completed the associated tasks:

- ❑ [“GroupWise System Overview” on page 43](#)
- ❑ [“Planning Your GroupWise System” on page 47](#)
- ❑ [“Primary Domain Worksheet” on page 61](#)
- ❑ [“Secondary Domain Worksheet” on page 62](#)
- ❑ [“Post Office Worksheet” on page 63](#)
- ❑ [“Installing the GroupWise Server Software” on page 65](#)

You are now ready to create your GroupWise system.

IMPORTANT: If you plan to install GroupWise in a clustered server environment, see [“Setting up a GroupWise Cluster”](#) the *GroupWise 18 Interoperability Guide* before starting to set up your GroupWise system.

- ♦ [“Creating the Primary Domain” on page 71](#)
- ♦ [“Adding a Secondary Domain” on page 72](#)
- ♦ [“Adding a Post Office” on page 73](#)
- ♦ [“Handling an Installation Timeout” on page 75](#)
- ♦ [“Changing the Authentication Mode for the Installation Console” on page 75](#)

Creating the Primary Domain

When you are finished installing the GroupWise Server software, close the Installation Wizard and open the GroupWise Installation console from the **GroupWise Install** shortcut created on the desktop.

IMPORTANT: As a security feature, the Installation console times out after one hour. For instructions to renew the session, see [“Handling an Installation Timeout” on page 75](#).

- 1 In the GroupWise Installation console, click **Create a New GroupWise System** to display the System Settings page.

NOTE: The following steps assume that you do not want to run the Internet Agent in the primary domain and that you do not want to create a post office on the same server with the primary domain.

- 2 Fill in the following fields from the [Primary Domain Worksheet](#):

[System Name](#)

[Internet Domain Name](#)
[Host](#)
[GroupWise Domain Name](#)
[Domain Folder](#)
[Language](#)
[Time Zone](#)
MTA Settings
[MTA MTP Port](#)
[MTA HTTP Port](#)
[Admin Port](#)

You can click **Help** for more information about the fields.

- 3 Click **Next** to display the Credential Settings page:
- 4 Fill in the following fields from the [Primary Domain Worksheet](#):

[Admin Name](#)
[Password](#)

You can click **Help** for more information about the fields.

- 5 Click **Next** to display the Summary page.
- 6 Review the information that you have provided, and then click **Finish** to create the primary domain for your GroupWise system.
- 7 (Optional) Click **GroupWise Administration Console** to display the GroupWise Admin console and administer the domain.

For usage instructions, see [Chapter 13, “Working with the GroupWise Administration Console,” on page 79](#).

- 8 Continue with the task that you want to do next:
 - ♦ [“Adding a Secondary Domain” on page 72](#)
 - ♦ [“Adding a Post Office” on page 73](#)

Adding a Secondary Domain

To add a secondary domain:

- 1 Install the GroupWise Server software on the domain server that you listed on the [Secondary Domain Worksheet](#).

For instructions, see [Installing the GroupWise Server Software](#).

When you are finished installing the GroupWise Server software, close the Installation Wizard and open the GroupWise Installation console from the **GroupWise Install** shortcut created on the desktop.

IMPORTANT: As a security feature, the Installation console times out after one hour. For instructions to renew the session, see [“Handling an Installation Timeout” on page 75](#).

- 2 In the GroupWise Installation console, click **Add a New Domain** to display the System Settings page.

- 3 Fill in the following fields from the [Secondary Domain Worksheet](#):

[Primary Domain Host](#)
[Primary Domain Admin Port](#)
[Admin Name](#)
[Password](#)

You can click **Help** for more information about the fields.

- 4 Click **Next**.

Because no GroupWise software is yet installed on the new GroupWise server, the connection between it and the owning domain server is not yet trusted. This is normal.

- 5 Click **Trust Connection** to display the Domain Settings page.

- 6 Fill in the following fields from the [Secondary Domain Worksheet](#):

[GroupWise Domain Name](#)
[Domain Folder](#)
[Host](#)
[Link to Domain](#)
[Language](#)
[Time Zone](#)

MTA Settings

[MTA MTP Port](#)
[MTA HTTP Port](#)
[Admin Port](#)

Internet Agent Settings

[Hostname/DNS "A Record" Name](#) (optional)

You can click **Help** for more information about the fields.

- 7 Click **Next** to display the Summary page.

- 8 Review the information that you have provided, and then click **Finish** to create a secondary domain in your GroupWise system.

- 9 (Optional) Click **GroupWise Administration Console** to display the GroupWise Admin console and administer the domain.

For usage instructions, see [Chapter 13, "Working with the GroupWise Administration Console," on page 79](#).

- 10 Continue with [Adding a Post Office](#).

Adding a Post Office

To add a post office:

- 1 Install the GroupWise Server software on the post office server that you listed on the [Post Office Worksheet](#).

For instructions, see [Chapter 9, "Installing the GroupWise Server Software," on page 65](#).

When you are finished installing the GroupWise Server software, close the Installation Wizard and open the GroupWise Installation console from the **GroupWise Install** shortcut created on the desktop.

IMPORTANT: As a security feature, the Installation console times out after one hour. For instructions to renew the session, see [“Handling an Installation Timeout” on page 75](#).

- 2 In the GroupWise Installation console, click **Add a New Post Office** to display the System Settings page.
- 3 Fill in the following fields from the [Post Office Worksheet](#):

[Owning Domain Host](#)
[Owning Domain Admin Port](#)
[Admin Name](#)
[Password](#)

You can click **Help** for more information about the fields.

- 4 Click **Next**.

Because no GroupWise software is yet installed on the new GroupWise server, the connection between it and the owning domain server is not yet trusted. This is normal.

- 5 Click **Trust Connection** to display the Post Office Settings page.
- 6 Fill in the following fields from the [Post Office Worksheet](#):

[Post Office Name](#)
[Host](#)
[Post Office Folder](#)
[Language](#)
[Time Zone](#)
POA Settings
[POA Client/Server Port](#)
[POA MTP Port](#)
[POA HTTP Port](#)
[Admin Port](#)
[Create Document Viewer Agent](#)

You can click **Help** for more information about the fields.

- 7 Click **Next** to display the Summary page.
- 8 Review the information that you have provided, and then click **Finish** to create a new post office in your GroupWise system.
- 9 Click **GroupWise Administration Console** to display the GroupWise Admin console.
- 10 Continue with [Adding Users to Your GroupWise System](#).

Handling an Installation Timeout

As a security feature, the Installation console times out after one hour. This helps prevent access by unauthorized persons if the Installation console is left unattended. When an installation session times out, you see the authorization page.

You then run the following command to obtain a new security token:

Linux: `/opt/novell/groupwise/admin/gwadmin-ipc authorize token_string`

Windows: `c:\Program Files\Novell\GroupWise Server\admin\gwadmin-ipc.exe
authorize token_string`

If the Timeout page does not provide a token string, use the following method to gain access to the Installation console:

Linux: Reselect **Configure** in the Installation Wizard to authorize the Installation console session.

Windows: Close the existing browser window.

Double-click **GroupWise Install** on the desktop to start a new authorized Installation console session.

Changing the Authentication Mode for the Installation Console

By default, the Installation console uses token-based authentication. After initial installation, you can change the authentication method as needed.

To configure the Installation console to prompt for a user name and password to allow access, use the following command:

```
gwadminutil installcfg -m user -u user_name -p
```

To configure the Installation console to not allow logins so that the configuration of your GroupWise system cannot be changed by unauthorized users, use the following command:

```
gwadminutil installcfg -m disabled
```

To re-enable logins, specify an authentication method:

```
gwadminutil installcfg -m token
```

```
gwadminutil installcfg -m user -u user_name -p
```


12 Adding Users to Your GroupWise System

You can add users to your new GroupWise system by manually typing the user information or by importing the user information from an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory. You use the Admin console for either approach. You need to create at least two users in order to test your new GroupWise system.

- ♦ [“Manually Adding Users to the Internal GroupWise Directory” on page 77](#)
- ♦ [“Importing Users from an LDAP Directory” on page 77](#)
- ♦ [“Testing the Users” on page 78](#)

Manually Adding Users to the Internal GroupWise Directory

To manually add a user to the internal GroupWise directory:

- 1 In the [GroupWise Admin console](#), click **Users** > **New**.
- 2 Specify the user’s GroupWise user name, along with the user’s first name and last name.
- 3 In the **Post Office** field, start typing the name of the post office to select it.
or
Select the post office from the drop-down list.
- 4 Select **Create Another User** to create at least one more user in your new GroupWise system.
For more detailed information about planning and adding users, see [“Creating GroupWise Accounts”](#) in the *GroupWise 18 Administration Guide*.
- 5 To provide additional information for each user, click **Users**, and then click each user to display and edit the properties of each User object.
- 6 After you have created at least two users, continue with [Testing the Users](#).

Importing Users from an LDAP Directory

In order to add users to your new GroupWise system from an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory, you must first provide configuration information about the LDAP directory, and then import the users.

Providing LDAP Directory Information

To configure GroupWise for the LDAP directory:

- 1 In the [GroupWise Admin console](#), click **System** > **LDAP Servers** > **New Directory**.
- 2 Fill in the following fields from the [Simple GroupWise System Worksheet](#) or the [Post Office Worksheet](#):

Name
Type
Address
Port
TLS Certificate (if needed)
LDAP User
LDAP User Password
Base DN (optional)

You can click **Help** for more information about the fields. For more detailed instructions, see “[Setting Up an LDAP Directory](#)” in the *GroupWise 18 Administration Guide*.

- 3 Click **Test Connection** to verify that you have specified the required information correctly.
- 4 Click **OK** to save the LDAP directory information and add the LDAP directory to the list of LDAP directories.
- 5 Click **Close** to close the list and return to the main Admin console window.
- 6 Continue with [Importing Users](#).

Importing Users

To import users into GroupWise:

- 1 In the [GroupWise Admin console](#), click **System > User Import**.
- 2 Select the post office to import the users into.
- 3 Click **Preview** to list the users to import.
- 4 (Conditional) If there are individual users that you do not want to import, delete them from the list.
- 5 (Conditional) If the list is too long, use the **Context** and **LDAP Filter** fields to restrict the list, and then click **Update Preview**.

You can click **Help** for more information about the fields.

- 6 When the list contains the correct set of users, click **Import Users** to perform the import.
- 7 Click **Close**.
- 8 To see that the users have been imported, click **Users**.
- 9 Continue with [Testing the Users](#).

Testing the Users

How to test users:

- 1 Install the GroupWise client in order to provide mailbox access on a Windows workstation.
See [Installing the GroupWise Client](#) for workstation system requirements and installation instructions.
- 2 Log in as each test user and exchange email messages in order to test the POA and the MTA.
- 3 Exchange email messages with colleagues whose email systems are across the Internet from your GroupWise system in order to test the GWIA.

13 Working with the GroupWise Administration Console

The GroupWise Administration console enables you to perform GroupWise administration anywhere you have a web browser and an Internet connection.

- ♦ “Accessing the Admin Console” on page 79
- ♦ “Making the Most of the System Overview” on page 80
- ♦ “Finding Objects in Object Lists” on page 80
- ♦ “Finding Frequently Used Objects Quickly” on page 81
- ♦ “Working with Objects and Object Properties” on page 81
- ♦ “Using System Tools” on page 81

Accessing the Admin Console

When you complete a session in the Installation console, you can go immediately into the Admin console.

NOTE: If your installation session times out before you access the Admin console, see [Handling an Installation Timeout](#).

To access the Admin console directly:

Click the Admin console icon on your desktop.

or

Enter the following URL in your web browser:

`https://groupwise_server_address:admin_port/gwadmin-console`

Replace *groupwise_server_address* with the IP address or DNS hostname of the GroupWise server. If you are not using the default Admin port, replace *admin_port* with the Admin port number. If you are using the default Admin port number, you do not need to specify it.

Making the Most of the System Overview

On the System Overview page, you can quickly view and configure all domains, post offices, and agents in your GroupWise system. The System Overview page also provides status information for all GroupWise agents, with easy access to their agent consoles and to the controls for starting and stopping them.

Domains are automatically added to the System Overview page when you create them.

- 1 If you do not want a specific domain to be displayed, simply close it.
- 2 To display it again, click **Options > Add Domains**.
- 3 Click a domain, post office, or agent to view its properties.

Agents display status indicators to show whether they are running.

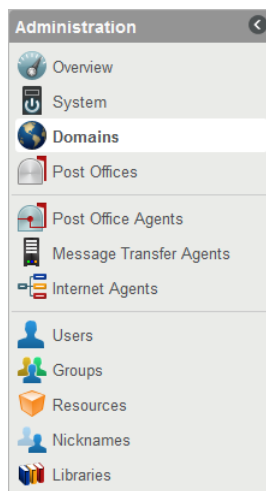
To stop or start an agent:

- 1 Click **Running** or **Stopped**.
- 2 Click the name of the agent to display agent properties.
- 3 Click **Stop Agent** or **Start Agent**.

The agent consoles can also be displayed from the status icons and from the agent properties pages when the agents are running.

Finding Objects in Object Lists

Click any object type in the **Administration panel** to list all objects of that type in your GroupWise system.



Finding Frequently Used Objects Quickly

When you are not quite sure what you are looking for, the object lists available from the **Administration** panel can help you find it. After you have gone to the same object many times, there are faster ways to display the object that you want.

- | | |
|----------------------|---|
| Global Search | As you start typing in the Global Search field, the Admin console starts building a list of objects that match. When you see what you want, click the object in order to go to its property page. |
| Recent | Every object that you go to is added to your Recent list, with the most recent object at the top of the list. This makes it very easy to return to any object that you have worked with recently. |
| Favorites | Any object you go to can be added to your Favorites list. Click ☆ in the upper-right corner of any object property page to add it to your Favorites list. Favorite objects are alphabetized in the list so that your Favorites list has a predicable order.

A ★ on an object property page shows that it is on your Favorites list. Click ★ to remove that object from your Favorites list. |

Working with Objects and Object Properties

You can edit the properties of any GroupWise objects that you have rights to modify. If you are logged in to the GroupWise Admin console as the GroupWise Super Admin, you can edit all objects. If you are logged in as a subordinate administrator, objects that you do not have rights to modify are dimmed. GroupWise tools on the System page are dimmed if you do not have rights to use them.

Usually, when you work with objects, your changes are saved immediately. Sometimes, changes need to replicate throughout your GroupWise system before the change is complete. When that happens, the object is dimmed and you cannot make further changes to the object until replication is finished.

Using System Tools

You can find all of the GroupWise system operations and object-specific utilities on the System page.

The System tools are described in detail in the [GroupWise 18 Administration Guide](#).

14 Working with the GroupWise Agents

The GroupWise agent software is automatically installed when you create domains and post offices. For a domain, you run the MTA and optionally the GWIA. For a post office, you run the POA and optionally the DVA. All of the agents are configured to automatically restart whenever the server restarts.

- ♦ [“Linux: Managing the GroupWise Agents” on page 83](#)
- ♦ [“Windows: Managing the GroupWise Agents” on page 96](#)
- ♦ [“Monitoring the Agents from Your Web Browser” on page 99](#)

Basic agent monitoring and management is most easily performed on the System Overview page in the Admin console. For instructions, see [Making the Most of the System Overview](#).

For detailed configuration information about each agent, see the following sections in the *GroupWise 18 Administration Guide*:

- ♦ [“Post Office Agent”](#)
- ♦ [“Message Transfer Agent”](#)
- ♦ [“Internet Agent”](#)
- ♦ [“Document Viewer Agent”](#)

Linux: Managing the GroupWise Agents

Basic agent monitoring and management is most easily performed on the System Overview page in the Admin console. For instructions, see [“Making the Most of the System Overview” on page 80](#). Refer to the following additional tasks as you maintain all the GroupWise agents on Linux:

- ♦ [“Manually Starting and Stopping the Linux GroupWise Agents” on page 83](#)
- ♦ [“Running the Linux GroupWise Agents as a Non-root User” on page 85](#)
- ♦ [“Automatically Restarting the Linux GroupWise Agents with the GroupWise High Availability Service” on page 89](#)
- ♦ [“Using the Linux GroupWise Agent Log Files” on page 95](#)

Manually Starting and Stopping the Linux GroupWise Agents

This section has information for options you can use to manually start and stop Linux GroupWise agents.

Starting and Stopping the Linux Agents as Services

There are two ways to start or stop Linux agents as services.

- ♦ [“Using the grpwise Script” on page 84](#)
- ♦ [“Using the gwsc Command” on page 85](#)

Using the grpwise Script

All of the Linux GroupWise agents except the Monitor Agent can be started as services by using the `grpwise` script. The Monitor Agent uses its own customized `grpwise-ma` script that works essentially the same way. When the agents run as services, they do not have a user interface.

In the `grpwise` script, each agent is designated in terms of the name of the domain and post office associated with it, in the following format:

```
POA:    post_office.domain
MTA:    domain
GWIA:   gwia.domain
DVA:    gwdva
```

Use the following set of `rcgrpwise` commands to start and stop the agents as services and verify their status:

<code>rcgrpwise status</code>	Displays the status of the GroupWise agents that are configured to run on the server.
<code>rcgrpwise status agent_location_name</code>	Displays the status of the specified agent.
<code>rcgrpwise start</code> <code>rcgrpwise restart</code>	Starts/restarts the GroupWise agents that are configured to run on the server.
<code>rcgrpwise start agent_location_name</code> <code>rcgrpwise restart agent_location_name</code>	Starts/restarts the specified agent.
<code>rcgrpwise stop</code>	Stops the GroupWise agents that are configured to run on the server.
<code>rcgrpwise stop agent_location_name</code>	Stops the specified agent. If an agent does not respond to the <code>rcgrpwise stop</code> command, you can use the Linux <code>kill pid_number</code> command to stop it.
<code>rcgrpwise print</code>	Lists the contents of the <code>gwha.conf</code> file where the agents are configured. For information about the <code>gwha.conf</code> file, see Automatically Restarting the Linux GroupWise Agents with the GroupWise High Availability Service .

When the agents run without a user interface, you can monitor them by using their agent consoles. See [Monitoring the Agents from Your Web Browser](#).

Using the gwsc Command

You can also manage the GroupWise agents by using the `gwsc` command, which is short for the `gadminutil services` command.

For the `gwsc` command, each agent is designated in terms of its object name or of the name of the domain and post office associated with it:

POA: `poa_object_name` or `post_office_name`
MTA: `mta_object_name` or `domain_name`
GWIA: `gwia_object_name`
DVA: `dva_object_name`

Use the following set of `gwsc` commands to start and stop the agents as services and verify their status:

<code>gwsc -query</code>	Displays the status of the GroupWise agents that are configured to run on the server.
<code>gwsc -query name</code>	Displays the status of the specified agent.
<code>gwsc -start</code>	Starts the GroupWise agents that are configured to run on the server.
<code>gwsc -start name</code>	Starts the specified agent.
<code>gwsc -stop</code>	Stops the GroupWise agents that are configured to run on the server.
<code>gwsc -stop name</code>	Stops the specified agent.
<code>gwsc -list</code>	Lists the agent services that are configured on the server.

Running the Linux GroupWise Agents as a Non-root User

For security reasons, it is preferable that the GroupWise agents do not run with `root` user privileges. For example, if an intruder manages to assume the identity of a GroupWise agent, the intruder gains all the privileges of the commandeered process. If the process is running with `root` user privileges, then the intruder has `root` access to your system. If the process is running as a user with minimal privileges, then the intruder has only restricted access to your system. Therefore, your system is more secure if the GroupWise agents do not run as `root`.

The `root` user still needs to start the agents, because the agents do need to access some `root`-only resources on startup. However, you can configure the agents to switch to a different user after they start. After the agents are running as the non-`root` user, they need adequate access to the locations where each domain, post office, and library is located.

- ♦ [“Setting Up Typical Non-root Access” on page 86](#)
- ♦ [“Setting Up Non-root Access on an NSS Volume on Micro Focus Open Enterprise Server” on page 87](#)
- ♦ [“Changing the Non-root User” on page 88](#)

NOTE: You can configure the POA, MTA, and GWIA to run as a non-root user. The DVA must still run as root. Unlike the other agents, the Monitor Agent can be started as a non-root user by default, so no setup is required for it to run as a non-root user.

Setting Up Typical Non-root Access

To configure the GroupWise agents to switch users after startup:

- 1 Ensure that you are logged in as root.
- 2 Select a Linux user for the agents to run as, and ensure that the user is listed in the `/etc/passwd` file.
You might want to create a new user specifically for this purpose, perhaps named `gwagents`. The user name must not match any local user names on the Linux server.

IMPORTANT: All agents running on the same server must run as the same user.

- 3 Change to the `groupwise` folder under `/etc`:

```
cd /etc/opt/novell/groupwise
```

- 4 Create a new `agents` folder, and then change to that folder:

```
mkdir agents
cd agents
```

- 5 Create a file named `uid.conf`.
- 6 Type the selected user name in the file, for example:

```
gwagents
```

- 7 Stop and then start the agents.

While starting as root, the agents automatically change the ownership of the domain and post office folder structures from root to the user you specified in the `uid.conf` file. Then, they switch users and run as the user you specified, rather than as root.

IMPORTANT: The first time you start an agent as a non-root user (or if you change from one non-root user to another), the agent might take longer than usual to start, because of the change in ownership of the directories and files accessed by that agent. This is especially true of a POA that services a large post office and that requires access to a restore area, especially a restore area on a remote server.

- 8 (Optional) List the agent processes to see that they are no longer running as root.

```
ps -eaf | grep gw
```

- 9 Repeat [Step 1](#) through [Step 8](#) on each domain and post office server.

Later on, if you want to change the user that the agents are running as, follow the instructions in [Changing the Non-root User](#).

Setting Up Non-root Access on an NSS Volume on Micro Focus Open Enterprise Server

When your domains, post offices, and libraries are located on a Micro Focus Open Enterprise Server (OES) NSS volume, you must set up an eDirectory user for the agents to run as and you must Linux-enable that user. On OES, you can use NetIQ iManager to accomplish these tasks.

To configure the agents to switch users after startup and provide access to an NSS volume:

- 1 Select or create an eDirectory user for the agents to run as.

You might want to create a new user specifically for this purpose, perhaps named `gwagents`. The user name must not match any local user names on the Linux server.

- 1a From the Open Enterprise Server Welcome page in your web browser, click the **Management Services** tab, and then click **iManager**.

- 1b To log in to iManager, specify a user name, a password, and a tree.

- 1c In the left pane, expand **Users**, and then click **Create User**.

- 1d Provide the required information, and then click **OK**.

The user does not need a password.

IMPORTANT: All agents running on the same server must run as the same user.

- 2 Linux-enable the user you just created:

- 2a In the left pane, expand **Linux User Management**, and then click **Enable User for Linux**.

- 2b Browse to and select the user you just created, and then click **OK**.

- 2c Select the primary group for the user to belong to (for example, `admin`group).

- 2d Change `/bin/bash` to `/bin/false` because the user does not need a shell.

- 2e Click **OK** to Linux-enable the user.

- 3 Ensure that you are logged in as `root`.

- 4 Change to the `groupwise` folder under `/etc`:

```
cd /etc/opt/novell/groupwise
```

- 5 Create a new `agents` folder, and then change to that folder:

```
mkdir agents
cd agents
```

- 6 Create a file named `uid.conf`.

- 7 Type the selected user name in the file, for example:

```
gwagents
```

- 8 Use the following command to grant the user the required rights to the folders that the agents need to access on the local server:

```
rights -f /folder_name -r rwcmf trustee user.context.tree
```

The POA needs access to the post office folder. The MTA and the GWIA need access to the domain folder.

9 Stop and then start the agents.

While starting as `root`, the agents automatically change the ownership of the domain and post office folder structures from `root` to the user you specified in the `uid.conf` file. Then, they switch users and run as the user you specified, rather than as `root`.

IMPORTANT: The first time you start an agent as a non-`root` user (or if you change from one non-`root` user to another), the agent might take longer than usual to start, because of the change in ownership of the directories and files accessed by that agent. This is especially true of a POA that services a large post office and that requires access to a restore area, especially a restore area on a remote server.

10 (Optional) List the agent processes to see that they are no longer running as `root`.

```
ps -eaf | grep gw
```

11 Repeat [Step 3](#) through [Step 10](#) on each domain and post office server.

Later on, if you want to change the user that the agents are running as, follow the instructions in [“Changing the Non-root User” on page 88](#).

Changing the Non-root User

To prevent an agent from running as a different user than the one for which it was originally configured, the GroupWise agents create a `uid.run` file in the domain or post office folder that they service. The GWIA creates the `uid.run` file in its `gwia` directory (typically `domain/wpgate/gwia`).

If, for any reason, the user specified in the `uid.run` file does not match the user specified in the `uid.conf` file, the agent displays the following message:

```
Error: Running the agent with conflicting effective users
```

This could happen if the user specified in the `uid.conf` file is manually edited, or if the `uid.conf` file is deleted, thus changing or removing the information about the user that the agent should run as. If this message appears, verify that the `uid.conf` file specifies the desired user, and then delete the `uid.run` file.

After displaying the message, the agent does not start, because it no longer has appropriate permissions in the domain or post office folder that it needs to service. By deleting the `uid.run` file, you enable the agent to reset the permissions in the domain or post office folder to the appropriate user and then start successfully.

After configuring an agent to run as a specific non-`root` user:

- ♦ If you want the agent to run as a different non-`root` user, modify the `uid.conf` file in the `/etc/opt/novell/groupwise/agents` folder to specify the desired non-`root` user. Then delete the `uid.run` file from the folder serviced by the agent.
- ♦ If you want the agent to run as `root` again, delete the `uid.conf` file from the `/etc/opt/novell/groupwise/agents` folder, and delete the `uid.run` file from the folder serviced by the agent.

Automatically Restarting the Linux GroupWise Agents with the GroupWise High Availability Service

You can use the GroupWise High Availability Service (gwaha), in conjunction with GroupWise Monitor, to detect when a Linux GroupWise agent has stopped unexpectedly and to restart it automatically.

NOTE: On Windows, Microsoft Clustering Services can automatically restart a GroupWise agent service that is not responding. However, on Linux, some clustering environments do not include this capability, so it is provided by the GroupWise High Availability Service.

The GroupWise High Availability Service is installed automatically. After you enable it, it automatically starts when your server starts.

The High Availability Service relies on the Monitor Agent to detect when a Linux GroupWise agent is no longer running. The Monitor Agent notifies the GroupWise High Availability Service of any problem. Then the GroupWise High Availability Service then issues the command by using the `grpwise` script to start the problem agent. The GroupWise High Availability Service runs as `root`, as configured in the `/etc/xinetd.d/gwaha` file.

A single Monitor Agent can service multiple instances of the GroupWise High Availability Service on multiple servers, as long as all instances use the same user name and password to communicate with the Monitor Agent.

NOTE: You can use either the Linux Monitor Agent or the Windows Monitor Agent to monitor the Linux GroupWise agents. However, you cannot use the GroupWise High Availability Service to restart the Windows GroupWise agents.

- ♦ [“Reconfiguring the GroupWise High Availability Service \(Optional\)” on page 89](#)
- ♦ [“Enabling the GroupWise High Availability Service” on page 92](#)
- ♦ [“Creating a GroupWise High Availability Service User” on page 93](#)
- ♦ [“Configuring the Monitor Agent to Communicate with the GroupWise High Availability Service” on page 93](#)
- ♦ [“Testing the High Availability Service” on page 95](#)

Reconfiguring the GroupWise High Availability Service (Optional)

The default configuration of the High Availability Service is often appropriate, but you can optionally edit its configuration files to customize its functionality:

- ♦ [“Editing the gwaha File to Change the Port Number \(Optional\)” on page 90](#)
- ♦ [“Editing the gwaha.conf File to Enable TLS and Customize Agent Management \(Optional\)” on page 90](#)

Editing the gwha File to Change the Port Number (Optional)

The basic configuration for the GroupWise High Availability Service is contained in the `/etc/xinetd.d/gwha` file:

```
socket_type = stream
user = root
server = /opt/novell/groupwise/agents/bin/gwha
wait = no
instances = 1
protocol = tcp
type = UNLISTED
port = 8400
disable = yes
```

The only option you can change in this file is the port number. By default, the GroupWise High Availability service listens on port 8400. If that port number is already in use on the server where you are setting up the GroupWise High Availability service, you can change the port number in the `gwha` file.

IMPORTANT: The GroupWise High Availability service must use the same port number on all servers where you want it to restart the GroupWise agents.

- 1 In a terminal window, become `root` by entering `su -` and the `root` password.
- 2 Edit the `gwha` file in an ASCII text editor.
- 3 Change the port number as needed.

IMPORTANT: Do not change any other options in this file.

- 4 Save the file and exit the text editor.
- 5 Continue with [Editing the gwha.conf File to Enable TLS and Customize Agent Management \(Optional\)](#).

or

Continue with [Enabling the GroupWise High Availability Service](#).

Editing the gwha.conf File to Enable TLS and Customize Agent Management (Optional)

The interaction between the GroupWise High Availability service and the GroupWise agents is controlled by the following file:

`/etc/opt/novell/groupwise/gwha.conf`

You can reconfigure the following functionality:

- ♦ Enable TLS between the High Availability Service and the Monitor Agent.
- ♦ Change the length of time between when the `grpwise` script issues the command to start an agent and when the script displays a message indicating that the agent has started.
- ♦ If you changed the port number in the `/etc/xinetd.d/gwha` file, make the corresponding change in the `gwha.conf` file.

At the top of the `gwha.conf` file, in the `[gwha]` section, is a section for configuring TLS for communication between the GroupWise High Availability service and the Monitor Agent. After the `[gwha]` section are sections for each agent that is configured to run on the server, as shown. The headings for the agent sections match the agent designations listed in [Starting and Stopping the Linux Agents as Services](#).

```
[gwha]
TLS      = no
key      =
cert     =
password =

[domain_name]
server   = /opt/novell/groupwise/agents/bin/gwmta
command  = /etc/init.d/grpwise
startup  = domain_name.mta
delay    = 2
wait     = 10

[post_office_name.domain_name]
server   = /opt/novell/groupwise/agents/bin/gwpoa
command  = /etc/init.d/grpwise
startup  = post_office_name.poa
delay    = 2
wait     = 10

[gwia.domain_name]
server   = /opt/novell/groupwise/agents/bin/gwia
command  = /etc/init.d/grpwise
startup  = gwia.cfg
delay    = 2
wait     = 10

[gwdva]
server   = /opt/novell/groupwise/agents/bin/gwdva
command  = /etc/init.d/grpwise
startup  = gwdva.dva
delay    = 2
wait     = 10
```

To reconfigure the GroupWise High Availability service in the `gwha.conf` file:

- 1 In a terminal window, become `root` by entering `su -` and the `root` password.
- 2 Edit the `gwha.conf` file in an ASCII text editor.
- 3 (Conditional) If you use TLS, fill in the following fields in the `[gwha]` section:

```
[gwha]
TLS      = yes
key      = file_name.key
cert     = file_name.crt
password = password
```

- 4 (Conditional) If you changed the port number for the GroupWise High Availability service, as described in [Reconfiguring the GroupWise High Availability Service \(Optional\)](#), add the following line to the `[gwha]` section:

```
port = port_number
```

Replace `port_number` with the new port number you specified in the `gwha` file.

- 5 (Optional) If you want to control how the `grpwise` script manages starting and stopping the agents, modify the `delay =` and `wait =` settings.

The `delay =` setting controls the length of time between when the script issues the command to start an agent and when the script displays a message indicating that the agent has started. The default delay time is 2 seconds. Under certain circumstances, an agent could encounter a problem and fail to start after 2 seconds. In this case, you would receive the success message, but the agent would not be running. You need to increase the `delay =` setting to accommodate the length of time it typically takes for the agent to start successfully on your system.

The `wait =` setting controls the length of time between when the script issues the command to stop an agent and when the script kills the agent if the agent has not yet stopped. The default wait time is 10 seconds. Under certain circumstances, an agent could take longer than 10 seconds to perform a normal shutdown, and killing the agent under those circumstances would not be appropriate. You need to increase the `wait =` setting to accommodate the length of time it usually takes for the agent to shut down. A message notifies you if the script kills an agent because its shutdown exceeds the `wait =` setting.

The default settings are usually appropriate, so you do not need to change them unless you frequently encounter problems with starting or stopping an agent with the script.

- 6 Save the file and exit the text editor.
- 7 Continue with [Enabling the GroupWise High Availability Service](#).

Enabling the GroupWise High Availability Service

Starting in SLES 12, SLES supports `systemd` as a replacement for `xinetd`. In SLES 15, `xinetd` is not supported at all. Because of this, when you install GroupWise 18.3 or a later version on SLES 12 or on SLES 15, the install places `gwha.socket` and `gwha@.service` in `/usr/lib/systemd/system`. On SLES 12, you can still use the `xinetd` process to enable GWA. On SLES 15 you must use the `systemd` process to enable GWA.

Enabling GWA on xinetd (SLES 12)

To enable GWA on `xinetd`:

- 1 In YaST, click **Network Services > Network Services (xinetd)**.
- 2 (Conditional) If necessary, select **Enable** to activate the list of services.
- 3 Scroll down to the `gwha` line, select it, and then click **Toggle Status (On or Off)** to change the status to **On**.
- 4 Click **Finish**.
- 5 Repeat [Step 1](#) through [Step 4](#) on all servers where you want the GroupWise High Availability service to restart the GroupWise agents.
- 6 Continue with [Creating a GroupWise High Availability Service User](#).

Enabling GWha on systemd (SLES 12 and 15)

To enable the GWha service on `systemd` when the server is rebooted, open a terminal and run the following command:

```
systemctl enable gwha.socket
```

NOTE: If you previously had `xinetd` enabled on SLES 12, you must disable it before enabling `systemd`.

Creating a GroupWise High Availability Service User

The GroupWise High Availability service needs a login user on each server where GroupWise agents need to be restarted.

- 1 Create a new user and associated password on the local Linux server to represent the GroupWise High Availability service.

You might name it `gwhauser`.

IMPORTANT: Use a local user account for use only by the GroupWise High Availability service. Do not use a Micro Focus Linux-enabled user. Do not use `root`.

- 2 Create the same user on each Linux server where you want the GroupWise High Availability service to restart the GroupWise agents.
- 3 On each Linux server, configure the `gwha.allow` file for the new user:

3a Change to the following folder:

```
/etc/opt/novell/groupwise
```

3b Edit the `gwha.allow` file in an ASCII text editor.

3c Specify the user that you created in [Step 1](#).

3d Save the file and exit the text editor.

- 4 Continue with [Configuring the Monitor Agent to Communicate with the GroupWise High Availability Service](#).

Configuring the Monitor Agent to Communicate with the GroupWise High Availability Service

After you have the GroupWise High Availability service set up and working correctly on all Linux servers where you want it to restart the GroupWise agents, you need to configure the Monitor Agent to communicate with it, and then test it to ensure that you can rely on it in the future.

IMPORTANT: Although you need a GroupWise High Availability service running on each Linux server where there are GroupWise agents, you need only one Monitor Agent to monitor all agents in your GroupWise system.

- ♦ [“Configuring the Linux Monitor Agent” on page 94](#)
- ♦ [“Configuring the Windows Monitor Agent” on page 94](#)

Configuring the Linux Monitor Agent

- 1 Install the Linux Monitor Agent.

For installation instructions, see [Setting Up GroupWise Monitor](#).

- 2 Configure the Linux Monitor Agent with the `--hauser`, `--hapassword`, and `--hapoll` startup switches.

The Monitor Agent uses the `--hauser` and `--hapassword` switches to communicate with the GroupWise High Availability service on port 8400, as configured in the `/etc/xinetd.d/gwha` file. When the Monitor Agent notices that a GroupWise agent has stopped, it notifies the GroupWise High Availability Service. Then the GroupWise High Availability Service issues the command to restart the problem agent.

For more information, see “[Using Monitor Agent Startup Switches](#)” in the *GroupWise 18 Administration Guide*.

2a In YaST, click **System** > **/etc/sysconfig Editor**.

2b Expand **Network** > **Mail** > **GroupWise**.

2c Click **GROUPWISE_MA_OPTIONS**.

2d In the **Setting** field, set the `--hauser` and `--hapassword` switches for the user that you created in [Creating a GroupWise High Availability Service User](#).

TIP: An easy way to create the string is to copy the example at the bottom of the **Description** paragraph and replace `username` and `password` as needed.

2e In the **Setting** field, set the `--hapoll` switch for the number of seconds in the poll cycle on which the Monitor Agent contacts the GroupWise High Availability Service to provide agent status information.

2f Click **OK** to save the settings.

2g Click **OK** again to save the change.

2h Exit YaST.

- 3 Start the Monitor Agent.

```
rcgrpwise-ma start
```

- 4 Continue with [Testing the High Availability Service](#).

Configuring the Windows Monitor Agent

- 1 Install the Windows Monitor Agent as either an application with a server console on the server or as a Windows service without a user interface on the server.

For installation instructions, see [Setting Up GroupWise Monitor](#).

NOTE: The Windows Monitor Agent provides a server console that is not available on Linux. For more information, see “[Comparing the Monitor Consoles](#)” in the *GroupWise 18 Administration Guide*.

- 2 Configure the Windows Monitor Agent with the `/hauser`, `/hapassword`, and `/hapoll` startup switches.

The Monitor Agent uses the `--hauser` and `--hapassword` switches to communicate with the GroupWise High Availability service on port 8400, as configured in the `/etc/xinetd.d/gwha` file. When the Monitor Agent notices that a GroupWise agent has stopped, it notifies the GroupWise High Availability Service. Then the GroupWise High Availability Service issues the command to restart the problem agent.

For more information, see “[Using Monitor Agent Startup Switches](#)” in the *GroupWise 18 Administration Guide*.

3 (Conditional) If you installed the Windows Monitor Agent as an application:

3a Create a batch file similar to the following example:

```
c:\Program Files\Novell\GroupWise Server\Monitor\gwmon.exe
/hauser-gwha /hapassword-gwha /hapoll-60
```

3b Create a desktop icon for running the batch file.

3c To start the Monitor Agent, run the batch file.

4 (Conditional) If you installed the Windows Monitor Agent as a Windows service:

4a In the Control Panel, click **Administrator Tools > Services**.

4b Right-click **GroupWise Monitor**, and then click **Properties**.

4c In the **Start Parameters** field, specify the required Monitor Agent startup switches, and then click **OK**. For example:

```
/hauser-gwha /hapassword-gwha /hapoll-60
```

4d To start the Monitor Agent, right-click **GroupWise Monitor**, and then click **Start**.

Testing the High Availability Service

- 1 Stop one of the Linux agents, as described in [Starting and Stopping the Linux Agents as Services](#).
- 2 Check the status of the agent you stopped to make sure it is stopped.
- 3 Wait for the next Monitor Agent polling cycle.

You can check and, if necessary, change the Monitor Agent polling cycle in the [Monitor Agent console](#). Click **Preferences**, and then scroll down to the **HTTP Settings** section.

- 4 After the polling cycle has passed, check the status of the agent again.

The agent that you stopped should now be running again.

Using the Linux GroupWise Agent Log Files

Agent status messages and error messages are written to the agent log files (`mmdagent.nnn`) in agent-specific subfolders of the following folder:

```
/var/log/novell/groupwise
```

The log file name includes the month and day when it was created, the name of the agent, and an incrementing extension to accommodate multiple log files on the same day.

The agents also maintain a symbolic link to a file named `agent.currentlog`, where *agent* is the name of the agent object in the Admin console. This link points to the current agent log file, regardless of the date and incrementing extension of the actual agent log file name. This facilitates monitoring the current agent log file using the `tail` command.

NOTE: The `agent.currentlog` symbolic link is not available for the DVA log files.

Windows: Managing the GroupWise Agents

Basic agent monitoring and management is most easily performed on the System Overview page in the Admin console. For instructions, see [“Making the Most of the System Overview” on page 80](#). Refer to the following additional tasks as you maintain all the GroupWise agents on Windows:

- ♦ [“Manually Starting and Stopping the Windows GroupWise Agents” on page 96](#)
- ♦ [“Using the Windows GroupWise Agent Log Files” on page 98](#)
- ♦ [“Uninstalling the Windows GroupWise Agents and Applications” on page 98](#)

Manually Starting and Stopping the Windows GroupWise Agents

This section has information for options you can use to manually start and stop Windows GroupWise agents.

Manually Starting and Stopping the GroupWise Agents as Services

There are two ways to start or stop GroupWise agents as services on Windows.

- ♦ [“By Using the Windows Services Tool” on page 96](#)
- ♦ [“By Using the gwsc Command” on page 96](#)

By Using the Windows Services Tool

You can manage the GroupWise agents just as you would any other Windows services.

For example, on Windows Server 2012 R2:

- 1 From the Windows desktop, click **Start** > **Administrative Tools** > **Services**.
 - 2 Select the agent service, and then click **Start**.
- or
- Select the agent service, and then click **Stop**.

When the agents run without a user interface, you can monitor them by using their agent consoles. See [“Monitoring the Agents from Your Web Browser” on page 99](#).

By Using the gwsc Command

You can also manage the GroupWise agents by using the `gwsc` command, which is short for the `gadminutil services` command.

For the `gwsc` command, each agent is designated in terms of its object name or of the name of the domain and post office associated with it:

POA: `poa_object_name` or `post_office_name`
MTA: `mta_object_name` or `domain_name`
GWIA: `gwia_object_name`
DVA: `dva_object_name`

Use the following set of `gwsc` commands to start and stop the agents as services and verify their status:

<code>gwsc -query</code>	Displays the status of the GroupWise agents that are configured to run on the server.
<code>gwsc -query name</code>	Displays the status of the specified agent.
<code>gwsc -start</code>	Starts the GroupWise agents that are configured to run on the server.
<code>gwsc -start name</code>	Starts the specified agent.
<code>gwsc -stop</code>	Stops the GroupWise agents that are configured to run on the server.
<code>gwsc -stop name</code>	Stops the specified agent.
<code>gwsc -list</code>	Lists the agent services that are configured on the server.

Manually Starting the Windows Agents As Applications for Troubleshooting

In general, you should run the Windows agents as services without a user interface, so that they can be managed in the Admin console.

Occasionally, when troubleshooting a problem that occurs at agent startup, the problem can occur before the agent console can be displayed and before error messages can be written to the agent log file. Under such circumstances, you can start an agent with a user interface in order to view any errors that the agent displays on the server console before the agent stops again.

IMPORTANT: When an agent is running with a user interface, it cannot be managed in the Admin console.

To run the agents as applications, you can create desktop shortcuts for them. The desktop shortcuts need to contain the following commands:

Syntax:

```
c:\Program Files\Novell\GroupWise Server\agents\gwpoa.exe
                               /home \post_office_folder
c:\Program Files\Novell\GroupWise Server\agents\gwmta.exe
                               /home \domain_folder
c:\Program Files\Novell\GroupWise Server\agents\gwia.exe
                               /home /gwia_folder
c:\Program Files\Novell\GroupWise Server\agents\Monitor\gwmon.exe
                               /home \domain_folder
```

Example:

```
c:\Program Files\Novell\GroupWise Server\agents\gwpoa.exe
                               /home \mail\powin
c:\Program Files\Novell\GroupWise Server\agents\gwmta.exe
                               /home \mail\domwin
c:\Program Files\Novell\GroupWise Server\agents\gwia.exe
                               /home \mail\domwin\gwia
c:\Program Files\Novell\GroupWise Server\agents\Monitor\gwmon.exe
                               /home \mail\domwin
```

Using the Windows GroupWise Agent Log Files

Agent status messages and error messages are written to the agent log files (*mmdagent.nnn*) in the following directories:

POA:	<i>post_office_folder\wpcs\ofs</i>
MTA:	<i>domain_folder\mslocal</i>
GWIA:	<i>domain_folder\wpgate\gwia\000.prc</i>
DVA:	<i>c:\ProgramData\Novell\GroupWise\gwdva</i>
Monitor:	<i>c:\ProgramData\Novell\GroupWise Monitor</i>

NOTE: On some versions of Windows Server, the ProgramData folder is not visible by default. To display it in File Explorer, click **View**, and then select **Hidden items**.

Uninstalling the Windows GroupWise Agents and Applications

If you move the GroupWise agents to a different server, you can uninstall the agent software from the old location to reclaim disk space.

Agents: In the Control Panel, click **Programs and Features**. Right-click **Micro Focus GroupWise Server**, and click **Uninstall**.

Monitor: Stop the Monitor Agent, and then delete the *c:\Program Files\Novell\GroupWise Server\Monitor* folder.

Applications: Stop Tomcat, and then delete the following folder:

```
c:\Novell
```

Monitoring the Agents from Your Web Browser

To monitor any GroupWise agent from your web browser, view the agent console by supplying the IP address or DNS hostname and the port number of the agent. The following table lists the default port numbers:

```
POA:    http://server_network_address:7181
MTA:    http://server_network_address:7180
GWIA:   http://server_network_address:9850
DVA:    http://server_network_address:8301
Monitor: http://server_network_address:8200
```

For more information about the agent consoles, including instructions on protecting the agent consoles with passwords, see the following sections in the [GroupWise 18 Administration Guide](#):

- ♦ [“Using the POA Console”](#)
- ♦ [“Using the MTA Console”](#)
- ♦ [“Using the GWIA Console”](#)
- ♦ [“Using the DVA Console”](#)
- ♦ [“Using the Monitor Web Console”](#)

15 What's Next

After you have created your GroupWise system, you can expand the system in the following ways:

Task	Section in This Guide
Setting up GroupWise WebAccess so that users can access their mailboxes through a web browser on a computer or mobile device	See Setting Up GroupWise WebAccess (Legacy) .
Setting up a GroupWise Calendar Publishing Host so that GroupWise users can share their personal calendars and free/busy information with Internet users	See Setting Up the GroupWise Calendar Publishing Host .
Setting up GroupWise Monitor to monitor your GroupWise agents	See Setting Up GroupWise Monitor .
Setting up users to run the GroupWise client on their workstations	See Installing the GroupWise Client .
Setting up synchronization between users' GroupWise mailboxes and their mobile devices	See Using the GroupWise Mobility Service to Synchronize GroupWise Data to Mobile Devices .
Setting up instant messaging capabilities for users	See Using GroupWise Messenger to Provide Secure Instant Messaging for GroupWise Users .
Setting up team collaboration capabilities	See Using Micro Focus Vibe to Provide Team Workspaces for GroupWise Users .

After your GroupWise system is fully installed, you can maintain your GroupWise system in the following ways:

Task	Section in the <i>GroupWise 18 Administration Guide</i>
Adding multiple domains to your GroupWise system	See "Domains."
Adding post offices to new domains	See "Post Offices."
Adding more users to post offices	See "Users."
Defining resources that users can schedule	See "Resources."
Defining groups of users that GroupWise users can select when addressing messages	See "Groups."
Changing the GroupWise client from Online mode to Caching mode so that users' messages are stored on a local drive as well as in the post office	See "Client."

Task	Section in the <i>GroupWise 18 Administration Guide</i>
Setting up GroupWise Remote so that GroupWise client users can access their mailboxes from a computer that is not directly connected to your network	See “ Client .”
Controlling the functionality of users’ GroupWise client software	See “ Client .”
Setting up a library	See “ Libraries and Documents .”
Configuring the agents to support secure connections (TLS)	See “ Post Office Agent ,” “ Message Transfer Agent ,” “ Internet Agent ,” and “ Document Viewer Agent .”
Configuring GroupWise to run in a clustering environment	See the “ Setting up a GroupWise Cluster ” in the <i>GroupWise 18 Interoperability Guide</i> .

IV

GroupWise Component Installation and Setup

Refer to these sections for information about installing and configuring GroupWise components.

- ♦ [Chapter 16, “Setting Up GroupWise Web,” on page 105](#)
- ♦ [Chapter 17, “Setting Up GroupWise WebAccess \(Legacy\),” on page 115](#)
- ♦ [Chapter 18, “Setting Up the GroupWise Calendar Publishing Host,” on page 127](#)
- ♦ [Chapter 19, “Setting Up GroupWise Monitor,” on page 145](#)
- ♦ [Chapter 20, “Setting Up GroupWise Calendar Server,” on page 163](#)
- ♦ [Chapter 21, “Installing the GroupWise Client,” on page 171](#)
- ♦ [Chapter 22, “Using Other Micro Focus Products with GroupWise,” on page 175](#)

16 Setting Up GroupWise Web

Reference the content in these sections to install or upgrade GroupWise Web. You must have a GroupWise 18.2 or later system installed to be able to use GroupWise Web. The GroupWise System version (backend) must also be equal to or later than the GroupWise Web version. It cannot be an earlier version than GroupWise Web.

NOTE: GroupWise Web replaced GroupWise WebAccess in GroupWise 18.2 and later and is regularly enhanced and updated. WebAccess is no longer maintained or supported.

- ♦ [“GroupWise Web System Requirements” on page 105](#)
- ♦ [“Planning Your GroupWise Web Install” on page 105](#)
- ♦ [“Installing Docker” on page 106](#)
- ♦ [“Downloading and Running the Web Configuration Utility” on page 107](#)
- ♦ [“Downloading and Running the GroupWise Web Image” on page 109](#)
- ♦ [“Upgrading the GroupWise Web Image” on page 111](#)
- ♦ [“Securing GroupWise Web with TLS Connections” on page 112](#)

GroupWise Web System Requirements

The following systems and setups are required to use GroupWise Web:

- ☐ Docker 20.10.6 or later on any Docker supported platform.
- ☐ GroupWise system version equal to or later than the GroupWise Web version.
Your GroupWise Admin Service must also pass certification verification to run the `web-config` utility. For information on certificate verification, see [Securing GroupWise Web using Certificate Verification](#).
- ☐ GroupWise POA with SOAP enabled. SOAP must have SSL enabled.
- ☐ GroupWise DVA with SSL enabled.
- ☐ (Optional) TLS certificates for GroupWise Web.
- ☐ For supported browsers to run GroupWise Web after setup, see [GroupWise Web User Requirements](#).

Planning Your GroupWise Web Install

When planning your GroupWise Web installation, you need to know the following information:

- ♦ Information about your GroupWise system (GroupWise Admin Service username, password, and port).

- ♦ The IP Address or DNS name of your GroupWise Primary Domain.
- ♦ The IP Address or DNS name of a GroupWise POA with SOAP enabled.
- ♦ The location of the `web.conf` file that contains the POA and DVA configuration of your GroupWise system. This is obtained by running the web-config utility. Directions for running this are found in [Downloading and Running the Web Configuration Utility](#).
- ♦ DNS name of your Docker server.
- ♦ IP Address of your DNS server.
- ♦ (Optional) Server certificate and key file for your GroupWise Web server. See [Securing GroupWise Web using a Commercial Certificate](#) for more information.
- ♦ **New in 18.4** - Certificate Verification POA and DVA selection. See [Securing GroupWise Web using Certificate Verification](#) for more information about Certificate Verification.
- ♦ **New in 18.5** - DVA certificate verification is enabled by default. For information, see [Using DVA Certificate Verification](#).

Write all of this information down on the [GroupWise Web Worksheet](#).

Installing Docker

GroupWise Web can be run on any supported Docker platform. Use the links below to find the steps to install Docker on your desired platform:

- ♦ [Docker Install documentation \(https://docs.docker.com/install/overview/\)](https://docs.docker.com/install/overview/)
- ♦ [Docker Hub Docker engine community downloads \(https://hub.docker.com/search/?type=edition&offering=community\)](https://hub.docker.com/search/?type=edition&offering=community)
- ♦ [Docker Engine product page \(https://www.docker.com/products/container-runtime\)](https://www.docker.com/products/container-runtime)

For your convenience, the steps to install Docker on SLES 12/15 and Windows are included below:

- ♦ [“Installing Docker on SLES 12/15” on page 106](#)
- ♦ [“Installing Docker Community on Windows” on page 107](#)

Installing Docker on SLES 12/15

- ☐ Add the **Containers Module** to your server using **YaST > Software > Add System Extensions or Modules**.

NOTE: You can also add the **Containers Module** during the SLES install.

- ☐ In a terminal, run the following commands:

```
sudo zypper install docker
sudo systemctl enable docker
sudo systemctl start docker
sudo usermod -G docker <username> - This command lets the specified
username run docker commands
```

- ☐ Run the following command to test the Docker install:

```
docker run hello-world
```

For more information on Docker on SLES, see the SLES documentation for your version of SLES:

- ♦ **SLES 12:** https://www.suse.com/documentation/sles-12/singlehtml/book_sles_docker/book_sles_docker.html
- ♦ **SLES 15:** https://www.suse.com/documentation/sles-15/singlehtml/book_sles_docker/book_sles_docker.html

Installing Docker Community on Windows

To install Docker Community on Windows, follow the steps found in [Install Docker Desktop on Windows \(https://docs.docker.com/docker-for-windows/install/\)](https://docs.docker.com/docker-for-windows/install/). Docker Community is only supported on Windows 10. If you want to install Docker on a Windows server, you need to contact Docker about purchasing Docker Enterprise.

Downloading and Running the Web Configuration Utility

Before you can run the GroupWise Web image, you must run the `web-config` utility to create five files that have the GroupWise, POA, DVA, and certificate configuration of your GroupWise system. There are two options to download and run the `web-config` utility:

- ♦ **Option 1 - Using the Docker Image** (*recommended*): Using a run command from your Docker server is the recommended way to download and run the `web-config` utility.
- ♦ **Option 2 - Using the Micro Focus Download** (*if required*): If your server does not have access to the Internet you can use this option to download the Docker image from the Micro Focus download site.

IMPORTANT: If you make changes to your GroupWise POAs or DVAs after running this utility, you need to rerun the `web-config` utility to generate new files and stop and start your GroupWise Web container.

New in 18.4 - Your GroupWise Admin Service must pass certificate verification in order for the `web-config` utility to run. For information on certificate verification, see [Securing GroupWise Web using Certificate Verification](#).

New in 18.5 - Beginning in this version, DVA Certificate verification is enabled by default and checked when running the `web-config` utility container and the GroupWise Web container. For information, see [Using DVA Certificate Verification](#).

Option 1 - Using the Docker Image

To download and run the `web-config` utility using Docker:

- ❑ Run the following command to download the `web-config` Docker image on your Docker server:

```
docker pull mfgroupwise/web-config
```
- ❑ Run the following command to create the configuration files specifying in the `Web-Config` location where you want to place the configuration files and filling out the information about your GroupWise system:

```
docker run -it -v <Web-Config Location>:/config -e
GWADMIN_SERVICE=<GroupWise Admin Service Username>@<GroupWise Primary
Domain>:<GroupWise Admin Service Port> -e
GWSOAP_HOST_DEFAULT=<GroupWise POA with SOAP> mfgroupwise/web-config
```

Example command:

```
docker run -it -v /opt/novell/gw:/config -e
GWADMIN_SERVICE=admin@192.168.1.1:9710 -e
GWSOAP_HOST_DEFAULT=192.168.1.2 mfgroupwise/web-config
```

- ❑ If you want to disable DVA verification when running the command to create the configuration files, follow the example below:

Example command disabling DVA verification:

```
docker run -it -v /opt/novell/gw:/config -e
GWADMIN_SERVICE=admin@192.168.1.1:9710 -e
GWSOAP_HOST_DEFAULT=192.168.1.2 -e GWDVA_SSL_VERIFY=off mfgroupwise/
web-config
```

Option 2 - Using the Micro Focus Download

When running the commands below:

- ❑ Download the <gw.version>-xxx-web-config_docker.tar.gz from the GroupWise download site on your docker server.
- ❑ Run the following command to load the docker image (make sure to replace the xxx in the file name):

```
docker load -i <gw.version>-xxx-web-config_docker.tar.gz
```

- ❑ Run the following command to view a list of your docker images. Make sure the web-config image is in the list:

```
docker image list
```

- ❑ Run the following command to create the files specifying in the Web-Config location where you want to place the configuration files and filling out the information about your GroupWise system:

```
docker run -it -v <Web-Config Location>:/config -e
GWADMIN_SERVICE=<GroupWise Admin Service Username>@<GroupWise Primary
Domain>:<GroupWise Admin Service Port> -e
GWSOAP_HOST_DEFAULT=<GroupWise POA with SOAP> mfgroupwise/web-
config:<gw.version>-xxx
```

Example command:

```
docker run -it -v /opt/novell/gw:/config -e
GWADMIN_SERVICE=admin@192.168.1.1:9710 -e
GWSOAP_HOST_DEFAULT=192.168.1.2 mfgroupwise/web-config:<gw.version>-111
```

IMPORTANT: If the GroupWise Admin Service user name you are using is configured with Multi-Factor Authentication, you need to have the user registered with a UI-less method so they can enter their password when prompted as password&ui-lessauthmethod.

- ❑ If you want to disable DVA verification when running the command to create the configuration files, follow the example below:

Example command disabling DVA verification:

```
docker run -it -v /opt/novell/gw:/config -e
GWADMIN_SERVICE=admin@192.168.1.1:9710 -e
GWSOAP_HOST_DEFAULT=192.168.1.2 -e GWDVA_SSL_VERIFY=off mfgroupwise/
web-config:<gw.version>-111
```

Downloading and Running the GroupWise Web Image

The first time you run the GroupWise Web image, you need to specify the folder that has the files created when the `web-config` utility ran and (optionally) your TLS certificates. For convenience, the Web Client can create certificates for your system. For information about certificate best practices and troubleshooting certificate issues in GroupWise and GroupWise Web, see “[Certificate Best Practices](#)” in the *GroupWise 18 Administration Guide*.

There are two options to download and run the `web-config` utility:

- ♦ **Option 1 - Using a Docker Run Command (recommended):** Using a run command from your Docker server is the recommended way to download and run the GroupWise Web image.
- ♦ **Option 2 - Using the Micro Focus Download Site (if required):** If your server does not have access to the Internet you can use this option to download the GroupWise Web image from the Micro Focus download site.

Option 1 - Using a Docker Run Command

To download and run the GroupWise Web image using Docker:

- ❑ Run the following command to pull down the GroupWise Web image:

```
docker pull mfgroupwise/web
```

- ❑ Run the following command to run the image (use the information from the GroupWise Web Worksheet to fill out the command):

```
docker run -d -v <Web-config Location>:/etc/nginx/gw --name gwweb --rm
-e FQDN=<Docker Server Name> -e DNS_SERVER=<DNS Server> -p 80:80 -p
443:443 -v <(Optional) Server Certificate>:/certs mfgroupwise/
web:latest
```

EXAMPLES:

- ♦ To run with GroupWise self-signed certificates:

```
docker run -d --rm -v /opt/novell/gw:/etc/nginx/gw --name gwweb -e
FQDN=webacc.acme.com -e DNS_SERVER=192.168.1.5 -p 80:80 -p 443:443
mfgroupwise/web:18.5.0-111
```

- ♦ To run with commercially signed certificates:

```
docker run -d --rm -v /opt/novell/gw:/etc/nginx/gw --name gwweb -e
FQDN=webacc.acme.com -e DNS_SERVER=192.168.1.5 -p 80:80 -p 443:443 -
v /opt/novell/gw/certs:/certs mfgroupwise/web:18.5.0-111
```

- ♦ To run with commercial certs while disabling DVA verification:

```
docker run -d --rm -v /opt/novell/gw:/etc/nginx/gw --name gwweb -e
FQDN=webacc.acme.com -e DNS_SERVER=192.168.1.5 -p 80:80 -p 443:443 -
v /opt/novell/gw/certs:/certs -e GWDVA_SSL_VERIFY=off mfgroupwise/
web
```

NOTE: /opt/novell/gw/certs should contain the server.key and server.crt files.

You can add --restart always after run -d in the command to have the image restart automatically after rebooting the Docker server. However, if you use --restart, you must remove --rm from your command as they do not work together.

- ❑ (Optional) If you want to run GroupWise Web on different ports than 80 and 443 (this is useful if you have more than one server running in Docker), you should change the initial port number (i.e. -p <port>:80 -p <TLS_port>:443) and add -e TLS_REDIRECT_PORT=<port> -e TLS_REDIRECT_PORT=<TLS_port>.

Example with commercial certs:

```
docker run -d --rm -v /opt/novell/gw:/etc/nginx/gw --name gwweb -e
FQDN=webacc.acme.com -e DNS_SERVER=192.168.1.5 -p 8080:80 -p 8443:443 -
e TLS_REDIRECT_PORT=8080 -e TLS_REDIRECT_PORT=8443 -v /opt/novell/gw/certs:/
certs mfgroupwise/web:18.5.0-111
```

You can now access GroupWise Web by going to https://<Docker_Server_Name>.

Option 2 - Using the Micro Focus Download Site

- ❑ Download the <gw.version>-xxx-web_docker.tar.gz from the GroupWise download site on your Docker server.
- ❑ Run the following command to load the Docker image (make sure to replace the xxx in the file name):

```
docker load -i <gw.version>-xxx-web_docker.tar.gz
```

- ❑ Run the following command to view a list of your Docker images. Make sure the GroupWise Web image is in the list:

```
docker image list
```

- ❑ Run the following command to run the image (use the information from the GroupWise Web Worksheet to fill out the command):

```
docker run -d -v <Web-config Location>:/etc/nginx/gw --name gwweb --rm
-e FQDN=<Docker Server Name> -e DNS_SERVER=<DNS Server> -p 80:80 -p
443:443 -v <(Optional) Server Certificate>:/certs mfgroupwise/
web:<gw.version>-xxx
```

EXAMPLES:

- ♦ To run with GroupWise self-signed certificates:

```
docker run -d --rm -v /opt/novell/gw:/etc/nginx/gw --name gwweb -e
FQDN=webacc.acme.com -e DNS_SERVER=192.168.1.5 -p 80:80 -p 443:443
mfgroupwise/web:18.5.0-111
```

♦ **To run with commercially signed certificates:**

```
docker run -d --rm -v /opt/novell/gw:/etc/nginx/gw --name gwweb -e
FQDN=webacc.acme.com -e DNS_SERVER=192.168.1.5 -p 80:80 -p 443:443 -
v /opt/novell/gw/certs:/certs mfgroupwise/web:18.5.0-111
```

NOTE: /opt/novell/gw/certs should contain the server.key and server.crt files.

You can add --restart always after run -d in the command to have the image restart automatically after rebooting the Docker server. However, if you use --restart, you must remove --rm from your command as they do not work together.

- ❑ (Optional) If you want to run GroupWise Web on different ports than 80 and 443 (this is useful if you have more than one server running in Docker), you should change the initial port number (i.e. -p <port>:80 -p <TLS_port>:443) and add -e TLS_REDIR_PORT=<port> -e TLS_REDIR_PORT=<TLS_port>.

Example with commercial certs:

```
docker run -d --rm -v /opt/novell/gw:/etc/nginx/gw --name gwweb -e
FQDN=webacc.acme.com -e DNS_SERVER=192.168.1.5 -p 8080:80 -p 8443:443 -
e TLS_REDIR_PORT=8080 -e TLS_REDIR_PORT=8443 -v /opt/novell/gw/certs:/
certs mfgroupwise/web:18.5.0-111
```

- ❑ (Optional) If you want to disable DVA certificate verification when you run the web image, follow this command example:

Example command disabling DVA verification with commercial certs:

```
docker run -d --rm -v /opt/novell/gw:/etc/nginx/gw --name gwweb -e
FQDN=webacc.acme.com -e DNS_SERVER=192.168.1.5 -p 80:80 -p 443:443 -v /
opt/novell/gw/certs:/certs -e GWDVA_SSL_VERIFY=off mfgroupwise/
web:18.5.0-111
```

Upgrading the GroupWise Web Image

To update the image to the latest version, you simply need to stop the image and start a new instance with the latest code:

- ❑ To stop and remove the old image, run the following commands:

```
docker stop gwweb
```

```
docker rm gwweb
```

- ❑ Run the following command to pull down the latest webacc-ng image:

```
docker pull mfgroupwise/web
```

- ❑ Re-run the Docker run command that you used in [Downloading and Running the GroupWise Web Image](#) to use the same web-config file and certificates.

Securing GroupWise Web with TLS Connections

These sections contain information for securing GroupWise Web using certificates.

- ♦ [“Securing GroupWise Web using a Commercial Certificate” on page 112](#)
- ♦ [“Updating POA/DVA Certificates while GroupWise Web is Running” on page 112](#)
- ♦ [“Securing GroupWise Web using Certificate Verification” on page 113](#)

Securing GroupWise Web using a Commercial Certificate

GroupWise Web creates self-signed certificates when you run the Docker image. You can supply your own commercial certificates for GroupWise Web for enhanced security. The certificates must follow the requirements found in [“Configuring Server Certificates and TLS”](#) in the *GroupWise 18 Administration Guide*.

When you run with commercially signed certificates, you need to specify the location of the certificates in the Docker run command. Below is an example of the command to run GroupWise Web with commercially signed certificates:

Running GroupWise Web with commercially signed certificates:

```
docker run -d --rm -v /opt/novell/gw:/etc/nginx/gw --name gwweb -e
FQDN=webacc.acme.com -e DNS_SERVER=192.168.1.5 -p 80:80 -p 443:443 -v /opt/
novell/gw/certs:/certs mfgroupwise/web:18.5.0-111
```

`/opt/novell/gw/certs` should contain the `server.key` and `server.crt` files for your commercially signed certificates.

IMPORTANT: At this time, GroupWise Web does not support the use of password protected `.key` files. In order to use a key file that has password protection, you must remove it before running the Docker command above or the Web app will fail when launched. This can be done by running the following command on a machine with OpenSSL installed:

```
openssl rsa -in passwordprotected.key -out nopassword.key
```

Updating POA/DVA Certificates while GroupWise Web is Running

If you update the certificate on the POA/DVA after the GroupWise Web image is running, you can have GroupWise Web grab the new certificates and use the POA/DVA without having to restart the GroupWise Web image. This is also needed if the POA/DVA was not accessible when the GroupWise Web image was started, but is now available. Use the following Docker command to update the certificates:

```
docker exec <container_name or container_id> bash -c "/update/update-
certs.sh"
```

Example: `docker exec gwweb bash -c "/update/update-certs.sh"`

You can use either the container name or the container id to run the command.

NOTE: Restarting the GroupWise Web image also updates the POA/DVA certificates.

Securing GroupWise Web using Certificate Verification

In GroupWise 18.4 and later, GroupWise Web has enhanced security by doing certificate checks for the GroupWise Admin Service, POA, and DVA certificates. The certificate checks make sure the Subject Alternative Name on the certificate matches the GroupWise Admin Server, POA, and DVA and that the certificate date is valid.

The GroupWise Admin Service check is enabled by default and cannot be disabled. The POA check is enabled by default and can be disabled. Beginning in GroupWise 18.5, the DVA check is enabled by default and can be disabled. However, to be fully secure, you should keep all of the certificate verification checks enabled.

NOTE: The POA check and the DVA check are independent of each other and can be run together, separate, or not at all.

As part of the 18.5 changes, the `env.list` file is generated when running the Docker command in the Web Config utility container and the `GWDVA_SSL_VERIFY` switch is added to the file with the switch set to "ON" by default.

- ♦ ["Using GroupWise Admin Service Certificate Verification" on page 113](#)
- ♦ ["Using POA Certificate Verification" on page 113](#)
- ♦ ["Using DVA Certificate Verification" on page 114](#)

Using GroupWise Admin Service Certificate Verification

The GroupWise Admin Service check is done when the `web-config` utility runs to get the POA and DVA information for your GroupWise system. If the GroupWise Admin Service check runs properly, the `web-config` utility creates five files: `web.conf`, `poas.conf`, `dvas.conf`, `env.list` and `ca.crt`.

In order for the GroupWise Admin Service check to pass, you need to use a GroupWise self-signed certificate with the Fully Qualified Domain Name or IP address of the GroupWise server as the Subject Alternative Name on the certificate.

Using POA Certificate Verification

The POA check is part of the running GroupWise Web image and is enabled by default. GroupWise Web checks every POA against its certificate to make sure it matches and is valid.

In order for the POA check to pass, the certificate Subject Alternative Name must match the hostname specified in the `poa.conf` file. Certificate requirements and recommendations can be found in ["Configuring Server Certificates and TLS"](#) in the *GroupWise 18 Administration Guide*.

NOTE: If the Subject Alternative Name in the certificate and the `poa.conf` file do not match, it is easier to change the `poa.conf` file than to get a new certificate.

You do not need to change your Docker run command if you want to use POA certificate verification. If you do not want to use POA certificate verification, you must include the switch `GWSOAP_SSL_VERIFY=off`. Below is an example of running the GroupWise Web Docker image with POA certificate verification turned off:

```
docker run -d --rm -v /opt/novell/gw:/etc/nginx/gw --name gwweb -e
FQDN=webacc.acme.com -e DNS_SERVER=192.168.1.5 -p 80:80 -p 443:443 -v /opt/
novell/gw/certs:/certs -e GWSOAP_SSL_VERIFY=off mfgroupwise/web:18.5.0-111
```

Using DVA Certificate Verification

The DVA check is part of running the GroupWise Web image and is enabled by default beginning in GroupWise 18.5. In order for the DVA check to pass, the certificate Subject Alternative Name (SAN) must match the domain name specified by the `GWDVA_SSL_DNS=` setting in the `env.list` file that is created by the `web.config` utility Docker command. Wildcard certificates can be used for your DVAs as long as the `GWDVA_SSL_DNS=` setting switch specifies the DNS that is in the SAN on the wildcard certificate. Certificate requirements and recommendations can be found in [“Configuring Server Certificates and TLS”](#) in the *GroupWise 18 Administration Guide*.

Although not recommended, you can disable the DVA verification check. If the `env.list` file already exists, you should override the check directly from the file by changing the `GWDVA_SSL_VERIFY` switch to `off`. This file is generated in the `/opt/novell/gw` folder when you run the `web-config` utility.

NOTE: If the `env.list` file does not exist, run the `web-config` utility Docker command to generate the required configuration files including the `env.list` file.

If the `env.list` file does not exist and you are unable to run the `web-config` utility Docker command, and if you do not want to use DVA certificate verification when running the GroupWise Web Docker image, you must include the `GWDVA_SSL_VERIFY=off` switch.

Examples - Running the GroupWise Web Docker Image

Two examples are provided below for running the GroupWise Web Docker image with the DVA check ON and OFF. In both examples, the `env.list` file does not exist:

- ♦ **DVA certificate verification OFF:**

```
docker run -d --rm -v /opt/novell/gw:/etc/nginx/gw --name gwweb -e
FQDN=webacc.acme.com -e DNS_SERVER=192.168.1.5 -p 80:80 -p 443:443 -v /
opt/novell/gw/certs:/certs -e GWDVA_SSL_VERIFY=off mfgroupwise/web
```

- ♦ **DVA certificate verification ON (default), using the `GWDVA_SSL_DNS` switch:**

```
docker run -d --rm -v /opt/novell/gw:/etc/nginx/gw --name gwweb -e
FQDN=webacc.acme.com -e DNS_SERVER=192.168.1.5 -p 80:80 -p 443:443 -v /
opt/novell/gw/certs:/certs -e GWDVA_SSL_DNS=*.lab.acmegwsystem.com
mfgroupwise/web
```

NOTE: The `GWDVA_SSL_DNS` setting is only required or used when DVA certificate verification is ON, not OFF.

17 Setting Up GroupWise WebAccess (Legacy)

IMPORTANT: GroupWise WebAccess is not supported in GroupWise 18.3 and later versions.

GroupWise WebAccess enables users to access GroupWise mailboxes through [desktop web browsers](#), through [tablet devices](#) such as Apple iPads, and through [mobile devices](#). The following sections provide information to help you successfully install the GroupWise WebAccess Application in your existing GroupWise system.

- ♦ [“GroupWise WebAccess Overview” on page 115](#)
- ♦ [“GroupWise WebAccess System Requirements” on page 118](#)
- ♦ [“Planning GroupWise WebAccess” on page 119](#)
- ♦ [“Installing the GroupWise WebAccess Software” on page 121](#)
- ♦ [“Testing GroupWise WebAccess” on page 124](#)
- ♦ [“What’s Next” on page 126](#)
- ♦ [“GroupWise WebAccess Installation Worksheet” on page 126](#)

GroupWise WebAccess Overview

IMPORTANT: GroupWise WebAccess is not supported in GroupWise 18.3 and later versions.

Functionality, components, and security requirements are explained in these sections.

- ♦ [“GroupWise WebAccess Functionality” on page 115](#)
- ♦ [“GroupWise WebAccess Components” on page 116](#)
- ♦ [“WebAccess Security Requirements” on page 116](#)

GroupWise WebAccess Functionality

When used in a desktop web browser, GroupWise WebAccess provides much of the functionality available in the GroupWise client. On a tablet device, the most commonly used functionality is available. WebAccess functionality on mobile devices is limited compared to WebAccess in a desktop browser or on a tablet device.

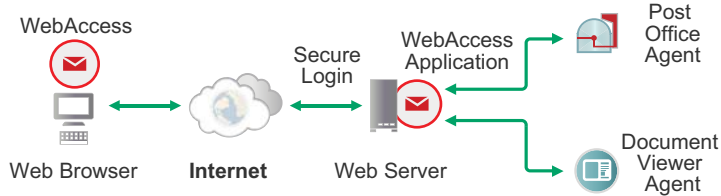
See the following guides for WebAccess user functionality details:

- ♦ [GroupWise 18 WebAccess User Guide](#)
- ♦ [GroupWise 18 WebAccess Mobile User Guide](#)
- ♦ [WebAccess Basic Interface Quick Start](#)

After you set up GroupWise WebAccess, see [What’s Next](#) for additional information that you might want to be aware of as you configure, maintain, and expand GroupWise WebAccess.

GroupWise WebAccess Components

GroupWise WebAccess consists of four components: the browser-based WebAccess user interface (desktop computer, tablet device, or mobile device), the WebAccess Application, the Post Office Agent (POA), and the Document Viewer Agent (DVA).



- ♦ **WebAccess User Interface:** The WebAccess user interface in web browsers gives users access to their GroupWise mailboxes anywhere an Internet connection is available.
- ♦ **WebAccess Application:** The WebAccess Application, which resides on the web server, provides the GroupWise WebAccess user interface. As users perform actions in WebAccess, the WebAccess Application passes information between the web browser and the Post Office Agent.
- ♦ **Post Office Agent:** The POA receives user requests from the WebAccess Application, accesses post offices and libraries to process the requests, and then passes information back to the WebAccess Application.
- ♦ **Document Viewer Agent:** The DVA isolates the conversion process for attached document files. The DVA can simultaneously convert multiple document files into HTML format. If it encounters a problem converting a document file, the problem does not affect conversion of other document files, nor does it affect the functioning of the WebAccess Application. Therefore, GroupWise WebAccess users do not experience interruptions because of document files that fail to convert into HTML. Document files that fail in the conversion process simply cannot be viewed in WebAccess. The DVA is typically installed along with the POA.

WebAccess Security Requirements

The WebAccess Application can be configured to support the level of security you have established for your Internet/intranet communication.

If you are not concerned about security issues (for example, you only plan to use the WebAccess Application on a secured intranet), you can install the WebAccess Application to any web server that provides access for your users and meets the requirements listed in [GroupWise WebAccess System Requirements](#).

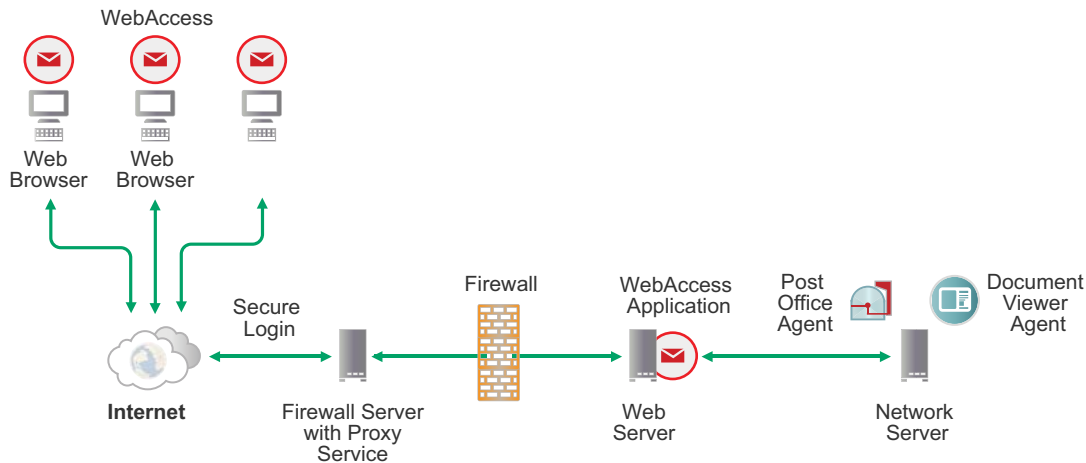
If you plan to use the WebAccess Application to provide users with access to their mailboxes from anywhere on the Internet (rather than only within a secured intranet), and you already have a firewall in place to provide security, you have the following options for configuring the WebAccess Application:

- ♦ Install the WebAccess Application inside your firewall and use a proxy service. See [WebAccess with a Proxy Service](#). This is the recommended configuration.
- ♦ Install the WebAccess Application on a web server outside your firewall, and install the POA and the DVA on a server inside your firewall. See [WebAccess without a Proxy Service](#).

WebAccess with a Proxy Service

If your firewall includes a proxy service, you can install the WebAccess Application to a web server inside your firewall. The POA is located on a post office server, which is also inside the firewall.

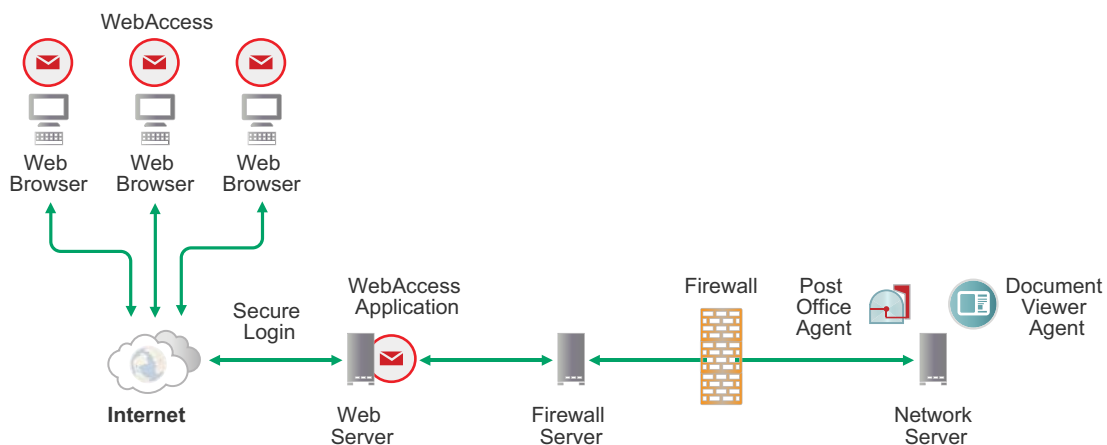
In this configuration, only the firewall server with the proxy service is located outside the firewall, as shown in the following illustration.



WebAccess without a Proxy Service

If your firewall does not provide a proxy service, you need to install the WebAccess Application to a web server that is outside the firewall. The POA is located on a post office server, which is inside the firewall.

In this configuration, both the web server and the firewall server are located outside the firewall, as shown in the following illustration.



The firewall must allow inbound IP packets to be sent from the web server to the IP address and port of the POA (for example, 172.16.5.18:1677).

In addition, the firewall must allow outbound IP packets to be sent from the POA to the web server.

GroupWise WebAccess System Requirements

This section has information about requirements for GroupWise WebAccess.

- ♦ [“Server Requirements” on page 118](#)
- ♦ [“GroupWise Requirements” on page 118](#)
- ♦ [“User Requirements” on page 119](#)

Server Requirements

- ❑ Your server must meet the requirements found in [GroupWise Server Requirements](#).

IMPORTANT: If you are installing on SLES 15 SP1 or later, you need to add the `Python 2 Module 15 SP1 x86_64` module as well as the other modules before installing WebAccess.

- ❑ If installing on OES or SLES:

- ♦ **Apache 2.2 with ModProxy Module:** Apache with ModProxy is installed by the GroupWise install if a Linux repository is available during the install.

IMPORTANT: Apache must be configured with TLS for WebAccess or WebAccess will not work.

- ♦ **Tomcat 9:** Tomcat is installed by the GroupWise install and does not need to be installed on the server.
- ♦ **OpenJDK 11:** OpenJDK is installed by the GroupWise install and does not need to be preinstalled on the server if a Linux repository is available.

A Linux repository should be available when you run the GroupWise Installation Wizard. Apache, the JRE or JDK, and the ModProxy Module are automatically installed from the Linux repository if they are not already present on the Linux server.

If no Linux repository is available during the GroupWise installation, you are prompted to manually install these required components from the Linux media, and then restart the GroupWise installation.

- ❑ If installing on a Windows Server:

- ♦ **Oracle Java Runtime Environment (JRE) 8:** Oracle JRE 8 is automatically installed with the GroupWise software if it is not already present on the server.
- ♦ **Tomcat 9:** Tomcat is installed with the GroupWise installation and does not need to be installed on the server.

- ❑ Adequate server disk space:

- ♦ Approximately 525 MB (shared with the Calendar Publishing Host Application and the Monitor Application when they are installed on the same web server; varies by platform)

GroupWise Requirements

- ❑ One or more Post Office Agents (POAs) configured for SOAP and secure TLS connections.
- ❑ DVA configured with SSL to view documents in WebAccess.

User Requirements

See the following sections for WebAccess requirements for users, both mobile and desktop:

- ♦ [“WebAccess User Requirements” on page 119](#)
- ♦ [“WebAccess Mobile User Requirements” on page 119](#)

WebAccess User Requirements

- ☐ Any of the following web browsers:
 - ♦ **Linux:** Mozilla Firefox; Google Chrome
 - ♦ **Windows:** Microsoft Internet Explorer 11 or later; Mozilla Firefox; Google Chrome; Microsoft Edge
 - ♦ **Macintosh:** The latest version of Safari for your version of Mac OS; Mozilla Firefox; Google Chrome
- ☐ Any mobile device that supports Wireless Access Protocol (WAP) and has a microbrowser that supports Hypertext Markup Language (HTML) 4.0 or later

WebAccess Mobile User Requirements

Any of the following tablet operating systems and tablets:

- ☐ Android 4.1, 5.0, or later, with Google Chrome, on any Android device
- ☐ Apple iOS 7.x, 8.x, 9.x, 10.x, 11.x or later, with Apple Safari
- ☐ Kindle Fire, with Amazon Silk
- ☐ Windows Mobile 8.0 or later Pro, with Microsoft Internet Explorer, on any Windows device (full WebAccess, no template)

Planning GroupWise WebAccess

Use the [GroupWise WebAccess Installation Worksheet](#) to record the information required to install the WebAccess Application.

The topics in this section present the required information in a convenient planning sequence. The Installation Worksheet organizes the information in the order in which you need it during installation.

- ♦ [“Selecting the WebAccess Application Platform” on page 119](#)
- ♦ [“Gathering Web Server Information” on page 120](#)
- ♦ [“Determining the WebAccess Application’s Configuration” on page 120](#)
- ♦ [“Connecting the WebAccess Application with Supporting Agents” on page 121](#)

Selecting the WebAccess Application Platform

The WebAccess Application can be installed to a web server on Linux or Windows. See [GroupWise WebAccess System Requirements](#) for supported web servers.

GROUPWISE WEBACCESS APPLICATION INSTALLATION WORKSHEET

Under **Web Server Platform**, mark whether you plan to install the WebAccess Application to a Linux or Windows web server.

Gathering Web Server Information

The WebAccess Application integrates with your web server to pass mailbox information gathered by the POA to your web browser for display in WebAccess. The location of the WebAccess Application files that are installed depends on the web server that it is being integrated with.

The default web server paths vary by platform:

Apache Web Server on OES:	/etc/opt/novell/httpd/conf.d
Tomcat on OES:	/opt/novell/grpwise-tomcat8/ webapps
Apache Web Server on SLES:	/etc/apache2/conf.d
Tomcat on SLES:	/etc/grpwise-tomcat
Tomcat on Windows:	c:\novell\groupwise\tomcat\webap ps

GROUPWISE WEBACCESS APPLICATION INSTALLATION WORKSHEET

Under **Web Server Information**, select the type of web server where you plan to install the WebAccess Application. Also specify the web server's root directory.

On Windows, if the Internet Information Server services more than one website, specify the website where you want to install the WebAccess Application.

Determining the WebAccess Application's Configuration

WebAccess Application configuration information is stored in a configuration file (`webacc.cfg`). The `webacc.cfg` file is located in the following folders:

Linux: /var/opt/novell/groupwise/webaccess
Windows: c:\novell\groupwise\webaccess

To change the WebAccess Application's configuration, you must manually modify the `webacc.cfg` file.

GROUPWISE WEBACCESS APPLICATION INSTALLATION WORKSHEET

Under **Configuration File Location**, note the location of the `webacc.cfg` file for the platform where you are installing WebAccess.

Connecting the WebAccess Application with Supporting Agents

The WebAccess Agent needs to communicate with a POA.

GROUPWISE WEBACCESS APPLICATION INSTALLATION WORKSHEET

Under **POA Network Address**, specify the IP address or DNS hostname of a POA that the WebAccess Application can communicate with, along with that POA's SOAP port. The default SOAP port for the POA is 7191.

IMPORTANT: The POA that the WebAccess Application communicates with must be configured for SOAP. A secure TLS connection between the POA and the WebAccess Application is highly recommended.

For instructions on preparing the POA to work successfully with the WebAccess Application, see the following sections in the [GroupWise 18 Administration Guide](#):

- ♦ [“Supporting SOAP Clients”](#)
- ♦ [“Securing the Post Office with SSL Connections to the POA”](#)

For instructions on preparing the DVA to work successfully with the WebAccess Application, see the following sections in the [GroupWise 18 Administration Guide](#):

- ♦ [“Multiple DVAs for WebAccess”](#)
- ♦ [“Installing the DVA”](#)

Installing the GroupWise WebAccess Software

As you install the WebAccess software, use the [GroupWise WebAccess Installation Worksheet](#) that you filled out in [Planning GroupWise WebAccess](#) to provide the required information.

- ♦ [“Linux: Installing the GroupWise WebAccess Software” on page 121](#)
- ♦ [“Windows: Installing the GroupWise WebAccess Software” on page 122](#)

Linux: Installing the GroupWise WebAccess Software

Reference the sections below for information about installing GroupWise WebAccess on Linux.

- ♦ [“Preparing the Linux Server for GroupWise WebAccess” on page 121](#)
- ♦ [“Installing the Linux WebAccess Software” on page 122](#)

Preparing the Linux Server for GroupWise WebAccess

To prepare the Linux server for GroupWise WebAccess:

- 1 Ensure that the web server where you are installing the WebAccess Application meets the system requirements listed in [GroupWise WebAccess System Requirements](#).
- 2 Ensure that the Linux operating system media is available, either physically or in a repository, in case the Installation Wizard needs to install supporting packages on the Linux server.

- 3 Ensure that the server has a static IP address.
- 4 Ensure that the POA that the WebAccess Application will communicate with has SOAP enabled on a secure TLS connection, as described in [Connecting the WebAccess Application with Supporting Agents](#).
- 5 Continue with [Installing the Linux WebAccess Software](#).

Installing the Linux WebAccess Software

To install Linux WebAccess software:

- 1 Download and extract the GroupWise 18 software to a temporary location on your server.
- 2 In a terminal window, become `root` by entering `su -` and the `root` password.
- 3 Browse to the location of the extracted software, and run the following command to start the install:

```
./install.sh
```

- 4 Type the number for the language in which you want to run the GroupWise Installation Wizard, and press Enter to select **OK**.
- 5 (Optional) Type 1 for **Documentation**, and then press Enter to review the Readme, Quick Start, and Installation Guide to better prepare yourself for the installation.
- 6 Type 2 for **Installation** and press Enter.
- 7 Enter `a` to accept the License Agreement and to display the Software list.
- 8 Type 2 for **GroupWise WebAccess**, to display the Actions list.
- 9 Enter 1 for **Install** and to install GroupWise WebAccess.

The WebAccess package is installed on the server. If any supporting packages are not available on the server, the Installation Wizard automatically installs them from the operating system media.

- 10 When the installation is finished, press any key to return to the Installation Options list.
- 11 Enter 2 for **Configure** to configure the WebAccess Application.
- 12 Follow the prompts to configure the WebAccess Application, using the following information from the [GroupWise WebAccess Installation Worksheet](#):

[POA Network Address](#)

[Web Server Information](#)

- 13 Press any key to exit WebAccess Configuration.
- 14 Exit the GroupWise Installation Wizard.
- 15 Continue with [Testing GroupWise WebAccess](#).

Windows: Installing the GroupWise WebAccess Software

Reference the sections below for information about installing GroupWise WebAccess on Windows.

- ♦ [“Preparing the Windows Server for GroupWise WebAccess” on page 123](#)
- ♦ [“Installing the Windows WebAccess Software” on page 123](#)

Preparing the Windows Server for GroupWise WebAccess

To prepare the Windows Server for GroupWise WebAccess installation:

- 1 Ensure that the web server where you are installing the WebAccess Application meets the system requirements listed in [“GroupWise WebAccess System Requirements” on page 118](#).
- 2 Ensure that the server has a static IP address.
- 3 Ensure that the POA that the WebAccess Application will communicate with has SOAP enabled on a secure TLS connection, as described in [“Connecting the WebAccess Application with Supporting Agents” on page 121](#).
- 4 Continue with [Installing the Windows WebAccess Software](#).

Installing the Windows WebAccess Software

To install the Windows WebAccess software:

- 1 Run `setup.exe` at the root of the extracted GroupWise software to start the GroupWise Installation Wizard.
- 2 (Optional) Review the Readme, Quick Start, and Installation Guide to better prepare yourself for the installation.
- 3 Click **GroupWise WebAccess**.
- 4 Click **Next** to display the Web Server Information page.

The Installation Wizard provides diagrams that help you understand how the various components interact with each other. Review the diagrams as you provide the requested information.
- 5 Follow the prompts to configure the WebAccess Application, using the following information from the [GroupWise WebAccess Installation Worksheet](#):
[Web Server Information](#)
[POA Network Address](#)
- 6 Click **Next** to display the Installation Summary.
- 7 Review the Installation Summary page, and then click **Install** to install the WebAccess Application.
- 8 (Conditional) If prompts appear because your web server is running, decide whether you want the Installation Wizard to stop your web server.
- 9 When the installation is complete, click **Finish** to exit the WebAccess Installation Wizard.

You can choose to have the Installation Wizard restart the web server for you.

Along with the WebAccess Application, the WebAccess Installation Wizard also installs Tomcat 9 to `c:\novell\tomcat`, integrates it with your web server, and automatically starts it to support the WebAccess Application.
- 10 Exit the GroupWise Installation Wizard.
- 11 Continue with [Testing GroupWise WebAccess](#).

Testing GroupWise WebAccess

After you have installed WebAccess, you should test it in the environments where you think that your GroupWise users will typically use it.

- ♦ [“Testing WebAccess on a Workstation” on page 124](#)
- ♦ [“Testing WebAccess on a Tablet Device” on page 124](#)
- ♦ [“Testing the WebAccess Basic Interface on a Mobile Device” on page 125](#)
- ♦ [“Assisting Users with Login Problems” on page 125](#)
- ♦ [“Monitoring the WebAccess Application” on page 125](#)

Testing WebAccess on a Workstation

To test WebAccess on a workstation:

- 1 To access GroupWise WebAccess, use the following URL:

```
http://web_server_address/gw/webacc
```

Replace *web_server_address* with the IP address or DNS hostname of your web server. If the web server uses TLS, use `https` rather than `http`.

- 2 Type your GroupWise user name in the **User Name** field and your GroupWise mailbox password in the **Password** field.
- 3 (Optional) Click **Settings**, and then select the interface language you want from the **Language** drop-down list.
- 4 Click **Login** to display the GroupWise WebAccess main window.
- 5 Click **Options > Help** for more information about using GroupWise WebAccess.

Testing WebAccess on a Tablet Device

To test WebAccess on a tablet device:

- 1 To access GroupWise WebAccess on a tablet device such as an iPad, use the following URL:

```
http://web_server_address/gw/webacc
```

Replace *web_server_address* with the IP address or DNS hostname of your web server. If the web server uses TLS, use `https` rather than `http`.

or

(Conditional) If you have a tablet device that is not yet [supported](#), but you want to see how well the mobile interface works on your device, use the following URL:

```
http://web_server_address/gw/webacc?User.interface=mobile
```

Replace *web_server_address* with the IP address or DNS hostname of your web server. If the web server uses TLS, use `https` rather than `http`.

- 2 Type your GroupWise user name in the **User Name** field and your GroupWise mailbox password in the **Password** field.

- 3 (Optional) Tap **Settings**, and then select the interface language you want from the **Language** drop-down list.
- 4 Tap **Login** to display the GroupWise WebAccess main window.
- 5 Tap **Options** > **Help** for more information about using GroupWise WebAccess on your iPad.

Testing the WebAccess Basic Interface on a Mobile Device

To test the WebAccess basic interface on a mobile device:

- 1 To access GroupWise WebAccess in the web browser on your mobile device, use the following URL:

```
http://web_server_address/gw/webacc
```

Replace *web_server_address* with the IP address or DNS hostname of your web server. If the web server uses TLS, use https rather than http.

- 2 Follow the instructions in your mobile device's documentation to add this URL to your Favorites or Bookmarks so you do not need to type the URL every time you log in on your mobile device.
- 3 Type your GroupWise user name in the **User Name** field and your GroupWise mailbox password in the **Password** field.
- 4 Tap **Login** to display the GroupWise WebAccess main window.

The appearance of the WebAccess basic interface varies depending on the size of the screen where it is displayed.

For more information about using WebAccess on your mobile device, see the [WebAccess Basic Interface Quick Start](#).

As an alternative to this limited interface, you can synchronize GroupWise data to your mobile device using the GroupWise Mobility Service. For more information, see the *GroupWise Mobility Service 18 Administration Guide* on the [GroupWise documentation site](#).

Assisting Users with Login Problems

The WebAccess Login page includes a **Can't log in** link, which provides the following information to WebAccess users by default:

If you have forgotten your GroupWise password, contact your local GroupWise administrator.

For your convenience and for the convenience of your WebAccess users, you can customize the information that is provided by the **Can't log in** link. For setup instructions, see "[Helping Users Who Forget Their GroupWise Passwords](#)" in the *GroupWise 18 Administration Guide*.

Monitoring the WebAccess Application

You can monitor the WebAccess Application from your web browser. For more information, see "[Using the WebAccess Application Console](#)" in the *GroupWise 18 Administration Guide*.

What's Next

You can further configure and maintain GroupWise WebAccess in the following ways:

Task	Section in the <i>GroupWise 18 Administration Guide</i>
Scale GroupWise WebAccess to meet the needs of your users and environment	See “Scaling Your GroupWise WebAccess Installation.”
Control users’ access to GroupWise WebAccess	See “Managing User Access” and “Helping Users Who Forget Their GroupWise Passwords.”
Configure the WebAccess Application	See “Configuring the WebAccess Application.”
Monitor the WebAccess Application	See “Monitoring the WebAccess Application.”
Control logging for the WebAccess Application	See “Using WebAccess Application Log Files.”

GroupWise WebAccess Installation Worksheet

Installation Wizard Field	Value for Your GroupWise System	Explanation
Web Server Platform		Selecting the WebAccess Application Platform
<ul style="list-style-type: none"> ♦ Linux ♦ Windows 		
POA Network Address		Connecting the WebAccess Application with Supporting Agents
<ul style="list-style-type: none"> ♦ IP address ♦ SOAP port (default 7191) 		
Web Server Information		Gathering Web Server Information
<ul style="list-style-type: none"> ♦ Apache path ♦ Tomcat path 		
Configuration File Location		Gathering Web Server Information
Linux		
/var/opt/novell/ groupwise/webaccess		
Windows		
c:\novell\groupwise\ webaccess		

18 Setting Up the GroupWise Calendar Publishing Host

The GroupWise Calendar Publishing (CalPub) Host publishes GroupWise users' calendars to the Internet, so that the calendars are readily available to colleagues who are not part of the GroupWise system. The CalPub Host also returns free/busy schedule status to Internet colleagues who want to set up appointments with GroupWise users. The free/busy search checks the main GroupWise Calendar and personal calendars.

- ♦ [“GroupWise Calendar Publishing Host Overview” on page 127](#)
- ♦ [“GroupWise Calendar Publishing Host System Requirements” on page 130](#)
- ♦ [“Planning a GroupWise Calendar Publishing Host” on page 131](#)
- ♦ [“Installing the GroupWise Calendar Publishing Host” on page 135](#)
- ♦ [“Configuring GroupWise to Support the Calendar Publishing Host” on page 138](#)
- ♦ [“Testing GroupWise Calendar Publishing” on page 141](#)
- ♦ [“What’s Next” on page 142](#)
- ♦ [“GroupWise Calendar Publishing Host Worksheets” on page 142](#)

GroupWise Calendar Publishing Host Overview

Reference these sections for an overview of GroupWise Calendar Publishing functionality, components, and security requirements.

- ♦ [“GroupWise Calendar Publishing Host Functionality” on page 127](#)
- ♦ [“GroupWise Calendar Publishing Host Components” on page 128](#)
- ♦ [“GroupWise Calendar Publishing Host Security Requirements” on page 128](#)

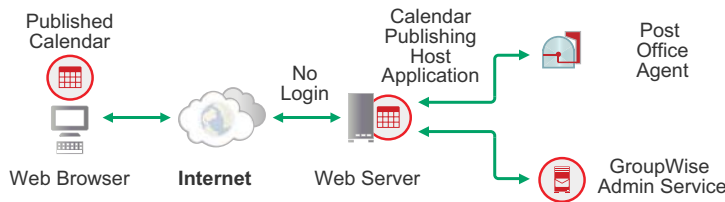
GroupWise Calendar Publishing Host Functionality

The CalPub Host enables Internet users to view GroupWise users' published calendars and to retrieve free/busy information from their calendars to assist with scheduling available appointment times. Internet users do not need login access to the GroupWise system in order to view published calendars and obtain free/busy status. Information provided by the CalPub Host is publicly available to Internet users everywhere.

For calendar publishing user functionality details, see the [GroupWise 18 Calendar Publishing Quick Start](#).

GroupWise Calendar Publishing Host Components

The CalPub Host includes three components: the CalPub Host Application, which connects to the Internet through a web server, the Post Office Agent (POA), which connects to your GroupWise system, and the GroupWise Administration Service, which provides authentication to the CalPub Host Administration console.



- ♦ **Calendar Publishing Host Application:** The CalPub Host Application, which resides on the web server, provides the browser interface for users across the Internet. As users request calendar and free/busy information from GroupWise users, the CalPub Host Application passes the information between the web browser and the POA.
- ♦ **Post Office Agent:** The POA receives user requests from the CalPub Host Application, accesses post offices and mailboxes to process the requests, and then passes information back to the CalPub Host Application in the form of ICS (Internet Calendaring and Scheduling) files and IFB (Internet Free Busy) files. These files can be imported into GroupWise, Outlook, and Macintosh iCal calendaring applications.
- ♦ **GroupWise Admin Service:** The CalPub Host has an Administration console for configuration and management tasks. You can authenticate to the CalPub Host Admin console by using the user name and password of any GroupWise administrator user.

GroupWise Calendar Publishing Host Security Requirements

The CalPub Host Application can be configured to support the level of security you have established for your Internet/intranet communication.

If you are not concerned about security issues (for example, you only plan to use the CalPub Host Application on a secured intranet), you can install the CalPub Host Application to any web server that provides access for your users and meets the requirements listed in [GroupWise Calendar Publishing Host System Requirements](#).

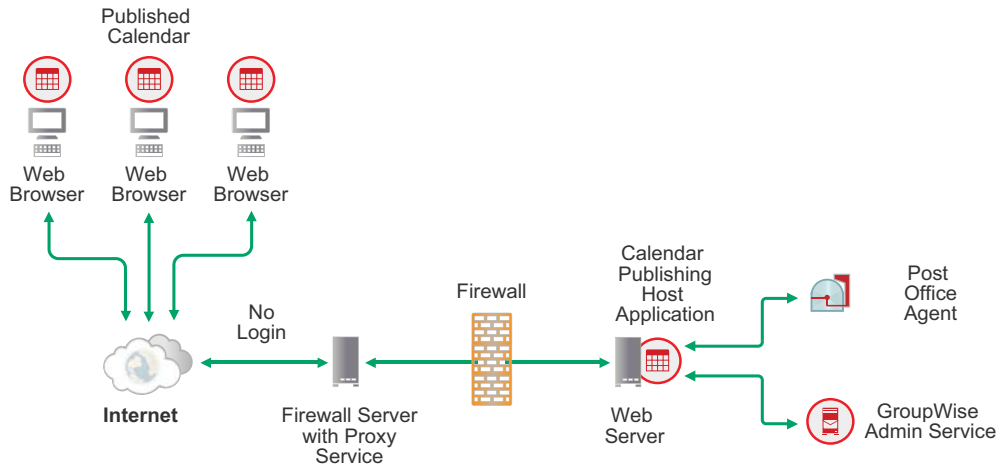
If you plan to use the CalPub Host Application to provide calendar and free/busy information to users anywhere on the Internet (rather than simply within a secured intranet), and you already have a firewall in place to provide security, you have the following options for configuring the CalPub Host Application:

- ♦ Install the CalPub Host Application inside your firewall and use a proxy service, as described in [Calendar Publishing Host with a Proxy Service](#). This is the recommended configuration.
- ♦ Install the CalPub Host Application on a web server outside your firewall and have it communicate with a POA through your firewall, as described in [Calendar Publishing Host without a Proxy Service](#).

Calendar Publishing Host with a Proxy Service

If your firewall includes a proxy service, you can install the CalPub Host Application to a web server inside your firewall. The POA is located on a post office server, which is also located inside the firewall.

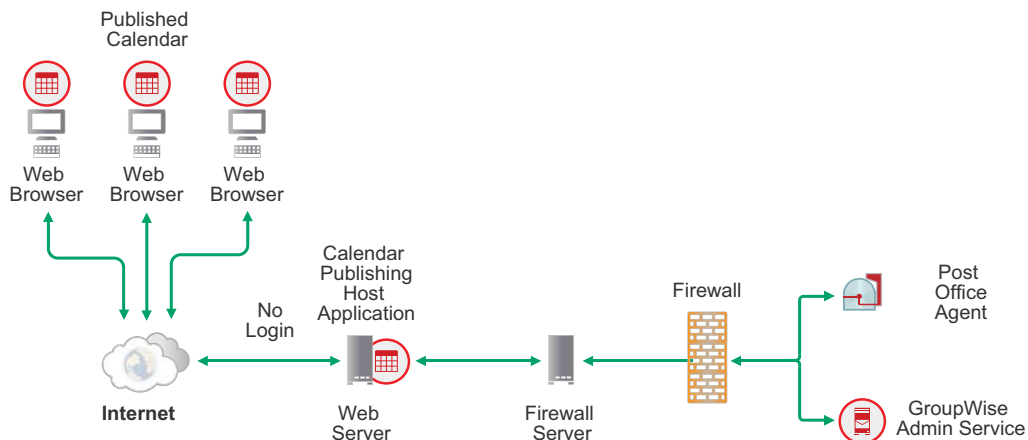
In this configuration, only the firewall server with the proxy service is located outside the firewall, as shown in the following illustration.



Calendar Publishing Host without a Proxy Service

If your firewall does not provide a proxy service, you need to install the CalPub Host Application to a web server that is outside the firewall. The POA is located on a post office server, which is located the firewall.

In this configuration, both the web server and the firewall server are located outside the firewall, as shown in the following illustration.



The firewall must allow inbound IP packets to be sent from the web server to the POA's internal or external IP address and the calendar publishing port for the POA (for example, 172.16.5.18:7171). If you are using an external IP address, all POAs that support calendar publishing must be configured

to use the same external IP address. For more information about external POA IP addresses, see [“Securing Client Access through an External Proxy Server”](#) in the *GroupWise 18 Administration Guide*.

In addition, the firewall must allow outbound IP packets to be sent from the POA to the web server.

GroupWise Calendar Publishing Host System Requirements

Reference these sections for server and web browser requirements for Calendar Publishing:

- ♦ [“Server Requirements” on page 130](#)
- ♦ [“Web Browser Requirements” on page 131](#)

Server Requirements

- ❑ Your server must meet the requirements found in [GroupWise Server Requirements](#).

IMPORTANT: If you are installing on SLES 15 SP1, you need to add the “Python 2 Module 15 SP1 x86 64” module as well as the other modules before installing CalPub.

- ❑ If installing on OES or SLES:

- ♦ **Apache 2.2 with ModProxy Module:** Apache with ModProxy is installed by the GroupWise install if a Linux repository is available during the install.

IMPORTANT: Apache must be configured with TLS for WebAccess or WebAccess will not work.

- ♦ **Tomcat 9:** Tomcat is installed by the GroupWise install and does not need to be installed on the server.
- ♦ **OpenJDK 11:** OpenJDK is installed by the GroupWise install and does not need to be preinstalled on the server if a Linux repository is available.
- ♦ **OES11 / OES 2015 / OES 2018 / SLES 11:** IBM Java Runtime Environment (JRE) 8 or later
SLES 12 / SLES 15: OpenJDK 11

A Linux repository should be available when you run the GroupWise Installation Wizard. Apache, the JRE or JDK, and the ModProxy Module are automatically installed from the Linux repository if they are not already present on the Linux server.

If no Linux repository is available during the GroupWise installation, you are prompted to manually install these required components from the Linux media, and then restart the GroupWise installation.

- ❑ If installing on a Windows Server:

- ♦ **Oracle Java Runtime Environment (JRE) 8:** Oracle JRE 8 is automatically installed with the GroupWise software if it is not already present on the server.
- ♦ **Tomcat 9:** Tomcat is installed with the GroupWise install and does not need to be installed on the server.

- ❑ Adequate server disk space:
 - ♦ Approximately 525 MB (shared with the WebAccess Application and the Monitor Application when they are installed on the same web server; varies by platform)
 - ♦ 50 KB per published calendar
 - ♦ 50 KB per user for free/busy searching

Web Browser Requirements

Any of the following web browsers for the GroupWise Calendar Publishing Host user web pages and the Calendar Publishing Host Administration console:

- ❑ **Linux:** Mozilla Firefox; Google Chrome
- ❑ **Windows:** Microsoft Internet Explorer 11 or later; Mozilla Firefox; Google Chrome; Microsoft Edge
- ❑ **Macintosh:** The latest version of Safari for your version of Mac OS; Mozilla Firefox; Google Chrome

Planning a GroupWise Calendar Publishing Host

Use the [GroupWise Calendar Publishing Host Worksheets](#) to record the information required to install and configure the CalPub Host Application.

The topics in this section present the required information in a convenient planning sequence. The Installation Worksheet organizes the information in the order in which you need it during installation.

- ♦ [“Selecting the Calendar Publishing Host Application Platform” on page 131](#)
- ♦ [“Gathering Web Server Information” on page 132](#)
- ♦ [“Choosing the Calendar Publishing Host Name” on page 132](#)
- ♦ [“Determining the URL of the Calendar Publishing Host” on page 133](#)
- ♦ [“Selecting a Calendar Publishing Host Administrator” on page 133](#)
- ♦ [“Connecting the Calendar Publishing Host to a POA” on page 134](#)
- ♦ [“Designing Your Calendar Browse List” on page 134](#)
- ♦ [“Selecting Calendar Publishing Settings” on page 135](#)

Selecting the Calendar Publishing Host Application Platform

The CalPub Host can be installed to a web server on Linux or Windows. See [GroupWise Calendar Publishing Host System Requirements](#) for supported web servers.

GROUPWISE CALENDAR PUBLISHING HOST INSTALLATION WORKSHEET

Under **Web Server Platform**, mark whether you plan to install the CalPub Host Application to a Linux or Windows web server.

Gathering Web Server Information

The CalPub Host Application integrates with your web server to pass calendar information gathered by the Post Office Agent to your web browser for display. The location of the CalPub Application files that are installed depends on the web server that it is being integrated with.

The default web server paths vary by platform:

Apache Web Server on OES:	<code>/etc/opt/novell/httpd/conf.d</code>
Tomcat on OES:	<code>/opt/novell/grpwise-tomcat8/ webapps</code>
Apache Web Server on SLES:	<code>/etc/apache2/conf.d</code>
Tomcat on SLES:	<code>/etc/grpwise-tomcat</code>
Tomcat on Windows:	<code>c:\novell\groupwise\tomcat\webap ps</code>

GROUPWISE CALENDAR PUBLISHING HOST INSTALLATION WORKSHEET

Under **Web Server Information**, select the type of web server where you plan to install the CalPub Host Application. Also specify the web server's root directory.

On Windows, if the Internet Information Server services more than one website, specify the website where you want to install the CalPub Host Application.

The CalPub Host needs the IP address and TCP port number of the web server so that they can communicate.

GROUPWISE CALENDAR PUBLISHING HOST CONFIGURATION WORKSHEET

Under **Calendar Publishing Host Configuration**, list the IP address of the web server and the web server port number (by default, 80).

Choosing the Calendar Publishing Host Name

You must provide a unique and descriptive name for the CalPub Host. The name might include the platform or location of the CalPub Host, or perhaps the users it serves. You specify this name when you install the CalPub Host Application and again when you configure it in the GroupWise Admin console. The name must be specified identically in both places, including spacing and capitalization.

The CalPub Host name is stored in the `calhost.cfg` file, located in the following folders:

Linux:	<code>/var/opt/novell/groupwise/calhost</code>
Windows:	<code>c:\novell\groupwise\calhost</code>

GROUPWISE CALENDAR PUBLISHING HOST INSTALLATION WORKSHEET

Under **Calendar Publishing Host Name**, specify a unique name for this CalPub Host.

GROUPWISE CALENDAR PUBLISHING HOST CONFIGURATION WORKSHEET

Under **Calendar Publishing Host Configuration**, list the name for the CalPub Host name again. Ensure that the names are specified identically on both worksheets.

If desired, provide a helpful description of the CalPub Host.

Determining the URL of the Calendar Publishing Host

The CalPub Host uses the DNS hostname of the web server as part of its base URL.

`http://web_server_address:port/gwcal`

Replace *web_server_address* with the DNS hostname of the web server. Replace *port* with the port number on which the CalPub Host communicates with the web server. The default port number is 80; it does not need to be specified if your web server uses that default.

IMPORTANT: Select the URL carefully. This URL is disseminated by GroupWise users to their Internet colleagues when they publish their personal calendars and free/busy information. If you change the URL later, GroupWise users need to send updated information to Internet colleagues.

You might want to create a generic URL, such as `http://gwcal.example.com/gwcal`, and then configure your network to redirect incoming traffic to the CalPub Host server.

GROUPWISE CALENDAR PUBLISHING HOST CONFIGURATION WORKSHEET

Under **Calendar Publishing Host Configuration**, list the CalPub Host base URL (`http://web_server_address/gwcal`).

You typically need only one CalPub Host in your GroupWise system. However, depending on the size of your GroupWise system and the locations of your GroupWise users, you might need multiple CalPub Hosts in various locations if some users experience slowness when accessing the initial location.

Selecting a Calendar Publishing Host Administrator

The web-based CalPub Admin console is provided for additional configuration of the CalPub Host. You must select at least one GroupWise user to access the Calpub Admin console. You might want to select a GroupWise user who is already a GroupWise system administrator, domain administrator, or post office administrator, but this is not required. Any GroupWise user can be a CalPub Host administrator.

The CalPub administrator logs into the CalPub Admin console using the same user name and password that is used for mailbox access.

GROUPWISE CALENDAR PUBLISHING HOST CONFIGURATION WORKSHEET

Under **Authentication Information**, list at least one GroupWise user to serve as a CalPub Host administrator.

Connecting the Calendar Publishing Host to a POA

The CalPub Host connects to your GroupWise system through the POA of a post office. For initial installation, you enable one POA for calendar publishing. As you roll out calendar publishing to your GroupWise users, you must enable calendar publishing for the POA of every post office where users publish calendars and free/busy information.

The initially selected POA must be configured to communicate with the CalPub Host. The POA server's IP address or DNS hostname is required, along with a calendar publishing port. The default calendar publishing port is 7171.

Use the default port number unless it is already in use on the server.

GROUPWISE CALENDAR PUBLISHING HOST INSTALLATION WORKSHEET

Under **Post Office Agent Information**, specify the IP address or DNS hostname of the POA that will communicate with the CalPub Host, along with the calendar publishing port number. The default calendar publishing port is 7171.

GROUPWISE CALENDAR PUBLISHING HOST CONFIGURATION WORKSHEET

Under **Calendar Publishing Post Office**, transfer the IP address or DNS hostname of the POA, along with the calendar publishing port from the *Installation Worksheet* to the **Configuration Worksheet**. You need this information during installation and during configuration.

For a complete list of default port numbers used by the GroupWise agents, see “[GroupWise Port Numbers](#)” in the *GroupWise 18 Administration Guide*.

Designing Your Calendar Browse List

The CalPub Host collects a list of published calendars for Internet users to browse and select from at the following URL:

`http://web_server_address/gwcal/calendar`

However, by default, no calendars are displayed in this calendar browse list. You can handle the calendar browse list in three different ways:

- ♦ Do not provide a calendar browse list.

Users need to notify Internet colleagues by email of the URL to access their published calendars.

- ♦ Use the calendar browse list only for calendars of general corporate interest.

If you want to have such a corporate browse list, you restrict which users can list calendars on the browse list by allowing only a few specific users who manage the corporate calendars to publish to the calendar browse list.

- ♦ Allow most, if not all, users to publish their personal calendars on the calendar browse list.

This open approach to the calendar browse list makes users' published calendars easily accessible to anyone who knows the URL of the calendar browse list for your GroupWise system.

GROUPWISE CALENDAR PUBLISHING HOST CONFIGURATION WORKSHEET

Under **Calendar Browse List**, mark whether you want to enable the calendar browse list, and if so, what kind (corporate or open).

Selecting Calendar Publishing Settings

After you have set up the CalPub Host, you can configure how you want it to work for your GroupWise users. The following settings are available in the GroupWise Admin Console:

- ♦ **Enable Calendar Publishing:** Enables users to publish personal GroupWise calendars on the Internet. When calendar publishing is enabled, users of the GroupWise client and GroupWise WebAccess can right-click a personal calendar, and then click **Publish** to select options for publishing a personal calendar.
- ♦ **Enable Rules To Move Items to a Published Calendar:** Enables users to create rules that move specific items to a published GroupWise calendar. Rules are disabled by default.
- ♦ **Enable Publish Free/Busy Search:** Enables users to make their appointment information available to external users, so external users can perform Free/Busy Searches on users' GroupWise calendars. Free/Busy searching is disabled by default. Free/busy publishing can be enabled even if no Calendar Publishing Host has been selected.
- ♦ **Enable Subscribe to Calendar:** Enables users to subscribe to Internet calendars that are updated on a regular basis, such as calendars for sporting events. Calendar subscription is disabled by default. Calendar subscription can be enabled even if no Calendar Publishing Host has been selected.

GROUPWISE CALENDAR PUBLISHING HOST CONFIGURATION WORKSHEET

Under **Calendar Publishing Options**, mark the options you want to enable for the CalPub Host.

Installing the GroupWise Calendar Publishing Host

As you set up the CalPub Host, use the [GroupWise Calendar Publishing Host Worksheets](#) that you filled out in [Planning a GroupWise Calendar Publishing Host](#) to provide the required information.

- ♦ [“Linux: Installing the Calendar Publishing Host Software” on page 135](#)
- ♦ [“Windows: Installing the Calendar Publishing Host Software” on page 137](#)

Linux: Installing the Calendar Publishing Host Software

The sections below have instructions for preparing and installing the Calendar Publishing Host on a Linux Server.

- ♦ [“Preparing the Linux Server for the Calendar Publishing Host” on page 136](#)
- ♦ [“Installing the Linux Calendar Publishing Host Software” on page 136](#)

Preparing the Linux Server for the Calendar Publishing Host

To prepare the Linux Server for the Calendar Publishing Host:

- 1 Ensure that the web server where you are installing the CalPub Host Application meets the system requirements listed in [GroupWise Calendar Publishing Host System Requirements](#).
- 2 Ensure that the Linux operating system media is available, either physically or in a repository, in case the Installation Wizard needs to install supporting packages on the Linux server.
- 3 Ensure that the server has a static IP address.
- 4 Continue with [Installing the Linux Calendar Publishing Host Software](#).

Installing the Linux Calendar Publishing Host Software

To install the Calendar Publishing Host on a Linux Server:

- 1 In a terminal window, become `root` by entering `su -` and the `root` password.
- 2 Browse to the location of the extracted software, and run the following command to start the install:

```
./install.sh
```

- 3 Type the number for the language in which you want to run the GroupWise Installation Wizard, and press Enter to select **OK**.
- 4 (Optional) Type 1 for **Documentation**, and then press Enter to review the Readme, Quick Start, and Installation Guide to better prepare yourself for the installation.
- 5 Type 2 for **Installation** and press Enter.
- 6 Enter `a` to accept the License Agreement and to display the Software list.
- 7 Type 3 for **Calendar Publishing Host**, to display the Actions list.
- 8 Enter 1 for **Install** and to install the GroupWise Calendar Publishing Host.

The CalPub Host package is installed on the server. If any supporting packages are not available on the server, the Installation Wizard automatically installs them from the operating system media.

- 9 When the installation is finished, press any key to return to the Installation Options list.
- 10 Enter 2 for **Configure** to configure the CalPub Host Application
- 11 Follow the prompts to configure the CalPub Host Application, using the following information from the [Calendar Publishing Host Installation Worksheet](#):

[Calendar Publishing Host Name](#)

[Post Office Agent Information](#)

[Web Server Information](#)

- 12 When the installation is finished, review the instructions for configuring the Calendar Publishing Host.
- 13 Press any key to exit CalPub Host Configuration.
- 14 Exit the GroupWise Installation Wizard.
- 15 Continue with [Configuring the Calendar Publishing Host in the GroupWise Admin Console](#).

Windows: Installing the Calendar Publishing Host Software

Reference the following sections, to install the Calendar Publishing Host on a Windows Server.

- ♦ [“Preparing the Windows Server for the Calendar Publishing Host” on page 137](#)
- ♦ [“Installing the Windows Calendar Publishing Host Software” on page 137](#)

Preparing the Windows Server for the Calendar Publishing Host

To prepare the Windows Server for the Calendar Publishing Host installation:

- 1 Ensure that the web server where you are installing the CalPub Host Application meets the system requirements listed in [“GroupWise Calendar Publishing Host System Requirements” on page 130](#).
- 2 Ensure that the server has a static IP address.
- 3 Continue with [Installing the Windows Calendar Publishing Host Software](#).

Installing the Windows Calendar Publishing Host Software

To install the Calendar Publishing Host on Windows Server:

- 1 Run `setup.exe` at the root of the extracted GroupWise software to start the GroupWise Installation Wizard.
- 2 (Optional) Review the Readme, Quick Start, and Installation Guide to better prepare yourself for the installation.
- 3 Click **GroupWise Calendar Publishing Host**.
- 4 Click **Next** to display the Calendar Publishing Host Name page.
The Installation Wizard provides diagrams that help you understand how the various components interact with each other. Review the diagrams as you provide the requested information.
- 5 Follow the prompts to configure the CalPub Host Application, using the following information from the [Calendar Publishing Host Installation Worksheet](#):

[Calendar Publishing Host Name](#)

[Web Server Information](#)

[Post Office Agent Information](#)

- 6 Click **Next** to display the Installation Summary.
- 7 (Conditional) If prompts appear because your web server is running, decide whether you want the Installation Wizard to stop your web server.
- 8 When the installation is finished, review the instructions for configuring the Calendar Publishing Host.
- 9 Click **Next** to continue.
- 10 When the installation is complete, click **Finish** to exit the Calendar Publishing Host Installation Wizard.

You can choose to have the Installation Wizard restart the web server for you.

Along with the Calendar Publishing Host Application, the Calendar Publishing Host Installation Wizard also installs Tomcat 9 to `c:\novell\tomcat`, integrates it with your web server, and automatically starts it to support the Calendar Publishing Host Application.

- 11 Exit the GroupWise Installation Wizard.
- 12 Continue with [Configuring GroupWise to Support the Calendar Publishing Host](#).

Configuring GroupWise to Support the Calendar Publishing Host

After you install the Calendar Publishing Host Application, additional configuration is still required.

- ♦ [“Configuring the Calendar Publishing Host in the GroupWise Admin Console” on page 138](#)
- ♦ [“Enabling Calendar Publishing” on page 139](#)
- ♦ [“Configuring a POA for Calendar Publishing” on page 139](#)
- ♦ [“Setting Up Calendar Publishing Administration” on page 140](#)
- ♦ [“Using the Published Calendar Browse List” on page 141](#)

Configuring the Calendar Publishing Host in the GroupWise Admin Console

Use the information under **Calendar Publishing Host Configuration** and **Calendar Browse List** on your [Calendar Publishing Host Configuration Worksheet](#) as you configure the CalPub Host.

- 1 In the [GroupWise Admin console](#), click **System > Calendar Publishing**, and then click **New**.
- 2 Fill in the fields to configure the CalPub Host, using the following information from the [Calendar Publishing Host Configuration Worksheet](#)

Name:

URL:

Description:

Address:

Port:

IMPORTANT: The name that you specify in the GroupWise Admin console must be the identical name that you specified during installation, including spacing and capitalization, as described in [Choosing the Calendar Publishing Host Name](#).

If you decide that you want to use a different name after you have already installed the CalPub Host Application, you must reinstall the software, and then specify the identical name during the re-installation that you specify in the GroupWise Admin console.

- 3 Click **OK** to save the CalPub Host configuration information.
- 4 If you want to allow users to add their published calendars to the calendar browse list as the default for your GroupWise system, select **Enable Publishing of Calendars to the Browse List**.
or

If you want to set up a corporate calendar browse list or provide no calendar browse list, leave **Enable Publishing of Calendars to the Browse List** deselected.

- 5 Click **OK** when you are finished.
- 6 Continue with [Enabling Calendar Publishing](#).

Enabling Calendar Publishing

Use the information under **Calendar Publishing Options** on your [GroupWise Calendar Publishing Host Worksheets](#) as you enable calendar publishing.

- 1 In the [GroupWise Admin console](#), click **Post Offices**, and then click the name of the post office where you want to enable calendar publishing.
For convenience in testing your Calendar Publishing Host setup, you might want to start with your post office.
- 2 Click **Client Options > Calendar > Web Calendar**.
As you roll out calendar publishing, you can use Client Options to enable it at the domain, post office, and user level.
- 3 Select a Calendar Publishing Host from the drop-down list.
- 4 Set the Web Calendar options as you planned on your [Calendar Publishing Host Installation Worksheet](#).
- 5 Click **OK** to save the Web Calendar settings, and then click **Close**.
- 6 Restart Tomcat:

SLES: `rcgrpwise-tomcat restart`

- Windows
1. At the Windows server, click **Start > Administrative Tools > Services**.
 2. Right-click **Tomcat 9**, and then click **Restart**.

- 7 Continue with [Configuring a POA for Calendar Publishing](#).

Configuring a POA for Calendar Publishing

After calendar publishing is enabled, the POA can look up calendar information and return it to the CalPub Host in the form of ICS (Internet Calendaring and Scheduling) or IFB (Internet Free Busy) files. Internet users can import these files into GroupWise, Outlook, and Macintosh iCal calendaring applications.

- 1 In the [GroupWise Admin console](#), click **Post Office Agents**, and then click the name of the POA that you want to configure for calendar publishing.
- 2 Click **Agent Settings**, and then scroll down to the **Calendar Publishing** section.
- 3 Select **Enabled**.
- 4 (Optional) Decrease the number in the **Max Calendar Publishing Threads** field as needed.
The default maximum number of calendar publishing threads is 4. By default, the POA creates 2 calendar publishing threads and adds more as needed. However, you cannot set the maximum higher than 4. The default setting is highly recommended.

- 5 Click **OK** to save the calendar publishing configuration settings.
- 6 As you roll out calendar publishing to your GroupWise users, enable calendar publishing on the POA for each post office where users will publish calendars and free/busy information.
To determine which POAs have been enabled for calendar publishing, see “[Viewing Calendar Publishing Status in the POA Console](#)” in the *GroupWise 18 Administration Guide*.
- 7 Continue with [Setting Up Calendar Publishing Administration](#).

Setting Up Calendar Publishing Administration

After calendar publishing has been enabled and the POA is communicating with the CalPub Host, you use the CalPub Admin console to monitor the CalPub Host and to make configuration changes as needed. Any GroupWise administrator user can access the CalPub Host Admin console. Use the information under **Authentication Information** on your [Calendar Publishing Host Configuration Worksheet](#) as you set up Calendar Publishing Host administration.

- 1 Edit the `calhost.cfg` file in the following folder:

```
Linux:      /var/opt/novell/groupwise/calhost
Windows:    c:\Novell\GroupWise\calhost
```

- 2 Search to find the following line:

```
#Admin.WebConsole.enable=false
```

- 3 Remove the pound sign (#) to activate the setting.
- 4 Change `false` to `true`.
- 5 Save the file, and then exit the text editor.
- 6 Restart Tomcat:

```
SLES:      rcgrpwise-tomcat restart
```

- Windows
1. At the Windows server, click **Start > Administrative Tools > Services**.
 2. Right-click **Tomcat 9**, and then click **Restart**.

- 7 Display the CalPub Host Admin console:

```
http://server_network_address/gwcal/admin
```

- 8 Log in to the CalPub Host Admin console using any GroupWise administrator user name and password.

For more information about the CalPub Host Admin console, see “[Using the CalPub Admin Console](#)” in the *GroupWise 18 Administration Guide*.

- 9 (Conditional) If additional GroupWise administrators need to access the CalPub Admin console, notify them of the URL to access.
- 10 Continue with [Using the Published Calendar Browse List](#).

Using the Published Calendar Browse List

If you selected **Enable Publishing of Calendars to the Browse List** as your GroupWise system default, continue with [Testing GroupWise Calendar Publishing](#).

If you are planning to implement a corporate calendar browse list in the future, you can enable publishing of calendars to the browse list for yourself for testing purposes.

- 1 Browse to and right-click your User object, and then click **Properties**.
- 2 Click **GroupWise > Calendar Publishing**.
- 3 Select **Override**, and then select **Enable Publishing of Calendars to the Browse List**.
This gives you the right to add your calendars to the calendar browse list so that you can test the setup of the Calendar Publishing Host.
- 4 Continue with [Testing GroupWise Calendar Publishing](#).

Testing GroupWise Calendar Publishing

Reference this sections for information that will help you test GroupWise Calendar Publishing.

- ♦ [“Publishing a Personal Calendar” on page 141](#)
- ♦ [“Displaying the Browse List of Calendars” on page 142](#)
- ♦ [“Publishing Free/Busy Information” on page 142](#)

Publishing a Personal Calendar

- 1 In the GroupWise client, create and populate a personal calendar, as described in [“Creating a Personal Calendar”](#) in the *GroupWise 18 Client User Guide*.
- 2 Right-click the personal calendar, and then click **Publish**.
- 3 Select **Publish This Calendar**.
For more information, see [“Publishing Personal Calendars on the Internet”](#) in the *GroupWise 18 Client User Guide*.

This feature is also available in GroupWise WebAccess, as described in [“Publishing Personal Calendars on the Internet”](#) in the *GroupWise 18 WebAccess User Guide*.

For more information, see the [GroupWise 18 Calendar Publishing Host User Quick Start](#).

- 4 Click **Send Publish Location**, and then address and send the resulting message, which provides the URL from which Internet colleagues can obtain your calendar information.

The URL has the following format:

```
http://calpubhost_server/gwcal/freebusy/user_name@internet_domain
```

- 5 Click **OK** to publish the selected personal calendar.
- 6 Check your mailbox for the notification sent by the Calendar Publishing Host.
- 7 Continue with [Displaying the Browse List of Calendars](#).

Displaying the Browse List of Calendars

- 1 Display the following URL:
`http://web_server_address/gwcal/calendar`
Your newly published personal calendar should appear on the list.
- 2 Click your calendar to view it in its published format.

This assures you that your calendar is available for access by users across the Internet.

Publishing Free/Busy Information

- 1 In the GroupWise client, click **Tools > Options**.
- 2 Click **Calendar > Free/Busy**.
- 3 Click **Send Free/Busy Publish Location**, and then address and send the resulting message, which provides the URL from which Internet colleagues can obtain your free/busy information.
- 4 Click **OK**, and then click **Close**.
- 5 Check your mailbox for the notification sent by the Calendar Publishing Host.
- 6 Continue with [What's Next](#).

What's Next

You can further configure and maintain the Calendar Publishing Host in the following ways:

Task	Section in the <i>GroupWise 18 Administration Guide</i>
Using the CalPub Host Admin console to change the configuration of the CalPub Host	See "Configuring the Calendar Publishing Host."
Changing the appearance of the calendar browse list to represent your company	See "Customizing the Calendar Publishing Host Logo."
Restricting the posted list of calendars to those of corporate importance	See "Creating a Corporate Calendar Browse List."
Monitoring the CalPub Host at the POA console and through CalPub Host log files	See "Monitoring Calendar Publishing."

GroupWise Calendar Publishing Host Worksheets

Reference the worksheets in this section to install and configure GroupWise Calendar Publishing.

- ♦ ["Calendar Publishing Host Installation Worksheet"](#) on page 143
- ♦ ["Calendar Publishing Host Configuration Worksheet"](#) on page 144

Calendar Publishing Host Installation Worksheet

Installation Wizard Field	Value for Your GroupWise System	Explanation
Web Server Platform <ul style="list-style-type: none"> ♦ Linux ♦ Windows 		Selecting the Calendar Publishing Host Application Platform
Calendar Publishing Host Name		Determining the URL of the Calendar Publishing Host
Post Office Agent Information <ul style="list-style-type: none"> ♦ POA network address <ul style="list-style-type: none"> ♦ IP address ♦ DNS hostname ♦ Calendar publishing port (default 7171) 		Connecting the Calendar Publishing Host to a POA
Web Server Information OES <ul style="list-style-type: none"> ♦ Apache path ♦ Tomcat path 		Gathering Web Server Information
Web Server Information SLES <ul style="list-style-type: none"> ♦ Apache path <code>/etc/apache2/conf.d</code> ♦ Tomcat path <code>/usr/share/tomcat/webapps</code> 		Gathering Web Server Information
Web Server Information Windows <ul style="list-style-type: none"> ♦ Path to the web server's root directory 		Gathering Web Server Information

Calendar Publishing Host Configuration Worksheet

Configuration Field	Value for Your GroupWise System	Explanation
Calendar Publishing Host Configuration		Choosing the Calendar Publishing Host Name
<ul style="list-style-type: none"> ◆ Name ◆ URL ◆ Description ◆ IP address ◆ TCP port 		Determining the URL of the Calendar Publishing Host Gathering Web Server Information
Calendar Browse List		Designing Your Calendar Browse List
<ul style="list-style-type: none"> ◆ Yes <ul style="list-style-type: none"> ◆ Corporate (restricted) ◆ Open ◆ No 		
Calendar Publishing Options		Selecting Calendar Publishing Settings
<ul style="list-style-type: none"> ◆ Enable calendar publishing ◆ Enable rules to move items to a published calendar ◆ Enable subscribe to calendar ◆ Enable publish free/busy searches 		
Calendar Publishing Post Office		Connecting the Calendar Publishing Host to a POA
<ul style="list-style-type: none"> ◆ Name ◆ POA network address <ul style="list-style-type: none"> ◆ IP address ◆ DNS hostname ◆ Calendar publishing port (default 7171) 		
Authentication Information		Selecting a Calendar Publishing Host Administrator
<ul style="list-style-type: none"> ◆ GroupWise user name 		

19 Setting Up GroupWise Monitor

GroupWise Monitor is a monitoring and management tool that allows you to monitor GroupWise agents from any location where you are connected to the Internet and have access to a web browser. Some agent administration can also be performed from your web browser if the agent console is password protected.

- ♦ [“GroupWise Monitor Overview” on page 145](#)
- ♦ [“GroupWise Monitor System Requirements” on page 148](#)
- ♦ [“Planning GroupWise Monitor” on page 150](#)
- ♦ [“Installing the GroupWise Monitor Software” on page 153](#)
- ♦ [“Testing GroupWise Monitor” on page 158](#)
- ♦ [“GroupWise Monitor Installation Worksheets” on page 159](#)

IMPORTANT: If you are installing GroupWise Monitor in a clustered server environment, see the [“Setting up a GroupWise Cluster”](#) in the *GroupWise 18 Interoperability Guide* before you install Monitor.

GroupWise Monitor Overview

Overview information for GroupWise Monitor is included in the sections below.

- ♦ [“GroupWise Monitor Functionality” on page 145](#)
- ♦ [“GroupWise Monitor Components” on page 146](#)
- ♦ [“One Monitor Server versus Two” on page 146](#)
- ♦ [“Monitor Security Requirements” on page 147](#)
- ♦ [“Monitor and the GroupWise High Availability Service on Linux” on page 148](#)

GroupWise Monitor Functionality

GroupWise Monitor is a monitoring and management tool that allows you to monitor GroupWise agents from any location where you are connected to the Internet and have access to a web browser. Some agent administration can also be performed from your web browser. Monitor provides more detail than is provided on the System page in the GroupWise Admin console.

You can install Monitor on either Linux or Windows. Either version can monitor agents on both Linux and Windows. Depending on the installation platform, two or three different monitoring environments are available:

- ♦ **Monitor Web Console:** The Monitor Web console, provided by the Monitor Application, takes advantage of your web server’s capabilities to make agent status information available to you when you are outside your firewall.

- ♦ **Monitor Agent Console:** The Monitor Agent console, provided by the Monitor Agent itself, can be used only behind your firewall, but it provides capabilities that are not available in the main Monitor Web console. This section focuses on using the full-featured Monitor Agent console.

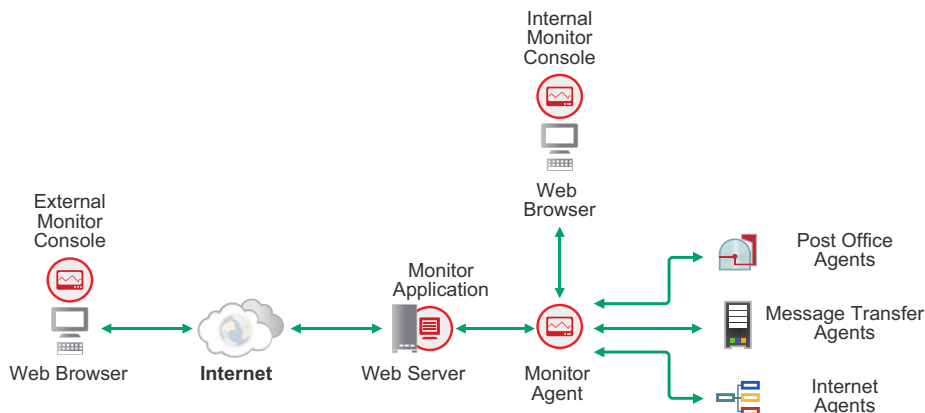
NOTE: The Monitor Web console and the Monitor Agent console are available on both Linux and Windows because they are browser based.

- ♦ **Windows Monitor Agent Server Console:** The Windows Monitor Agent server console is available only on the Windows server where the Windows Monitor Agent runs and only if you run the Monitor Agent as an application, rather than as a Windows service. All agent configuration tasks can be performed at the Windows Monitor Agent server console, but some reports are not available.

Specific differences in functionality between the three Monitor consoles are summarized in [“Comparing the Monitor Consoles”](#) in the *GroupWise 18 Administration Guide*.

GroupWise Monitor Components

GroupWise Monitor consists of two components: the Monitor Agent and the Monitor Application.



- ♦ **Monitor Agent:** The Monitor Agent continuously polls the POA, MTA, and GWIA; gathers status information from them; and displays the status information in the Monitor Agent console. The Monitor Agent also services requests for agent status information from the Monitor Application, which displays the Monitor Web console.
- ♦ **Monitor Application:** The Monitor Application extends the capability of your web server so that agent status information can be displayed in your web browser in the Monitor Web console.

One Monitor Server versus Two

The Monitor Agent and the Monitor Application can run together on a Linux server or a Windows server. The server where they run together must be a web server because the Monitor Application is installed into the web server.

The Monitor Agent and the Monitor Application can also run on different servers. The security issues discussed in [Monitor Security Requirements](#) might determine whether you run the Monitor Agent on the same server with the web server and the Monitor Application.

Monitor Security Requirements

GroupWise Monitor can be configured to support the level of security you have established for your Internet/intranet communication.

If you are not concerned about security issues (for example, you plan to use Monitor only on a secured intranet), you can install the Monitor components to any servers that provide access for your GroupWise administrators and that meet the requirements listed in [GroupWise Monitor System Requirements](#).

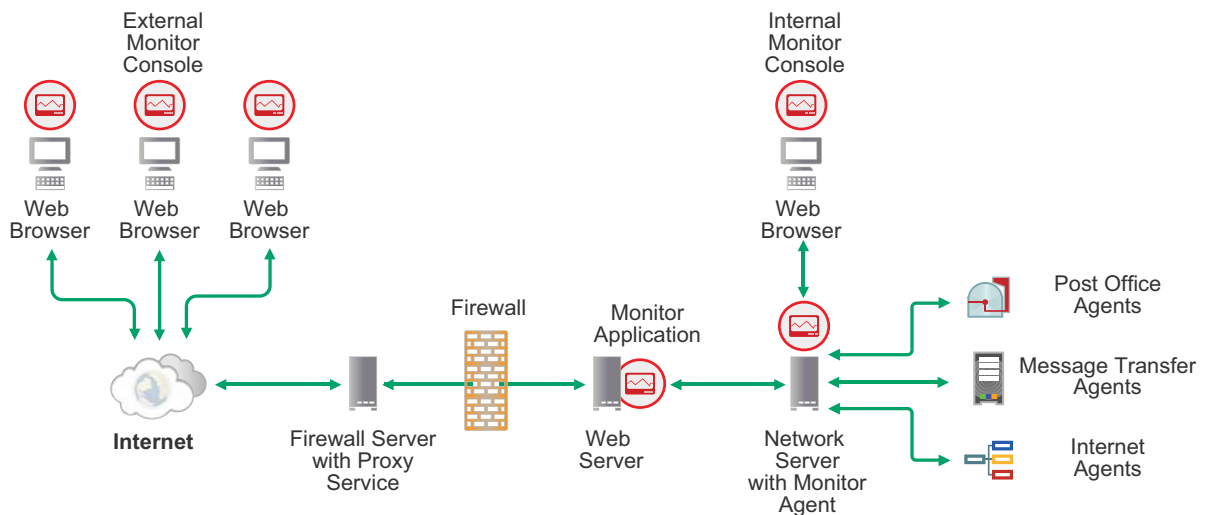
If you plan to use Monitor to provide GroupWise administrators with access to your GroupWise system from anywhere on the Internet (rather than simply within a secured intranet), and you already have a firewall in place to provide security, you have the following options for configuring Monitor:

- ♦ Install both Monitor components inside your firewall and use a proxy service. See [Configuring Monitor with a Proxy Service](#). This is the recommended configuration.
- ♦ Install the Monitor Application to a web server outside your firewall and the Monitor Agent on a server inside your firewall. See [Configuring Monitor without a Proxy Service](#).

Configuring Monitor with a Proxy Service

If your firewall includes a proxy service, you can install the Monitor Application to a web server inside your firewall, and the Monitor Agent to another server inside the firewall.

In this configuration, only the firewall server with the proxy service is located outside the firewall, as shown in the following illustration.

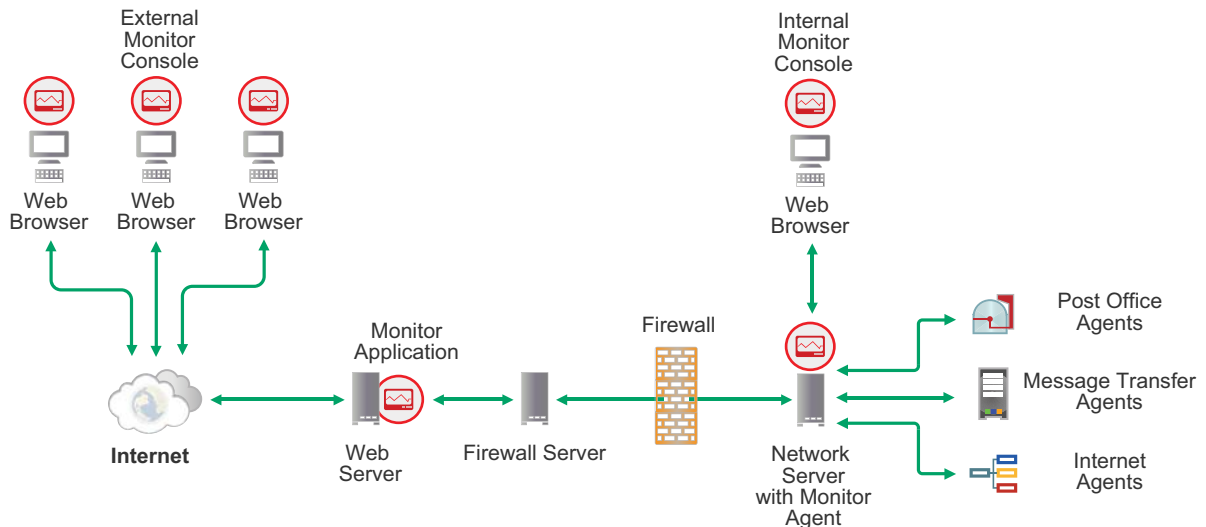


If desired, the Monitor Agent can also be installed to the web server rather than to a separate server, as described in [One Monitor Server versus Two](#).

Configuring Monitor without a Proxy Service

If your firewall does not provide a proxy service, you need to install the Monitor Application to a web server that is outside the firewall. However, the Monitor Agent requires direct access to a GroupWise domain folder, so it needs to be installed to a server that is located within the firewall. It should be installed to the same server where a domain folder is located.

In this configuration, both the web server and the firewall server are located outside the firewall, as shown in the following illustration.



The firewall must allow inbound IP packets to be sent from the web server to the IP address and port number of the Monitor Agent (for example, 172.16.5.18:8200).

In addition, the firewall must allow outbound IP packets to be sent from the Monitor Agent to the web server. This requires all high ports (above 1023) to be open to outbound IP packets.

Monitor and the GroupWise High Availability Service on Linux

The Monitor Agent can be used with the GroupWise High Availability service (`gwha`), which runs on Linux, to automatically restart GroupWise agents when they stop unexpectedly. For setup instructions, see [Automatically Restarting the Linux GroupWise Agents with the GroupWise High Availability Service](#).

There is no GroupWise High Availability service on Windows. Windows includes a mechanism for restarting services automatically when they stop unexpectedly. For more information, see [“Setting up a GroupWise Cluster”](#) in the *GroupWise 18 Interoperability Guide*.

GroupWise Monitor System Requirements

Requirements information for GroupWise Monitor is included in the sections below.

- ♦ [“Server Requirements” on page 149](#)
- ♦ [“Web Browser Requirements” on page 149](#)

Server Requirements

- ❑ Your server must meet the requirements found in [GroupWise Server Requirements](#).

IMPORTANT: If you are installing on SLES 15 SP1, you need to add the “Python 2 Module 15 SP1 x86 64” module as well as the other modules before installing Monitor.

- ❑ If installing on OES or SLES:

- ♦ **Apache 2.2 with ModProxy Module:** Apache with ModProxy is installed by the GroupWise install if a Linux repository is available during the install.

IMPORTANT: Apache must be configured with TLS for WebAccess or WebAccess will not work.

- ♦ **Tomcat 9:** Tomcat is installed by the GroupWise install and does not need to be installed on the server.
- ♦ **OpenJDK 11:** OpenJDK is installed by the GroupWise install and does not need to be preinstalled on the server if a Linux repository is available.
- ♦ **OES11 / OES 2015 / OES 2018 / SLES 11:** IBM Java Runtime Environment (JRE) 8 or later
SLES 12 / SLES 15: OpenJDK 11

A Linux repository should be available when you run the GroupWise Installation Wizard. Apache, the JRE or JDK, and the ModProxy Module are automatically installed from the Linux repository if they are not already present on the Linux server.

If no Linux repository is available during the GroupWise installation, you are prompted to manually install these required components from the Linux media, and then restart the GroupWise installation.

- ❑ If installing on a Windows Server:

- ♦ **Oracle Java Runtime Environment (JRE) 8:** Oracle JRE 8 is automatically installed with the GroupWise software if it is not already present on the server.
- ♦ **Tomcat 9:** Tomcat is installed with the GroupWise install and does not need to be installed on the server.

- ❑ Adequate server disk space:

- ♦ Approximately 525 MB (shared with the WebAccess Application and the Monitor Application when they are installed on the same web server; varies by platform)
- ♦ 50 KB per published calendar
- ♦ 50 KB per user for free/busy searching

Web Browser Requirements

Any of the following web browsers for the Monitor console:

- ❑ Linux: Mozilla Firefox; Google Chrome
- ❑ Windows: Mozilla Firefox; Microsoft Edge with Chromium Edge; Google Chrome
- ❑ Macintosh: Mozilla Firefox; Google Chrome; Safari

Planning GroupWise Monitor

Use the [GroupWise Monitor Installation Worksheets](#) to record your decisions about how to install GroupWise Monitor.

The topics in this section present the required information in a convenient planning sequence. The Installation Worksheet organizes the information in the order in which you need it during installation.

IMPORTANT: If you are installing GroupWise Monitor in a clustered server environment, see the “[Setting up a GroupWise Cluster](#)” in the *GroupWise 18 Interoperability Guide* before you install Monitor.

- ♦ “[Deciding Where to Install the GroupWise Monitor Components](#)” on page 150
- ♦ “[Determining the Monitor Agent’s Configuration](#)” on page 151
- ♦ “[Determining the Monitor Application’s Configuration](#)” on page 153

Deciding Where to Install the GroupWise Monitor Components

After reviewing [GroupWise Monitor Overview](#) and the system requirements listed in [GroupWise Monitor System Requirements](#), plan where you want to install the Monitor components in your system.

- ♦ “[Monitor Agent Server](#)” on page 150
- ♦ “[Web Server](#)” on page 151

Monitor Agent Server

The Monitor Agent runs on Linux and Windows. On Linux, the Monitor Agent runs as a daemon. On Windows, the Monitor Agent runs as a Windows service or as an application. When the Monitor Agent runs as an application, it has a user interface on the Windows server. When it runs as a Windows service, it does not.

If you want to install the Monitor Agent and the Monitor Application to the same server, you can install them at the same time. If you want to install them to different servers, you must run the Monitor Installation program twice, once for each server. For example, you might want to install the Monitor Application on Linux for use with a Linux web server, but you might want to install the Monitor Agent on Windows so that you can use its server console, which is not available on Linux.

The Monitor Agent needs to communicate with an MTA. If possible, install the Monitor Agent on the same server where a domain and MTA are already located. If you want to install the Monitor Agent on its own server, consider creating a domain on that server specifically for helping the Monitor Agent communicate with the rest of your GroupWise system.

The installation folder for the Monitor Agent depends on the platform:

Linux: The Linux Monitor Agent is automatically installed to /opt/novell/groupwise/agents.
Windows: The default installation directory is c:\Program Files\Novell\GroupWise Monitor.

On Windows, you can specify a different directory during installation. On Linux, you cannot.

GROUPWISE MONITOR AGENT INSTALLATION WORKSHEET

Under **Agent Software Platform**, mark the platform (Linux or Windows) where you plan to install the Monitor Agent.

Under **Server Information**, specify the directory on the Linux or Windows server where you plan to install the Monitor Agent software.

Web Server

The Monitor Application can be installed to a web server on Linux or Windows.

GROUPWISE MONITOR APPLICATION INSTALLATION WORKSHEET

Under **Web Server Platform**, mark whether you plan to install the Monitor Application to a Linux or Windows web server.

The Monitor Application integrates with your web server to pass agent status information gathered by the Monitor Agent to your web browser for display in the Monitor web console. The location of the Monitor Application files that are installed depends on the web server that it is being integrated with. The default web server paths vary by platform:

Apache Web Server on OES:	<code>/etc/opt/novell/httpd/conf.d</code>
Tomcat on OES:	<code>/var/opt/novell/tomcat9/webapps</code>
Apache Web Server on SLES:	<code>/etc/apache2/conf.d</code>
Tomcat on SLES:	<code>/usr/share/tomcat9/webapps</code>
Tomcat on Windows:	<code>c:\novell\tomcat9\webapps</code>

GROUPWISE MONITOR APPLICATION INSTALLATION WORKSHEET

Under **Web Server Information**, select the type of web server you want to use with Monitor, and specify the directory path to the web server root directory.

Determining the Monitor Agent's Configuration

As you install the Monitor Agent, you are prompted to supply the configuration information:

- ♦ [“Monitor Agent Network Address” on page 152](#)
- ♦ [“Domain Folder” on page 152](#)
- ♦ [“Service vs. Application \(Windows Only\)” on page 152](#)

Monitor Agent Network Address

The Monitor Agent communicates with the Monitor Application and with monitored agents by way of TCP/IP.

GROUPWISE MONITOR AGENT INSTALLATION WORKSHEET

Under **Server Information**, record the IP address or DNS hostname of the Linux or Windows server where you plan to install the Monitor Agent software. Use the default port number of 8200 unless that number is already in use on that server.

If you are installing the Monitor Application on a different server from where you are installing the Monitor Agent, record the same information under **Monitor Agent Information** on the [GroupWise Monitor Agent Installation Worksheet](#).

For a complete list of default port numbers used by the GroupWise agents, see “[GroupWise Port Numbers](#)” in the *GroupWise 18 Administration Guide*.

Domain Folder

The Monitor Agent can gather information about the locations of GroupWise agents to monitor by reading from a domain database. Using the gathered information, the Monitor Agent can display a list of monitored agents when you start it for the first time.

GROUPWISE MONITOR AGENT INSTALLATION WORKSHEET

Under **Domain Location**, specify the path to a domain folder where an MTA is running.

If the domain is located on a different server from where you are installing the Monitor Agent, specify the IP address or DNS hostname of the domain server.

Service vs. Application (Windows Only)

On Windows, you can choose to install the Monitor Agent as a Windows service or an application.

When you install the Monitor Agent as an application, it displays a Monitor Agent console on the server where it runs. You can start the Windows Monitor Agent on the Windows **Start** menu, or you can create a desktop icon for it.

When you install the Monitor Agent as a service, it does not display a server console. You manage it by using the Windows Services administrative tool.

GROUPWISE MONITOR AGENT INSTALLATION WORKSHEET

Under **Windows Installation Option**, mark **Service** or **Application**.

Determining the Monitor Application's Configuration

Monitor Application configuration information is stored in a configuration file (`gwmonitor.cfg`), located in the following directories:

Linux: `/var/opt/novell/groupwise/monitor`
Windows: `c:\novell\groupwise\gwmonitor`

The default configuration information is sufficient for an initial Monitor Application installation. For more information about configuring the Monitor Application, see [“Configuring the Monitor Application”](#) in the *GroupWise 18 Administration Guide* after you have installed the Monitor Application.

Installing the GroupWise Monitor Software

As you install the Monitor software, use the [GroupWise Monitor Installation Worksheets](#) that you filled out in [Planning GroupWise Monitor](#) to provide the required information.

IMPORTANT: If you are installing GroupWise Monitor in a clustered server environment, see the [“Setting up a GroupWise Cluster”](#) in the *GroupWise 18 Interoperability Guide* before you install Monitor.

- ♦ [“Linux: Installing the GroupWise Monitor Software” on page 153](#)
- ♦ [“Windows: Installing the GroupWise Monitor Software” on page 156](#)

Linux: Installing the GroupWise Monitor Software

These sections contain information for installing GroupWise Monitor on a Linux Server.

- ♦ [“Preparing the Linux Server for GroupWise Monitor” on page 153](#)
- ♦ [“Installing and Configuring the Linux Monitor Agent” on page 154](#)
- ♦ [“Installing and Configuring the Linux Monitor Application” on page 155](#)
- ♦ [“Starting the Linux Monitor Agent” on page 156](#)

Preparing the Linux Server for GroupWise Monitor

To prepare the Linux Server for GroupWise Monitor installation:

- 1 Ensure that the server where you are installing the Monitor Agent meets the system requirements listed in [GroupWise Monitor Installation Worksheets](#).
- 2 Ensure that the web server where you are installing the Monitor Application meets the system requirements.
- 3 Ensure that the server has a static IP address.
- 4 Ensure that the firewall on the server has the ports open that are used by the Monitor Agent and/or the Monitor Application and the web server.

For assistance, see “[GroupWise Port Numbers](#)” in the *GroupWise 18 Administration Guide*.

- 5 Continue with [Installing and Configuring the Linux Monitor Agent](#).

Installing and Configuring the Linux Monitor Agent

To install and configure the Linux Monitor Agent:

- 1 In a terminal window, become `root` by entering `su -` and the `root` password.
- 2 Browse to the location of the extracted software, and run the following command to start the install:

```
./install.sh
```

- 3 Type the number for the language in which you want to run the GroupWise Installation Wizard, and press Enter to select **OK**.
- 4 (Optional) Type 1 for **Documentation**, and then press Enter to review the Readme, Quick Start, and Installation Guide to better prepare yourself for the installation.
- 5 Type 2 for **Installation** and press Enter.
- 6 Enter `a` to accept the License Agreement and to display the Software list.
- 7 Type 4 for **GroupWise Monitor Agent**, to display the Actions list.
- 8 Enter 1 for **Install** and to install the Monitor Agent.

The Monitor Agent package is installed on the server. If any supporting packages are not available on the server, the Installation Wizard automatically installs them from the operating system media.

During the installation, any other GroupWise agents on the server are stopped and then started again after the Monitor software has been installed.

- 9 Enter 2 for **Configure** to configure the Monitor Agent.
- 10 Follow the prompts to configure the Monitor Agent, using the following information from the [GroupWise Monitor Agent Installation Worksheet](#):

[Domain Directory Path](#)

- 11 Type 1 for **Yes**, and then press Enter, to configure the Monitor Agent to automatically start when the server restarts.

IMPORTANT: The Monitor Agent must be running in order for the GroupWise High Availability Service (gwha) to automatically restart the GroupWise agents if they stop unexpectedly. For more information, see [Automatically Restarting the Linux GroupWise Agents with the GroupWise High Availability Service](#).

- 12 Press any key to exit the Monitor Agent Configuration.
- 13 Type `b` for Back to return to the Software list.
- 14 In a terminal window, start the Monitor Agent:

```
rcgrpwise-ma start
```

NOTE: Unlike the other GroupWise agents, you do not need to be logged in as `root` in order to start the Monitor Agent.

- 15 Continue with [Installing and Configuring the Linux Monitor Application](#).

Installing and Configuring the Linux Monitor Application

To install and configure the Linux Monitor application:

- 1 If you are installing the Monitor Application on the same server where you just installed the Monitor Agent, continue with [Step 2](#).

or

If you are installing the Monitor Application on a different server from where you installed the Monitor Agent:

- 1a Access the web server where you want to install the Monitor Application.
- 1b In a terminal window, become `root` by entering `su -` and the `root` password.
- 1c Browse to the location of the extracted software, and run the following command to start the install:

```
./install.sh
```
- 1d Type the number for the language in which you want to run the GroupWise Installation Wizard, and press Enter to select **OK**.
- 1e Type 2 for **Installation** and press Enter.
- 1f Enter `a` to accept the License Agreement and to display the Software list.
- 2 Type 5 for **GroupWise Monitor Application**, to display the Actions list.
- 3 Enter 1 for **Install** and to install the Monitor Application.
The Monitor Application is installed on the server. If any supporting packages are not available on the server, the Installation Wizard automatically installs them from the operating system media.
- 4 When the installation is finished, press any key to return to the Installation Options list.
- 5 Enter 2 for **Configure** to configure the Monitor Application.
- 6 Follow the prompts to configure the Monitor Application, using the following information from the [GroupWise Monitor Application Installation Worksheet](#):
[Server Information](#)
[Web Server Information](#)
- 7 Press any key to exit Monitor Application Configuration.
- 8 Exit the GroupWise Installation Wizard.
- 9 (Conditional) If you use a proxy service, follow the instructions in “[Configuring Proxy Service Support for the Monitor Console](#)” in the *GroupWise 18 Administration Guide*.
- 10 Continue with [Starting the Linux Monitor Agent](#).

Starting the Linux Monitor Agent

- 1 Use the following commands to manage the Monitor Agent:

```
rcgrpwise-ma start
rcgrpwise-ma restart
rcgrpwise-ma stop
rcgrpwise-ma status
```

- 2 (Optional) If desired, you can run the Monitor Agent executable directly:

- 2a Change to the GroupWise agent bin folder.

```
cd /opt/novell/groupwise/agents/bin
```

- 2b Use one of the following commands to start the Monitor Agent:

```
./gwmon --home /domain_folder &
./gwmon --ipa domain_server_ip_address --ipp mta_port_number &
```

- 3 For instructions on using the Monitor consoles, continue with [Testing GroupWise Monitor](#).

Windows: Installing the GroupWise Monitor Software

These sections contain information for installing GroupWise Monitor on Windows.

- ♦ [“Preparing the Windows Server for GroupWise Monitor” on page 156](#)
- ♦ [“Installing the Windows GroupWise Monitor Software” on page 157](#)
- ♦ [“Starting the Windows Monitor Agent” on page 157](#)

Preparing the Windows Server for GroupWise Monitor

To prepare the Windows Server for GroupWise Monitor installation:

- 1 Ensure that the server where you are installing the Monitor Agent meets the system requirements listed in [“GroupWise Monitor Installation Worksheets” on page 159](#).
- 2 Ensure that the web server where you are installing the Monitor Application meets the system requirements.
- 3 Ensure that the server has a static IP address.
- 4 Ensure that no GroupWise agents are currently running on the Windows server where you plan to install the Monitor Agent.
- 5 Ensure that the firewall on the server has the ports open that are used by the Monitor Agent and/or the Monitor Application and the web server.

For assistance, see [“GroupWise Port Numbers”](#) in the *GroupWise 18 Administration Guide*.

- 6 Continue with [Installing the Windows GroupWise Monitor Software](#).

Installing the Windows GroupWise Monitor Software

To install GroupWise Monitor on a Windows Server:

- 1 Run `setup.exe` at the root of the extracted GroupWise software to start the GroupWise Installation Wizard.
- 2 Click **GroupWise Monitor**, accept the License Agreement, and then click **Next**.
- 3 Click **Next** to display the GroupWise Monitor Components page.

The Installation Wizard provides diagrams that help you understand how the various components interact with each other. Review the diagrams as you provide the requested information.
- 4 (Conditional) If you are installing the Monitor Agent, follow the prompts to provide the information from your [GroupWise Monitor Agent Installation Worksheet](#):

[Server Information](#)

[Domain Directory](#)

[Service vs. Application](#)

- 5 (Conditional) If you are installing the Monitor Application, follow the prompts to provide the information from your [GroupWise Monitor Application Installation Worksheet](#):
[Monitor Agent Information](#) (This page does not appear when you install the Monitor Agent and the Monitor Application together on the same server.)

[Web Server Information](#)

- 6 Review the Installation Summary, and then click **Install**.
- 7 (Conditional) If prompts appear because your web server is running, decide whether you want the Installation Wizard to stop your web server.
- 8 When the installation is complete, click **Finish** to exit the Monitor Installation program.

You can choose to have the Monitor Installation program start the Monitor Agent and restart the web server for you.
- 9 Click **Finish** to exit the GroupWise Installation program.

If you chose to start the Monitor Agent immediately, the Monitor Agent server console displays on the Windows server.

If the Monitor Agent does not start successfully, see [Manually Starting the Windows Agents As Applications for Troubleshooting](#).
- 10 (Conditional) If you use a proxy service, follow the instructions in “[Configuring Proxy Service Support for the Monitor Console](#)” in the *GroupWise 18 Administration Guide*.
- 11 Continue with [Testing GroupWise Monitor](#).

Starting the Windows Monitor Agent

To start the Windows Monitor Agent:

- 1 If you installed the Monitor Agent as a Windows service, use the Services administrative tool to start and stop it.
or

If you installed the Monitor Agent as an application, start it on the Windows Start menu, or create a desktop icon to start it.

- 2 Continue with [Testing GroupWise Monitor](#).

Testing GroupWise Monitor

Monitor has two different web-based consoles. The main Monitor web console uses the capabilities of your web server to provide access from outside your firewall. The web-based Monitor Agent console is provided by the Monitor Agent itself and provides additional functionality beyond that which is available from outside your firewall.

On Windows, the Monitor Agent also has a server console that displays only on the Windows server where the Monitor Agent runs.

- ♦ [“Using the Monitor Web Console” on page 158](#)
- ♦ [“Using the Monitor Agent Console” on page 158](#)
- ♦ [“Using the Windows Monitor Agent Server Console” on page 159](#)

Using the Monitor Web Console

To display agent status information in your web browser from outside your firewall, enter the Monitor Web console URL in your web browser:

```
http://network_address/gwmon/gwmonitor
```

Replace *network_address* with the IP address or DNS hostname of the server where your web server runs. The Monitor console appears.

You can use this same URL to view the same agent status information in various browsers and on mobile devices.

You can perform many of the same monitoring activities at the Monitor Web console as you can at the Windows Monitor Agent server console. Refer to the online help in the Monitor Web console for additional information about each Monitor Web console page.

For more information about using the Monitor consoles, see [“Monitor”](#) in the *GroupWise 18 Administration Guide*.

Using the Monitor Agent Console

To display agent status information in your web browser from inside your firewall, enter the Monitor Agent console URL in your web browser:

```
http://network_address:8200
```

For instructions on protecting the Monitor Agent console with a password, see [“Securing the Monitor Web Console”](#) in the *GroupWise 18 Administration Guide*.

Using the Windows Monitor Agent Server Console

To start the Monitor Agent on a Windows server and display the Windows Monitor Agent server console click **Search > GroupWise Monitor**. You might find it convenient to pin GroupWise Monitor to the Windows **Start** menu for future use.

The Windows Monitor Agent server console appears.

In the Monitor Agent server console, you can perform many activities, for example:

- Use items on the **Configuration** menu to configure the Windows Monitor Agent as needed.
- Use items on the **View** menu to choose how much and what kind of agent status information to display.
- Create agent groups in order to monitor related agents together.
- Use items on the **Reports** menu to check the status of links throughout your GroupWise system and to organize status information into a format that can be emailed or printed.
- Use items on the **Actions** menu to control agent polling.

For more information about using the Windows Monitor Agent server console, see “**Monitor**” in the *GroupWise 18 Administration Guide*.

GroupWise Monitor Installation Worksheets

Reference the worksheets in this section to install the GroupWise Monitor agent and application.

- “[GroupWise Monitor Agent Installation Worksheet](#)” on page 159
- “[GroupWise Monitor Application Installation Worksheet](#)” on page 160

GroupWise Monitor Agent Installation Worksheet

Installation Program Field	Value for Your GroupWise System	Explanation
Monitor Component		GroupWise Monitor Overview
• GroupWise Monitor Agent		
Agent Software Platform		Deciding Where to Install the GroupWise Monitor Components
• Linux		
• Windows		

Installation Program Field	Value for Your GroupWise System	Explanation
Server Information		Deciding Where to Install the GroupWise Monitor Components
<ul style="list-style-type: none"> ♦ Installation path <p>Linux:</p> <pre>/opt/novell/ groupwise/agents/bin</pre> <p>Windows:</p> <pre>c:\Program Files\Novell\GroupWis e Monitor</pre> <ul style="list-style-type: none"> ♦ Network address <ul style="list-style-type: none"> ♦ IP address ♦ DNS hostname ♦ TCP port (default 8200) 		Monitor Agent Network Address
Domain Location		Domain Folder
<ul style="list-style-type: none"> ♦ Server ♦ Path 		
Windows Installation Option		Service vs. Application (Windows Only)
<ul style="list-style-type: none"> ♦ Service ♦ Application 		

GroupWise Monitor Application Installation Worksheet

Installation Program Field	Value for Your GroupWise System	Explanation
Monitor Component		GroupWise Monitor Overview
<ul style="list-style-type: none"> ♦ GroupWise Monitor Application 		
Web Server Platform		GroupWise Monitor Overview
<ul style="list-style-type: none"> ♦ Linux ♦ Windows 		
Monitor Agent Information		Monitor Agent Network Address
<ul style="list-style-type: none"> ♦ IP address ♦ DNS hostname ♦ TCP port (default 8200) 		

Installation Program Field	Value for Your GroupWise System	Explanation
Web Server Information: OES 11		Deciding Where to Install the GroupWise Monitor Components
♦ Apache path	<code>/etc/opt/novell/ httpd/conf.d</code>	
♦ Tomcat path	<code>/var/opt/novell/ tomcat9/webapps</code>	
Web Server Information: SLES 11		Deciding Where to Install the GroupWise Monitor Components
♦ Apache path	<code>/etc/apache2/conf.d</code>	
♦ Tomcat path	<code>/usr/share/tomcat9/ webapps</code>	
Web Server Information: Windows		Deciding Where to Install the GroupWise Monitor Components
♦ Path to the web server's root directory		
♦ Website	<code>c:\inetpub\wwwroot</code>	

20 Setting Up GroupWise Calendar Server

The GroupWise Calendar Server enables users to use CalDAV and CardDAV to sync their GroupWise Calendar and GroupWise Frequent Contacts book to their Mac devices. CalDAV also lets user run free/busy searches against other users in the GroupWise system.

- ♦ [“GroupWise Calendar Server Overview” on page 163](#)
- ♦ [“GroupWise Calendar Server System Requirements” on page 163](#)
- ♦ [“Planning GroupWise Calendar Server” on page 164](#)
- ♦ [“Installing the Calendar Server Software” on page 166](#)
- ♦ [“Configuring Auto-Discovery of the GroupWise Calendar Server” on page 167](#)
- ♦ [“Testing the GroupWise Calendar Server” on page 167](#)
- ♦ [“GroupWise Calendar Server Worksheet” on page 169](#)

GroupWise Calendar Server Overview

GroupWise Calendar Server allows you to use CalDAV and CardDAV to sync your GroupWise Calendar and your GroupWise Contacts book to your Mac. For full GroupWise functionality on Mac you need to also have the following configured:

- ♦ **IMAP:** Provides incoming mail server for the Mac Mail app.
- ♦ **SMTP:** Provides outgoing mail server for the Mac Mail app.

GroupWise Calendar Server System Requirements

Reference the sections below for information about GroupWise Calendar server and configuration requirements.

- ♦ [“Server Requirements” on page 163](#)
- ♦ [“Configuration Requirements” on page 164](#)

Server Requirements

- ❑ SUSE Linux Enterprise Server (SLES) 11, 12, or 15 plus the latest Service Pack.

IMPORTANT: If you are installing on SLES 15 SP1, you need to add the “Python 2 Module 15 SP1 x86 64” module as well as the other modules before installing Calendar Server.

Configuration Requirements

The majority of the configuration is done in a web browser. The following files are required on the machine where you are running the configuration:

- ☐ Valid certificate for the Calendar Server.
- ☐ Novell Push Notification Service certificate to push notifications to Mac devices. The NPNS certificate can be created at novell.com/npns.

Planning GroupWise Calendar Server

Use the [GroupWise Calendar Server Worksheet](#) to record the information required to install the Calendar Server application.

- ♦ [“Gathering the Primary Domain Information” on page 164](#)
- ♦ [“Gathering the Server Information” on page 164](#)
- ♦ [“Specifying the Application Admin” on page 165](#)
- ♦ [“Gathering SOAP Information” on page 165](#)
- ♦ [“Gathering the Novell Push Notification Certificate” on page 165](#)

Gathering the Primary Domain Information

The Calendar Server needs the server information for the GroupWise Primary Domain server to be able to connect to the GroupWise system. The Primary Domain server host name or IP address, the admin service port, and the admin service username and password are required.

GroupWise Calendar Server Worksheet

Under *GroupWise Domain Information*, enter the host name or IP address and admin service port, username, and password.

Gathering the Server Information

The Calendar Server requires an TLS port for secure communication to your Mac devices. Specify the TLS port you want to use if you don't want to use the default port 443.

GroupWise Calendar Server Worksheet

Under *Server Information*, enter an TLS port for the server.

If you are installing the Calendar Server in a cluster, you can bind to a specific IP address from the server or use all available IP addresses. If you are not installing in a cluster, leave **Listen on all interfaces** selected.

GroupWise Calendar Server Worksheet

Under *Server Information*, specify the IP address to listen on or specify **Listen on all interfaces**.

An TLS/TLS certificate is required for the Calendar Server service. Using a public or private CA, create a certificate and key (if applicable to the format you are using) for the GroupWise Calendar Server. The following formats are supported for the certificate:

- ♦ PEM
- ♦ DER
- ♦ PKCS #12
- ♦ Java keystore
- ♦ PEM encoded with multiple objects

GroupWise Calendar Server Worksheet

Under *Server Information*, specify the TLS/TLS certificate and key to use for the server.

Specifying the Application Admin

A read-only admin user is created at initial configuration of the Calendar Server that the service uses to connect to the GroupWise Admin Service. The user is called an application admin and does not consume a mailbox in your system. You do not need to create a user before configuring the Calendar Server, but should note the username and password you plan on using.

GroupWise Calendar Server Worksheet

Under *Admin Connection*, specify the application admin username and password.

Gathering SOAP Information

The Calendar Server receives SOAP connections from the POA servers. The Calendar Server needs a port to use to receive these SOAP connections.

GroupWise Calendar Server Worksheet

Under *SOAP Event Listener*, specify a port and an IP address if running in a cluster. Otherwise, specify **Listen on all interfaces**.

Gathering the Novell Push Notification Certificate

The Novell Push Notification Server is used to notify your Mac devices if they have updates to CalDAV or CardDAV. It uses push technology through an open IP connection to push notifications from the server to Mac devices even when the device is asleep or the app is no longer running. A certificate is required to be able to use this service. The NPNS certificate can be downloaded from novell.com/npns.

GroupWise Calendar Server Worksheet

Under *NPNS*, specify the name of the NPNS certificate and key.

Installing the Calendar Server Software

Before you can start installing Calendar Server, you need to have the GroupWise installation software available and extracted in a temporary directory on your server.

- 1 In a terminal windows, become root by entering **su -** and the root password
- 2 Start the GroupWise Installation Wizard at the root of the extracted GroupWise installation software:

```
./install.sh
```
- 3 Type the number for the language in which you want to run the GroupWise Installation Wizard.
- 4 (Optional) Enter 1 for **Documentation** to view the Readme, Quick Start, and Installation Guide.
- 5 Enter 2 for **Installation**.
- 6 Enter a to accept the License Agreement.
- 7 Enter 6 for **GroupWise Calendar Server**.
The packages for the GroupWise Calendar Server component are installed on the server.
- 8 When the installation is finished, press any key to return to the Installation Options list.
- 9 Type 2 for **Configure**.
- 10 When prompted, enter the host name or IP address of the GroupWise Primary Domain server.
- 11 Enter the port used by the GroupWise admin service on the Primary Domain server.
You are prompted to accept the admin service certificate if it is issued from an untrusted root CA. Enter **Yes** to accept the certificate. If the certificate is incorrect, enter **No** and any additional certificates appear with the option given to trust the additional certificate. If no more certificates are available, the utility will exit and will be unable to connect to the GroupWise admin service.
- 12 Browse to the URL displayed in the terminal on the machine where you will finish the configuration and login to the configuration page using the GroupWise admin service credentials.
- 13 Using the information from the [GroupWise Calendar Server Worksheet](#), fill in the fields to configure the Calendar Server.
- 14 In the **Connectivity Test** section, click **Run Scan** to verify the SOAP configuration of your POA servers. Use the information in [Troubleshooting Calendar Server Configuration Errors](#) to resolve any issues found during the scan.
If you want to only see POAs with problems, select **Only show POA's with problems**.
- 15 Click **Save**.

Configuring Auto-Discovery of the GroupWise Calendar Server

Auto-discovery allows your users to setup the accounts using their Groupwise email address and password. If you do not setup auto-discovery, the GroupWise Calendar server DNS name must be specified when creating the account. Auto-discovery does not work for CardDAV. To configure auto-discovery, a DNS record must be added to your DNS server for CalDAV.

Use the format below for the DNS record:

```
_caldavs._tcp 86400 IN SRV 0 1 TLS_port DNS_name
```

Example:

```
_caldavs._tcp 86400 IN SRV 0 1 443 calsvr.acme.com
```

If you have multiple [iDomains](#), one DNS record for each domain is required.

Testing the GroupWise Calendar Server

Reference the sections below for information about testing the GroupWise Calendar server.

- ♦ [“Calendar Server Service Name” on page 167](#)
- ♦ [“Testing Calendar Server on a Workstation” on page 167](#)
- ♦ [“Troubleshooting Calendar Server Configuration Errors” on page 167](#)
- ♦ [“Resolving an Untrusted CA” on page 168](#)

Calendar Server Service Name

The GroupWise Calendar Server is listed under the following service name:

gwcalsvr

Testing Calendar Server on a Workstation

To test Calendar Server, follow the steps found in the [GroupWise Mac User Quick Start](#) to configure your workstation.

Troubleshooting Calendar Server Configuration Errors

Use the table below to help you resolve errors in the SOAP connectivity test.

Error	Description	Resolution
SUCCESS	TLS connection was established and SOAP is responding properly.	No action required.
TLS_DISABLED	SOAP is responding properly, but the connection was not over TLS.	Enable TLS for SOAP on the POA.

Error	Description	Resolution
SOAP_DISABLED	SOAP is not enabled for the post office. No connection was attempted.	Enable SOAP on the POA.
UNREACHABLE	Failed to connect to the POA due to a connection failure or socket timeout.	<p>Ensure the POA service is running on the server.</p> <p>Ensure that the POA network is accessible from the Calendar Server.</p>
UNTRUSTED_CA	The certificate chain did not contain a trusted root certificate.	See Resolving an Untrusted CA .
UNTRUSTED_CERT	The endpoint certificate presented during the TLS handshake is invalid. This can be for multiple reasons including expiration or invalid usage of the cert.	<p>Issue a new TLS certificate to the POA.</p> <p>Trust the endpoint certificate. If the certificate is trusted, then the trust does not expire when the certificate expires. This also does not prevent man-in-the-middle attacks.</p>
HOSTNAME_MISMATCH	A valid TLS certificate is presented by a server that does not match either the CN of the certificate or any of the subject alternative names.	<p>Issue a new certificate that matches the hostname or IP address of the server.</p> <p>Correct the address of the POA so it matches the certificate.</p> <p>Trust the endpoint certificate. If the certificate is trusted, then the trust does not expire when the certificate expires. This also does not prevent man-in-the-middle attacks.</p>
UNKNOWN	Most likely caused by network instability, but includes any error not shown above.	<p>Manually check connectivity by running a curl command. See the format below:</p> <pre>curl -X options https:// POA_server:SOAP_port/ soap</pre>

Resolving an Untrusted CA

The following are possible resolutions for fixing an UNTRUSTED_CA error during the connectivity test:

- ◆ Configure the POA with a certificate that is issued from a publicly trusted root certificate authority.

- ◆ Configure the POA with a certificate that is issued by the GroupWise CA.
- ◆ Manually override the trust:
 - ◆ If the TLS handshake contained the CA certificate from the server, you can trust the CA in the pop up that appears when you click **Trust**.
 - ◆ If the TLS handshake did not contain the CA certificate from the server, you can manually upload the CA certificate into the **Trust** dialog.
 - ◆ You can choose to trust the endpoint certificate. While this is a haTLSe free way of overriding certificate validation issues during the TLS process, it does not prevent man-in-the-middle attacks. Also, the trust does not expire even if the certificate has expired.

GroupWise Calendar Server Worksheet

Configuration Information	Value for Your GroupWise System	Explanation
GroupWise Domain Information		Gathering the Primary Domain Information
◆ Primary Domain Host name or IP address		
◆ Port (default 9710)		
◆ Admin service Username and password		
Server Settings		Gathering the Server Information
◆ Port (default 443)		
◆ Bind Address OR Listen on all interfaces		
◆ TLS Certificate		
◆ TLS Key		
Admin Connection		Specifying the Application Admin
◆ Application		
◆ Password		
Soap Event Listener		Gathering SOAP Information
◆ Port		
◆ Bind Address OR Listen on all interfaces		

Configuration Information	Value for Your GroupWise System	Explanation
NPNS		Gathering the Novell Push Notification Certificate
<ul style="list-style-type: none"> ◆ Certificate ◆ Key 		

21 Installing the GroupWise Client

The following sections assist you with assigning GroupWise accounts to users and with installing the GroupWise 18 client.

- ♦ [“GroupWise Client Overview” on page 171](#)
- ♦ [“GroupWise Client Workstation Requirements” on page 171](#)
- ♦ [“Installing the GroupWise Client” on page 172](#)
- ♦ [“Starting the Groupwise Client” on page 174](#)
- ♦ [“What’s Next” on page 174](#)

For information about client licensing requirements, see [“Auditing Mailbox License Usage in the Post Office”](#) in the *GroupWise 18 Administration Guide*.

GroupWise Client Overview

Each user with a GroupWise account has a mailbox in a post office. In a corporate workplace environment, GroupWise users with Windows workstations can run the GroupWise client to access their mailboxes and to send and receive mail.

When the users are not at their workstations, they can access their GroupWise mailboxes from a web browser by using GroupWise WebAccess or on a tablet device by using GroupWise WebAccess Mobile. See [Setting Up GroupWise WebAccess \(Legacy\)](#).

Users can also synchronize GroupWise data to their mobile devices. See [Using the GroupWise Mobility Service to Synchronize GroupWise Data to Mobile Devices](#).

GroupWise Client Workstation Requirements

These are the requirements for the GroupWise Client workstation:

- ♦ x86-32 processor or x86-64 processor
 - On a 64-bit processor, GroupWise still runs as a 32-bit application.
- ♦ Any of the following desktop operating systems for the GroupWise client:
 - ♦ Windows 7 on a 1 GHz or higher workstation with at least 1 GB of RAM
 - ♦ Windows 8 or Windows 8.1 on a 1 GHz or higher workstation with at least 1 GB of RAM
 - ♦ Windows 10 on a 1 GHz or higher workstation with at least 1 GB of RAM
 - ♦ Windows 11 on a 1 GHz or higher workstation with at least 1 GB of RAM
- ♦ Microsoft Internet Explorer 9 or later

- ♦ Any of the following word processors for use as the GroupWise editor:
 - ♦ LibreOffice 3.6 or later
 - ♦ Microsoft Word 2007 or later
- ♦ Approximately 200 MB of free disk space on each user's workstation to install the GroupWise client.

Installing the GroupWise Client

The GroupWise client software is available on the GroupWise download page. A simple installation of the GroupWise client helps you test your GroupWise system as you are setting it up.

- ♦ [“Installing the GroupWise Client” on page 172](#)
- ♦ [“Implementing System-Wide GroupWise Client Rollouts” on page 173](#)

Installing the GroupWise Client

To install the GroupWise Client:

- 1 Install the GroupWise client software on a Windows workstation that meets the system requirements listed in [GroupWise Client Workstation Requirements](#).
- 2 Run the GroupWise Installation Wizard (`gw18.x.x_client_win_multi.exe`).
- 3 Select the language in which you want to run the GroupWise Client Installation Wizard, and then click **OK**.

All available languages are automatically installed on the workstation, but you select the specific language that you want to use for the Installation Wizard.

The GroupWise Client Installation Wizard appears.

- 4 Click **Next** to display the Setup Type dialog box.
- 5 Select one of the following options:
 - ♦ **Typical:** Installs the most commonly used components in the standard installation directory of `c:\Program Files\Novell\Groupwise` without prompting for further information. Review the Custom settings to see which ones are enabled by default.
 - ♦ **Custom:** Allows you to customize the following GroupWise client functionality:
 - ♦ Languages (select as needed)
 - ♦ Internet Browser Mail Integration (enabled by default)
 - ♦ Program Folder (Micro Focus GroupWise by default)
 - ♦ Add GroupWise to the Desktop (selected by default)
 - ♦ Add GroupWise to Quick Launch (selected by default)
 - ♦ Add Icons to the Start Menu (selected by default)
 - ♦ Add Notify to the Startup folder (disabled by default)

If Notify is not added to the Startup folder, Notify does not automatically run when Windows starts. Users can control how Notify starts in the GroupWise client. For instructions, see [“Starting Notify”](#) in the *GroupWise 18 Client User Guide*.

See “[Using GroupWise Client Custom Installation Options](#)” in the *GroupWise 18 Administration Guide* for more information about installing the GroupWise client.

6 Click **Next**.

7 (Conditional) If you selected **Typical** or **Upgrade**:

7a Click **Install** to install the client files.

When the client Installation Wizard has completed, a shortcut to run GroupWise appears on your desktop and in the Quick Launch area.

7b Click **Finish** to exit the GroupWise Installation program.

7c Continue with [Starting the Groupwise Client](#).

8 (Conditional) If you selected **Custom**:

8a Ensure that each component you want to install is selected.

Languages: Select which languages to install.

Internet Browser Mail Integration: Sets GroupWise to be the default email program on the workstation, so that whenever the user clicks an email link on a web page or chooses the **Mail** command in the browser, GroupWise starts.

8b Click **Next**.

8c Select the Program folder where you want to add the GroupWise icons.

The default is **Micro Focus GroupWise**.

8d Select whether you want the GroupWise icon added to your Desktop and Quick Launch.

8e Select whether you want GroupWise icons added to the Start menu.

8f Select whether you want Notify added to the Startup folder.

If Notify is not added to the Startup folder, Notify does not automatically run when Windows starts. Users can control how Notify starts in the GroupWise client. For instructions, see “[Starting Notify](#)” in the *GroupWise 18 Client User Guide*.

8g Click **Next**.

8h Click **Install** to install the client software files.

When the Installation Wizard has completed, a shortcut to run GroupWise appears on your desktop.

8i Click **Finish** to exit the GroupWise Client Installation Wizard.

8j Continue with [Starting the Groupwise Client](#).

Implementing System-Wide GroupWise Client Rollouts

For a system-wide rollout of the GroupWise client software, see “[Distributing the GroupWise Client](#)” in the *GroupWise 18 Administration Guide*.

Starting the Groupwise Client

At startup, the GroupWise client needs to know the location (IP address/hostname and port number) for the user's post office.

The GroupWise client can get the information for the initial login in two ways:

- ♦ The user can provide the post office location when prompted.
- ♦ The GroupWise client can access a GroupWise name server to get the user's post office location.

A GroupWise name server is a DNS hostname entry that defines the IP address of a POA. During startup, the GroupWise client automatically looks for the GroupWise name server in DNS. The POA identified as the GroupWise name server then redirects the client login to the POA for the user's post office. For information about creating a GroupWise name server, see "[Post Office Agent](#)" in the *GroupWise 18 Administration Guide*.

After the first successful login, the GroupWise client stores the post office location as the default for future logins. The user is subsequently presented with a simpler Startup dialog box.

To start the GroupWise client for the first time:

- 1 Double-click the GroupWise icon on the Windows desktop.
- 2 Enter the password and post office address information, and then click **OK**.

For more information about logging in, see "[Getting Started](#)" in the *GroupWise 18 Client User Guide*.

For information about providing users' GroupWise passwords automatically, see "[Security Options: Password](#)" in the *GroupWise 18 Administration Guide*.

What's Next

For information about using the features in the GroupWise client, click **Help > User's Guide**. The Help menu also has links to the What's New section in the User Guide, the GroupWise Community, and the Idea Exchange. The User Guide is also available on the [GroupWise 18 Documentation website](#) in HTML and PDF formats.

22 Using Other Micro Focus Products with GroupWise

The sections below contain information about using other Micro Focus products with GroupWise.

- ♦ [“Using the GroupWise Mobility Service to Synchronize GroupWise Data to Mobile Devices” on page 175](#)
- ♦ [“Using GroupWise Messenger to Provide Secure Instant Messaging for GroupWise Users” on page 175](#)
- ♦ [“Using Micro Focus Vibe to Provide Team Workspaces for GroupWise Users” on page 176](#)
- ♦ [“Using GroupWise Teamworks to Provide Team Workspaces for GroupWise Users” on page 176](#)

Using the GroupWise Mobility Service to Synchronize GroupWise Data to Mobile Devices

The GroupWise Mobility Service provides data synchronization between GroupWise mailboxes and mobile devices for synchronizing email, appointments, contacts, tasks, notes, and phone messages. The GroupWise Mobility Service is fast, reliable and scalable, and supports the latest device operating systems. For more information, see the [GroupWise Mobility Service Installation Guide](#).

Using GroupWise Messenger to Provide Secure Instant Messaging for GroupWise Users

GroupWise Messenger is a corporate-based, secure instant messaging solution that supports instant messaging, presence, and archiving of conversations. The Messenger client integrates with the GroupWise client to provide access to instant messaging features from within the GroupWise client. For more information, see:

- ♦ [GroupWise Messenger Installation Guide](#)
- ♦ [GroupWise and Messenger Quick Start](#)
- ♦ [“Messenger” in the GroupWise 18 Interoperability Guide](#)

Using Micro Focus Vibe to Provide Team Workspaces for GroupWise Users

Micro Focus Vibe enhances GroupWise by providing easy document management and document sharing, team calendars and task lists, workflows, discussion threads, wikis, blogs, RSS feeds, and more. For more information, see:

- ♦ [Micro Focus Vibe Documentation website \(http://www.novell.com/documentation/vibe4/\)](http://www.novell.com/documentation/vibe4/)
- ♦ “Micro Focus Vibe” in the *GroupWise 18 Interoperability Guide*

Using GroupWise Teamworks to Provide Team Workspaces for GroupWise Users

GroupWise TeamWorks helps you easily collaborate via your web browser, mobile device, or the GroupWise client. With TeamWorks, you can discuss ideas, post files, share links, and invite others to join the conversation in virtual discussion rooms. For more information, see:

- ♦ [TeamWorks Documentation website \(https://www.novell.com/documentation/teamworks-18/\)](https://www.novell.com/documentation/teamworks-18/)
- ♦ “GroupWise TeamWorks” in the *GroupWise 18 Interoperability Guide*



GroupWise System Upgrade

Reference the sections below for information about upgrading GroupWise to a newer version.

- ♦ [Chapter 23, “What’s New in GroupWise 18,” on page 179](#)
- ♦ [Chapter 24, “Understanding the Upgrade Process,” on page 181](#)
- ♦ [Chapter 25, “Preparing Your Existing GroupWise System for the Upgrade,” on page 187](#)
- ♦ [Chapter 26, “Installing the GroupWise 18 Software,” on page 189](#)
- ♦ [Chapter 27, “Upgrading the Primary Domain Server,” on page 193](#)
- ♦ [Chapter 28, “Upgrading a Secondary Domain Server,” on page 197](#)
- ♦ [Chapter 29, “Upgrading a Post Office Server,” on page 201](#)
- ♦ [Chapter 30, “Upgrading GroupWise Agents and Applications,” on page 203](#)
- ♦ [Chapter 31, “Upgrading Users’ GroupWise Client Software,” on page 209](#)
- ♦ [Chapter 32, “Transitioning from ConsoleOne,” on page 211](#)

23 What's New in GroupWise 18

To see a list of what's new in GroupWise 18, please see the [Micro Focus GroupWise 18 Readme](#).

24 Understanding the Upgrade Process

You can upgrade a GroupWise 8, GroupWise 2012, or GroupWise 2014 system to GroupWise 18.

IMPORTANT: If you need to upgrade from an older GroupWise version, you must upgrade at least to GroupWise 8, and preferably to GroupWise 2012, in order to ensure that your GroupWise data is compatible with the upgrade process that is provided in GroupWise 18.

If your GroupWise system is still on NetWare, see [“Migrating Away from NetWare”](#) in the *GroupWise 2012 Installation Guide*.

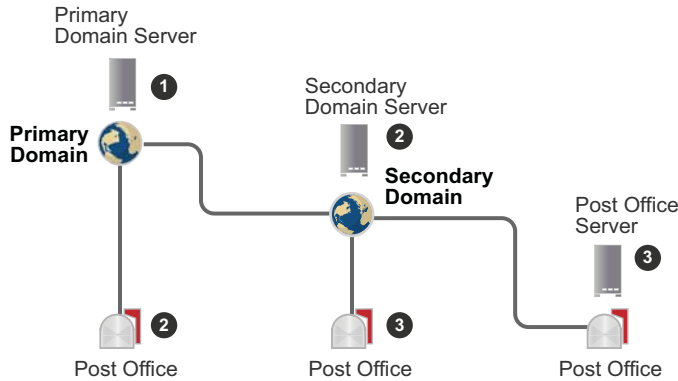
IMPORTANT: After you understand the upgrade process in general, you are ready to upgrade specific components of your existing GroupWise system. Do not start upgrading your GroupWise system until you have a solid understanding of the entire process.

For a large GroupWise system, you might need to maintain a mixed-version environment as you roll out GroupWise 18. For a table showing which GroupWise 8 and GroupWise 2012 components can be used with GroupWise 18, see [Appendix A, “GroupWise Version Compatibility,” on page 215](#).

- ♦ [“Domain and Post Office Upgrades” on page 182](#)
- ♦ [“Agent Upgrades” on page 183](#)
- ♦ [“Monitor Upgrades” on page 183](#)
- ♦ [“WebAccess Upgrades” on page 184](#)
- ♦ [“Calendar Publishing Host Upgrades” on page 184](#)
- ♦ [“GroupWise Client Upgrades” on page 184](#)
- ♦ [“Obsolete eDirectory Schema Extensions” on page 184](#)
- ♦ [“Obsolete Software Distribution Directories” on page 185](#)
- ♦ [“Obsolete GroupWise Gateways” on page 185](#)
- ♦ [“NetWare Compatibility” on page 185](#)

Domain and Post Office Upgrades

Functionality enhancements in GroupWise 18 require the GroupWise domain and post office databases to be upgraded. The following diagram illustrates the required upgrade sequence for installing the GroupWise 18 software.



1. Upgrade the primary domain server first, so that correct replication of GroupWise 18 information can take place as you upgrade secondary domains and post offices.

If there are secondary domains or post offices on the primary domain server, you can upgrade them at the same time as the primary domain, but this is not required.

2. Upgrade secondary domain servers.

If there are multiple secondary domains or post offices on a secondary domain server, you can upgrade them at the same time, but this is not required.

3. Upgrade post office servers after upgrading the secondary domains that they belong to.

When you install the GroupWise 18 software on a server where an earlier version of GroupWise is installed, the Installation Wizard stops the existing agents, installs the GroupWise 18 software, and then starts the GroupWise 18 agents.

IMPORTANT: Upgrading the domain and post office servers does not upgrade the domain and post office databases. Database upgrades are performed in a separate step using the GroupWise Administration Utility (`gwadminutil`). For information, see “[gwadminutil-upgrade\(1\)](#)” in the *GroupWise Utilities Reference*.

When you upgrade multiple domains and post office on the same server at the same time, the Installation console orchestrates the process of upgrading the databases in the proper order.

Agent Upgrades

POA POAs are automatically upgraded along with the post offices that they belong to.

The upgrade process looks for POA startup files. If a POA startup file is found, the setting of the --home switch is verified. If the home folder is valid, the existing POA startup file is used with the upgraded POA. If the POA startup file cannot be found, or if the home folder is not valid, a new POA startup file is created in the post office folder. The GroupWise 18 location for POA startup files is the post office folder.

If you have been running multiple POAs on multiple servers, the upgrade process cannot upgrade POAs on remote servers. In GroupWise 18, the need for running multiple POAs for a post office does not occur. You can configure the POA that runs on the server where the post office is located to handle all the needs of the post office.

If your existing POAs have been using the internal Document Converter Agent (DCA) rather than the independent Document Viewer Agent (DVA), you must run at least one DVA in your GroupWise 18 system.

MTA MTAs are automatically upgraded along with the domains that they belong to.

The upgrade process looks for MTA startup files. If an MTA startup file is found, the setting of the --home switch is verified. If the home folder is valid, the existing MTA startup file is used with the upgraded MTA. If the MTA startup file cannot be found, or if the home folder is not valid, a new MTA startup file is created in the domain folder. The GroupWise 18 location for MTA startup files is the domain folder.

GWIA GWIAs are automatically upgraded along with the domains that they belong to.

IMPORTANT: If you are upgrading to GroupWise 18 from GroupWise 8, you need to understand the important changes to where GWIA configuration information is stored. See [“Using Internet Agent Startup Switches”](#) in the *GroupWise 8 Administration Guide* before you upgrade to GroupWise 18.

DVA Existing DVAs are automatically upgraded along with the POAs that they were installed with. However, their startup files (`gwdva.dva`) are not modified. On Linux, the `gwha.conf` file already has an entry for each DVA. On Windows, the DVA service is already set up.

If you were not running a DVA in your existing GroupWise system, you must install and configure at least one DVA in your GroupWise 18 system.

Monitor Upgrades

GroupWise Monitor is not dependent on any other GroupWise agents, so you can upgrade the Monitor Agent and the Monitor Application to GroupWise 18 at any time.

IMPORTANT: If you are upgrading from GroupWise 8 directly to GroupWise 18, you need to understand that Monitor no longer relies on eDirectory objects for its configuration information. All configuration information is located in the `gwmonitor.cfg` file instead. See [“Understanding Monitor Updates”](#) and [“Updating GroupWise Monitor”](#) in the *GroupWise 2012 Installation Guide* before you upgrade Monitor from GroupWise 8 directly to GroupWise 18.

On Linux, the GroupWise High Availability Service (`gwha`), that works in conjunction with the Monitor Agent to automatically restart the GroupWise agents, has been made more secure.

WebAccess Upgrades

If you are upgrading from GroupWise 2012 to GroupWise 18, there are no WebAccess upgrade issues. You can upgrade your WebAccess software whenever it is convenient as you upgrade your GroupWise system. However, in order to use the WebAccess Application console, you must change the way it is configured. For instructions, see “[Using the WebAccess Application Console](#)” in the *GroupWise 18 Administration Guide*.

IMPORTANT: If you are upgrading from GroupWise 8 directly to GroupWise 18, you need to understand that the WebAccess Agent is no longer part of GroupWise. See “[Understanding WebAccess Updates](#)” and “[Updating GroupWise WebAccess](#)” in the *GroupWise 2012 Installation Guide* before you upgrade WebAccess from GroupWise 8 directly to GroupWise 18.

Calendar Publishing Host Upgrades

There are no Calendar Publishing Host upgrade issues. You can upgrade the Calendar Publishing Host to GroupWise 18 at any time after the POA that it communicates with has been upgraded. However, in order to use the CalPub Host Admin console, you must change the way it is configured. For instructions, see [Setting Up Calendar Publishing Administration](#).

GroupWise Client Upgrades

After a post office is upgraded to version 18, users can run the GroupWise 18 client on workstations that meet the requirements listed in [GroupWise User Requirements](#). If necessary, they can also continue to run their older GroupWise clients. However, older clients do not have GroupWise 18 functionality just because they are accessing mailboxes in a GroupWise 18 post office.

IMPORTANT: A user who needs to proxy into another user’s mailbox should not upgrade to the GroupWise 18 client until the mailbox owner’s post office has been upgraded to version 18. The GroupWise 18 client cannot proxy into a mailbox that has not been upgraded to GroupWise 18.

Obsolete eDirectory Schema Extensions

GroupWise 18 no longer extends the eDirectory schema to accommodate GroupWise-specific objects. After upgrading domains and post offices to GroupWise 18, the associated GroupWise objects in eDirectory are *not* used by GroupWise 18.

IMPORTANT: It is not necessary to remove obsolete GroupWise objects from eDirectory. If you want to remove them, use iManager (recommended) or ConsoleOne (not recommended). If you use ConsoleOne, remove (or move) the GroupWise snapins first. Otherwise, you run the risk of inadvertently deleting a GroupWise account. Always back up your domain database before taking any action.

Obsolete Software Distribution Directories

GroupWise 18 no longer uses software distribution directories. After you have upgraded post offices, you can delete the associated software distribution directories in the Admin console.

- 1 In the [GroupWise Admin console](#), click **System > Legacy**.
- 2 Click **Software Areas**.
- 3 Select the obsolete software distribution directory, and then click **Delete**.

GroupWise 18 uses the Client Auto-Update feature instead of software distribution directories. For usage instructions, see “[Using Client Auto-Update to Distribute the GroupWise Client Software](#)” in the *GroupWise 18 Administration Guide*.

Obsolete GroupWise Gateways

There are no known issues with using GroupWise gateways with GroupWise 18. However, GroupWise gateways are legacy products that are not supported with the current GroupWise version. You can delete obsolete gateways in the GroupWise Admin console.

- 1 In the [GroupWise Admin console](#), click **System > Legacy**.
- 2 On the **Gateways** tab, select the obsolete gateway, and then click **Delete**.

NetWare Compatibility

As of GroupWise 2012, GroupWise does not include GroupWise agents that run on NetWare, because NetWare has entered the Extended Support phase of the Micro Focus Support Life cycle. For more information, see TID 7003092, “NetWare Support,” in the [Micro Focus Support Knowledgebase](#) (<http://www.novell.com/support/>).

If you currently have NetWare servers in your GroupWise system, you must decide how to handle them as you move forward with your GroupWise 18 upgrade. You have several alternatives:

- ♦ Migrate NetWare servers to Open Enterprise Server (OES).
- ♦ Move domains and post offices from NetWare servers to [supported Linux servers](#).
- ♦ Move domains and post offices from NetWare servers to [supported Windows servers](#).

You might decide to use one or more of these alternatives as you upgrade your GroupWise system to GroupWise 18. Detailed instructions for each alternative are provided in “[Migrating Away from NetWare](#)” in the *GroupWise 2012 Installation Guide*, because GroupWise 2012 is the first version where NetWare is not supported.

25 Preparing Your Existing GroupWise System for the Upgrade

To prepare your GroupWise system to be upgraded to version 18, complete the following tasks:

- ❑ Validate your domain and post office databases to ensure that there are no physical inconsistencies with the database. If problems exist, you should recover or rebuild the database. For information about validating, recovering, or rebuilding a database, see the documentation for your current GroupWise version at the [Micro Focus Documentation website](#).
- ❑ Back up each domain or post office immediately before upgrading it. For information about backing up your GroupWise databases, see the documentation for your current GroupWise version at the [Micro Focus Documentation website](#).
- ❑ Collect the information about your existing GroupWise system that the GroupWise Installation Wizard prompts you for as you upgrade to GroupWise 18. You might find it helpful to review [Planning Your GroupWise System](#) and to record the information on the worksheets provided for an initial installation:
 - ♦ [Simple GroupWise System Worksheet](#) (for a small GroupWise system that is all on one server)
 - ♦ [Primary Domain Worksheet](#) (for a primary domain on its own server)
 - ♦ [Secondary Domain Worksheet](#) (for each secondary domain)
 - ♦ [Post Office Worksheet](#) (for each post office)
 - ♦ [GroupWise WebAccess Installation Worksheet](#) (for each WebAccess Application)
 - ♦ [GroupWise Calendar Publishing Host Worksheets](#) (for each Calendar Publishing Host Application)
 - ♦ [GroupWise Monitor Installation Worksheets](#) (for each Monitor Agent/Application)

- ❑ Prepare the existing agents for upgrade. The Installation console uses the same agent configuration for GroupWise 18 that is in use for your existing GroupWise system. Your current agent configuration might not be the best option for GroupWise 18. The [GroupWise 2012 Installation Guide](#) provides information for reconfiguring your existing agents in preparation for the upgrade.

Linux: The Installation console can locate agents that are listed in the `gwha.conf` file used by the GroupWise High Availability Service (gwha). For background information, see “[Enabling the GroupWise High Availability Service for the Linux GroupWise Agents](#)” in the *GroupWise 2012 Installation Guide*.

Also, the Admin console cannot manage agents that run with the user interface provided by the `--show` switch. For background information, see “[Starting the Linux Agents with a User Interface](#)” in the *GroupWise 2012 Installation Guide*.

Windows: The Installation console can locate agents that have been running as Windows services. For background information, see “[Starting the Windows Agents Manually or Automatically as Services](#)” in the *GroupWise 2012 Installation Guide*.

Also, the Admin console cannot manage agents that run as applications with a user interface. For background information, see “[Starting the Windows Agents Manually As Applications](#)” in the *GroupWise 2012 Installation Guide*.

In preparation for GroupWise 18, you can configure your existing agents to run without a user interface, so that the Installation console can automatically locate them, or you can specify the locations of domains and post offices during the upgrade process.

- ❑ Ensure that all GroupWise servers meet the system requirements listed in [GroupWise Server Requirements](#).
- ❑ When you upgrade the primary domain to GroupWise 18, you establish the user name and password for the GroupWise Super Admin. For background information about this administrative user, see [Primary Domain: Super Admin Creation](#). Decide on the Super Admin user name and password before you start the upgrade process.
- ❑ When you upgrade a domain or post office on a Linux server, ensure that the Linux operating system media is available, either physically or in a repository, in case the Installation Wizard needs to install supporting packages on the Linux server.
- ❑ Ensure that all GroupWise client user workstations meet the system requirements listed in [GroupWise User Requirements](#).

IMPORTANT: Before upgrading to 18.5, make sure your GroupWise server certificates pass the “[Certificate Best Practices](#)” requirements in the *GroupWise 18 Administration Guide* or you will have problems during/after the upgrade.

26 Installing the GroupWise 18 Software

Before installing the GroupWise 18 software, review the background information and complete the tasks in the following sections:

- ❑ [Chapter 24, “Understanding the Upgrade Process,” on page 181](#)
- ❑ [Chapter 25, “Preparing Your Existing GroupWise System for the Upgrade,” on page 187](#)

Then follow the installation instructions for the platform where the domain or post office to upgrade is located.

Linux: Installing the GroupWise 18 Software

- 1 Stop the existing GroupWise agents that are running on the server to upgrade.
- 2 Ensure that the Linux operating system media is available, either physically or in a repository, in case the Installation Wizard needs to install supporting packages on the Linux server.
- 3 In a terminal window, become `root` by entering `su -` and the `root` password.
- 4 Browse to the location of the extracted software, and run the following command to start the install:

```
./install.sh
```

- 5 Type the number for the language in which you want to run the GroupWise Installation Wizard, and press Enter to select **OK**.
- 6 Type 2 for **Installation** and press Enter.
- 7 Enter `a` to accept the License Agreement and to display the Software list.
- 8 Enter 1 for **GroupWise Server** and to display the Actions list.
- 9 Enter 1 for **Install** and to install the GroupWise Server component.

The packages for the GroupWise Server component (Admin Service and agents) are installed on the server. If any supporting packages are not available on the server, the Installation Wizard automatically installs them from the operating system media.

- 10 When the installation is finished, press any key to return to the Installation Options list.

All of the GroupWise agents are installed on every GroupWise server. The MTA and, optionally, the GWIA are configured to run on a domain server. The POA and the DVA are configured to run on a post office server.

The Installation Wizard starts any agents that typically run on the server.

IMPORTANT: Running the GroupWise 18 agents does not upgrade the GroupWise databases on the server to GroupWise 18. Updating the databases is performed in a subsequent step.

- 11 Enter 2 for **Configure** to start the GroupWise Admin Service and display instructions for accessing the Installation console to upgrade the GroupWise server to GroupWise 18.

- 12 Right-click the URL under **To install or configure a new GroupWise server**, and then click **Open Link** to open your web browser.

If your web browser does not offer this functionality, open your web browser and copy the URL into it.

- 13 Accept the GroupWise CA signed certificate that the Installation Wizard automatically provides for accessing the Installation console.

The browser session will then authorize you for the next hour to perform installation console tasks. If the browser does not automatically authorize the session, you must manually authorize it by running in a terminal the **gwsadmin-ipc authorize** command specified in your web browser.

- 14 Continue with the instructions for the upgrade task that you are performing:

- ♦ [Chapter 27, “Upgrading the Primary Domain Server,” on page 193](#)
- ♦ [Chapter 28, “Upgrading a Secondary Domain Server,” on page 197](#)
- ♦ [Chapter 29, “Upgrading a Post Office Server,” on page 201](#)

Windows: Installing the GroupWise 18 Software

- 1 Stop the existing GroupWise agents that are running on the server to upgrade.
- 2 Run **setup.exe** at the root of the extracted GroupWise software to start the GroupWise Installation Wizard.
- 3 Click **GroupWise Server** to install the GroupWise Server component.
- 4 Select the language in which you want to perform the installation, and then click **OK** to start the GroupWise Server Setup Wizard.
- 5 Click **Next** to continue.
- 6 Accept the **License Agreement**, and then click **Next** to display the Custom Setup page.

The following components are available for installation:

- ♦ **GroupWise Server:** (Required) Consists of the Admin Service, the POA, the MTA, the GWIA, and the DVA.

All of the GroupWise agents are installed on every GroupWise server. The MTA and, optionally, the GWIA are configured to run on a domain server. The POA and the DVA are configured to run on a post office server.

- ♦ **Client Auto-Update Repository:** (Optional) Helps you distribute the GroupWise client software to users' Windows workstations.

For usage instructions, see [“Using Client Auto-Update to Distribute the GroupWise Client Software”](#) in the *GroupWise 18 Administration Guide*.

- 7 Click **Next** to continue, and then click **Install** to install the GroupWise software.
- 8 When the GroupWise software is installed, click **Finish** to return to the main page of the Installation Wizard, and then close the Installation Wizard.
- 9 Reboot the Windows server to complete the installation and start the GroupWise Installation console.

You should see two new icons on your Windows desktop.

- 10** On your Windows desktop, double-click **GroupWise Install** to open your web browser and to access the Installation console.

This starts the GroupWise Admin Service and launches the GroupWise Installation console in your web browser.

After installation, use **GroupWise Admin Console** to access the Admin console for ongoing GroupWise system administration.

- 11** Accept the GroupWise CA signed certificate that the Installation Wizard automatically provides for accessing the Installation console.

The browser session will then authorize you for the next hour to perform installation console tasks. If the browser does not automatically authorize the session, you must manually authorize it by running in a terminal the **gwsadmin-ipc authorize** command specified in your web browser.

- 12** Continue with the instructions for the upgrade task that you are performing:

- ♦ [Chapter 27, “Upgrading the Primary Domain Server,” on page 193](#)
- ♦ [Chapter 28, “Upgrading a Secondary Domain Server,” on page 197](#)
- ♦ [Chapter 29, “Upgrading a Post Office Server,” on page 201](#)

27 Upgrading the Primary Domain Server

Before you upgrade the primary domain server, you should have reviewed the following sections and completed the accompanying tasks:

- ❑ [Chapter 3, “GroupWise System Architecture,” on page 21](#)
- ❑ [Chapter 4, “GroupWise Server Requirements,” on page 27](#)
- ❑ [Chapter 24, “Understanding the Upgrade Process,” on page 181](#)
- ❑ [Chapter 25, “Preparing Your Existing GroupWise System for the Upgrade,” on page 187](#)
- ❑ [Chapter 26, “Installing the GroupWise 18 Software,” on page 189](#)

After you install the GroupWise 18 software on the primary domain server, the Installation Wizard displays the Installation console in your web browser.

IMPORTANT: As a security feature, the Installation console times out after one hour. For instructions to renew the session, see [Handling an Installation Timeout](#).

- 1 In the Installation console, click **Upgrade an Existing Domain or Post Office to GroupWise 18**.
What displays next depends on whether the Installation console can detect the existing domains and post offices on the server. The conditions for automatic detection are described in [Preparing Your Existing GroupWise System for the Upgrade](#).
- 2 (Conditional) If the Installation console can locate existing domains and post offices:
 - 2a (Conditional) If there are any domains and post offices on the primary domain server that you do not want to upgrade along with the primary domain, select them, and then click **Remove** to remove them from the list.
 - 2b (Conditional) If you want to change the IP address or Admin port for any domain or post office, click its name to display the Network Information dialog box.
Specify the desired IP address or Admin port, and then click **OK**.
 - 2c Skip to [Step 4](#) to perform the upgrade.
- 3 (Conditional) If the Installation console cannot locate existing domains and post offices:
 - 3a Click **Add**.
 - 3b Browse to and select the primary domain folder.
 - 3c Click **OK**, and then review the MTA IP address and domain Admin port that the Installation console has provided.
 - 3d (Optional) Change the information as needed.
 - 3e Click **OK** to return to the Installation console.
 - 3f Repeat [Step 3a](#) through [Step 3e](#) for each additional domain and post office that you want to upgrade on the primary domain server.
 - 3g Continue with [Step 4](#) to perform the upgrade.

- 4 In the list of domains and post offices to upgrade, click **Next** to display the Credentials page.
- 5 Specify the user name for the GroupWise Super Admin, type the password twice for confirmation, and then click **Next** to display the Summary page.
- 6 Review the information to ensure that it is correct, and then click **Finish** to perform the upgrade.
- 7 Click **Go to the GroupWise Administration console now**.
- 8 Accept the GroupWise CA signed certificate that the Installation console has automatically provided for accessing the Admin console.

The Login fields are displayed.

- 9 Specify the GroupWise Super Admin user name and password that you established in [Step 5](#), and then click **Login** to display the Overview page in the GroupWise Admin console.

To finish the upgrade process, you must restart the MTA for the primary domain. You must also restart the agents for any other upgraded domains and post offices on the primary domain server.

If the primary domain has a GWIA, it was also upgraded along with the primary domain and its MTA. However, you do not need to restart the upgraded GWIA.

IMPORTANT: If you are upgrading from GroupWise 8, see [Agent Upgrades](#) for release-specific information.

- 10 To restart the MTA in the upgraded primary domain:

- 10a In the Domain box on the Overview page, click **MTA** or click **Running > MTA** to display the MTA properties page.

- 10b Click **Stop Agent**, and then click **Start Agent** to restart the upgraded MTA.

- 10c (Optional) Click **Launch MTA Console** to open the MTA console in a new browser window.

TIP: You can conveniently open the MTA console on the Overview page by clicking **Running**, and then clicking the IP address of the MTA.

If the primary domain has a GWIA, it was also upgraded along with the primary domain and its MTA. However, you do not need to restart the upgraded GWIA.

IMPORTANT: If you are upgrading from GroupWise 8, see [“Agent Upgrades” on page 183](#) for release-specific information.

- 10d Click **Overview** to return to the Overview page.

- 11 (Conditional) If the primary domain server has additional upgraded domains, repeat [Step 10](#) for the MTA in each upgraded domain.

- 12 (Conditional) If the primary domain server has upgraded post offices:

- 12a In the Domain box on the Overview page, click **Running** next to the Post Office icon , and then click **POA** to display the POA properties page.

- 12b Click **Stop Agent**, and then click **Start Agent** to restart the upgraded POA.

- 12c (Optional) Click **Launch POA Console** to open the POA console in a new browser window.

TIP: You can conveniently open the POA console on the Overview page by clicking **Running**, and then clicking the IP address of the POA.

- 12d** Click **Overview** to return to the Overview page.
- If the post office has a DVA, it was also upgraded along with the post office and its POA. However, you do not need to restart the upgraded DVA.
- 13** (Conditional) If the primary domain server has additional post offices, repeat [Step 12](#) for the POA in each upgraded post office.
- 14** Continue with the next upgrade task for your GroupWise system:
- ♦ [Upgrading a Secondary Domain Server](#)
 - ♦ [Upgrading a Post Office Server](#)
 - ♦ [Upgrading GroupWise WebAccess](#)
 - ♦ [Upgrading the Calendar Publishing Host](#)
 - ♦ [Upgrading GroupWise Monitor](#)

28 Upgrading a Secondary Domain Server

After you have upgraded the primary domain server in your GroupWise system, you can upgrade secondary domains in your GroupWise system in any order that is convenient for you.

Before you upgrade a secondary domain server, review the following sections and complete the accompanying tasks if you have not done so recently:

- ❑ [Chapter 3, “GroupWise System Architecture,” on page 21](#)
- ❑ [Chapter 4, “GroupWise Server Requirements,” on page 27](#)
- ❑ [Chapter 24, “Understanding the Upgrade Process,” on page 181](#)
- ❑ [Chapter 25, “Preparing Your Existing GroupWise System for the Upgrade,” on page 187](#)

To upgrade a secondary domain server:

- 1 Stop the existing GroupWise agents that are running on the server to upgrade.
- 2 Install the GroupWise 18 software on the secondary domain server.

See [Installing the GroupWise 18 Software](#) for instructions.

When the software installation is complete, the Installation Wizard displays the Installation console in your web browser.

IMPORTANT: As a security feature, the Installation console times out after one hour. For instructions to renew the session, see [Handling an Installation Timeout](#).

- 3 In the Installation console, click **Upgrade an Existing Domain or Post Office to GroupWise 18**.

What displays next depends on whether the Installation console can detect the existing domains and post offices on the server. The conditions for automatic detection are described in [Chapter 25, “Preparing Your Existing GroupWise System for the Upgrade,” on page 187](#).

- 4 (Conditional) If the Installation console can locate existing domains and post offices:

- 4a (Conditional) If there are any domains and post offices on the secondary domain server that you do not want to upgrade, select them, and then click **Remove**.

- 4b (Conditional) If you want to change the IP address or Admin port for any domain or post office, click its name to display the Network Information dialog box.

Specify the desired IP address or Admin port, and then click **OK**.

- 4c Skip to [Step 6](#) to perform the upgrade.

- 5 (Conditional) If the Installation console cannot locate existing domains and post offices:

- 5a Click **Add**.

- 5b Browse to and select the secondary domain folder.

- 5c Click **OK**, and then review the MTA IP address and domain Admin port that the Installation console has provided.

- 5d (Optional) Change the information as needed.

- 5e Click **OK** to return to the Installation console.

- 5f If you want to upgrade additional domains and post offices on the domain server, repeat [Step 5a](#) through [Step 5e](#).
- 5g Continue with [Step 6](#) to perform the upgrade.
- 6 In the list of secondary domains, and optionally, post offices to upgrade, click **Next** to display the Credentials page.
 - 7 Specify the IP address of the primary domain server and the password for the GroupWise Super Admin, and then click **Next** to display the Summary page.
 - 8 Review the information to ensure that it is correct, and then click **Finish** to perform the upgrade.
 - 9 (Optional) Click the Existing Configuration slide-out to list all upgraded domains and post offices.
 - 10 Click **Go to the GroupWise Administration console now**.
 - 11 Accept the GroupWise CA signed certificate that the Installation console has automatically provided for accessing the Admin console.
The Login fields are displayed.
 - 12 Specify the GroupWise Super Admin user name and password that you established when you upgraded the primary domain, and then click **Login** to display the Overview page in the Admin console.

To finish the upgrade process, you must restart the agents for all upgraded secondary domains and post offices on the secondary domain server.

If any secondary domains have GWIAs, they were also upgraded along with the secondary domains. However, you do not need to restart the upgraded GWIAs.
-
- IMPORTANT:** If you are upgrading from GroupWise 8, see [“Agent Upgrades” on page 183](#) for release-specific information.
-
- 13 To restart the MTA in the upgraded secondary domain:
 - 13a In the Domain box on the Overview page, click **MTA** or click **Running > MTA** to display the MTA properties page.
 - 13b Click **Stop Agent**, and then click **Start Agent** to restart the upgraded MTA.
 - 13c (Optional) Click **Launch MTA Console** to open the MTA console in a new browser window.
-
- TIP:** You can conveniently open the MTA console on the Overview page by clicking **Running**, and then clicking the IP address of the MTA.
-
- If any secondary domains have GWIAs, they were also upgraded along with the secondary domains. However, you do not need to restart the upgraded GWIAs.
-
- IMPORTANT:** If you are upgrading from GroupWise 8, see [“Agent Upgrades” on page 183](#) for release-specific information.
-
- 14 (Conditional) If the secondary domain server has additional upgraded domains, repeat [Step 13](#) for the MTA in each upgraded domain.

15 (Conditional) If the secondary domain server has upgraded post offices:

15a In the Domain box on the Overview page, click **Running** next to the Post Office icon , and then click **POA** to display the POA properties page.

15b Click **Stop Agent**, and then click **Start Agent** to restart the upgraded POA.

15c (Optional) Click **Launch POA Console** to open the POA console in a new browser window.

NOTE: You can conveniently open the POA console on the Overview page by clicking **Running**, and then clicking the IP address of the POA.

If the post office has a DVA, it was also upgraded along with the post office and its POA. However, you do not need to restart the upgraded DVA.

16 (Conditional) If the secondary domain server has additional post offices, repeat [Step 15](#) for the POA in each upgraded post office.

17 Continue with the next upgrade task for your GroupWise system:

- ♦ [Upgrading a Post Office Server](#)
- ♦ [Upgrading GroupWise WebAccess](#)
- ♦ [Upgrading the Calendar Publishing Host](#)
- ♦ [Upgrading GroupWise Monitor](#)

29 Upgrading a Post Office Server

You can upgrade a post office after you have upgraded the domain that owns it.

When the post office is located on the same server with the owning domain, you can upgrade it along with its domain. See these associated tasks:

- ❑ [Chapter 27, “Upgrading the Primary Domain Server,” on page 193](#)
- ❑ [Chapter 28, “Upgrading a Secondary Domain Server,” on page 197](#)

When the post office is on a separate post office server, review the following sections and complete the accompanying tasks if you have not done so recently:

- ❑ [Chapter 3, “GroupWise System Architecture,” on page 21](#)
- ❑ [Chapter 4, “GroupWise Server Requirements,” on page 27](#)
- ❑ [Chapter 24, “Understanding the Upgrade Process,” on page 181](#)
- ❑ [Chapter 25, “Preparing Your Existing GroupWise System for the Upgrade,” on page 187](#)

To upgrade a post office server:

- 1 Stop the existing GroupWise agents that are running on the server to upgrade.
- 2 Install the GroupWise 18 software on the post office server.
See [Chapter 26, “Installing the GroupWise 18 Software,” on page 189](#) for instructions.
When the software installation is complete, the Installation Wizard displays the Installation console in your web browser.
- 3 In the Installation console, click **Upgrade an Existing Domain or Post Office to GroupWise 18**.
What displays next depends on whether the Installation console can detect the existing domains and post offices on the server. The conditions for automatic detection are described in [Chapter 25, “Preparing Your Existing GroupWise System for the Upgrade,” on page 187](#).
- 4 (Conditional) If the Installation console can locate existing post offices:
 - 4a (Conditional) If there are any post offices on the post office server that you do not want to upgrade, select them, and then click **Remove**.
 - 4b (Conditional) If you want to change the IP address or Admin port for any post office, click its name to display the NetWork Information dialog box.
 - 4c Skip to [Step 6](#) to perform the upgrade.
- 5 (Conditional) If the Installation console cannot locate existing post offices:
 - 5a Click **Add**.
 - 5b Browse to and select the post office folder.
 - 5c Click **OK**, and then review the POA IP address and post office Admin port that the Installation console has provided.
 - 5d (Optional) Change the information as needed.
 - 5e Click **OK** to return to the Installation console.

- 5f** (Conditional) If you want to upgrade additional post offices on the post office server, repeat [Step 5a](#) through [Step 5e](#).
- 5g** Continue with [Step 6](#) to perform the upgrade.
- 6** In the list of post offices to upgrade, click **Next** to display the Credentials page.
- 7** Specify the IP address of the primary domain server and the password for the GroupWise Super Admin, and then click **Next** to display the Summary page.
- 8** Review the information to ensure that it is correct, and then click **Finish** to perform the upgrade.
- 9** (Optional) Click the Existing Configuration slide-out to list all upgraded domains and post offices.
- 10** Click **Go to the GroupWise Administration console now**.
- 11** Accept the GroupWise CA signed certificate that the Installation console has automatically provided for accessing the Admin console.
The Login fields are displayed.
- 12** Specify the IP address of the primary domain server and the password for the GroupWise Super Admin, and then click **Next** to display the Summary page.
To finish the upgrade process, you must restart the POAs for all upgraded post offices on the post office server.
- 13** To restart the POA in the upgraded post office:
- 13a** In the Domain box on the Overview page, click **Running** next to the Post Office icon , and then click **POA** to display the POA properties page.
- 13b** Click **Stop Agent**, and then click **Start Agent** to restart the upgraded POA.
- 13c** (Optional) Click **Launch POA Console** to open the POA console in a new browser window.
-
- NOTE:** You can conveniently open the POA console on the Overview page by clicking **Running**, and then clicking the IP address of the POA.
-
- 14** (Conditional) If the post office server has additional upgraded post offices, repeat [Step 13](#) for the POA in each upgraded post office.
- 15** Continue with the next upgrade task for your GroupWise system:
- ♦ [“Upgrading GroupWise WebAccess” on page 203](#)
 - ♦ [“Upgrading the Calendar Publishing Host” on page 205](#)
 - ♦ [“Upgrading GroupWise Monitor” on page 206](#)

30 Upgrading GroupWise Agents and Applications

See the following sections for information about upgrading GroupWise agents and applications.

- ♦ [“Upgrading the Document Viewer Agent” on page 203](#)
- ♦ [“Upgrading GroupWise WebAccess” on page 203](#)
- ♦ [“Upgrading the Calendar Publishing Host” on page 205](#)
- ♦ [“Upgrading GroupWise Monitor” on page 206](#)
- ♦ [“Implementing TLS Encryption” on page 207](#)

Upgrading the Document Viewer Agent

DVAs on the same servers with POA are automatically upgraded along with the POAs. The following situations require additional upgrade actions:

- ♦ If you installed additional DVAs on other servers, you must manually upgrade them. Stop the existing DVA, and then install and set up the GroupWise 18 DVA. For instructions, see [“Scaling Your DVA Installation”](#) in the *GroupWise 18 Administration Guide*.
- ♦ If you were not using the DVA in your existing GroupWise system, you must run at least one DVA in your GroupWise 18 system. For instructions, see [“Installing the DVA”](#) in the *GroupWise 18 Administration Guide*.

In all cases, in order to make the DVA appear in the Admin console, you must manually add a DVA object. For instructions, see [“Setting Up the DVA”](#) in the *GroupWise 18 Administration Guide*.

Upgrading GroupWise WebAccess

After you have upgraded a domain and a post office to GroupWise 18, you can upgrade WebAccess for that domain and post office. For information about upgrade issues that you should consider, see [WebAccess Upgrades](#).

The POA that the GroupWise WebAccess Application communicates with must be configured for SOAP. A secure TLS connection between the POA and the WebAccess Application is highly recommended.

IMPORTANT: Before you upgrade your WebAccess Application, you must upgrade all post offices that connect to your WebAccess Application or users can have issues logging in.

- ♦ [“Preparing to Upgrade the WebAccess Application” on page 204](#)
- ♦ [“Installing the GroupWise 18 WebAccess Application” on page 204](#)
- ♦ [“Clearing User Browser Caches to Display GroupWise 18 WebAccess Correctly” on page 205](#)

Preparing to Upgrade the WebAccess Application

GroupWise 18 requires WebAccess to use TLS. Before you upgrade, you must configure Apache with TLS or WebAccess will not run. After doing that, you can upgrade your WebAccess software whenever it is convenient as you upgrade your GroupWise system. However, in order to use the WebAccess Application console, you must change the way it is configured. For instructions, see [“Using the WebAccess Application Console”](#) in the *GroupWise 18 Administration Guide*.

IMPORTANT: If you are upgrading from GroupWise 8 directly to GroupWise 18, you need to understand that the WebAccess Agent is no longer part of GroupWise. See [“Understanding WebAccess Updates”](#) and [“Updating GroupWise WebAccess”](#) in the *GroupWise 2012 Installation Guide* before you upgrade WebAccess from GroupWise 8 directly to GroupWise.

Installing the GroupWise 18 WebAccess Application

- 1 (Conditional) If you are upgrading from GroupWise 8:
 - 1a Prepare the POA to work successfully with the WebAccess Application, as described in the following sections in [“Post Office Agent”](#) in the *GroupWise 18 Administration Guide*:
 - ♦ [“Supporting SOAP Clients”](#)
 - ♦ [“Securing the Post Office with SSL Connections to the POA”](#)
 - 1b Stop the existing WebAccess Agent.
- 2 (Conditional) On Linux, stop Tomcat.

```
SLES 11:      rcgrpwise-tomcat8 stop
```

On Windows, the Installation Wizard does this for you.

- 3 To upgrade WebAccess to GroupWise 18, follow the standard installation instructions in [Setting Up GroupWise WebAccess \(Legacy\)](#).

IMPORTANT: If more than one web-based GroupWise component (WebAccess, Calendar Publishing Host, and/or Monitor) is installed on the same server, you must upgrade all web-based GroupWise components at the same time. After one existing web-based component has been upgraded to GroupWise 18, other web-based components on the server do not work until they also are upgraded to GroupWise 18.

- 4 Reconfigure the WebAccess Application console.

For instructions, see [“Enabling the WebAccess Application Console”](#) in the *GroupWise 18 Administration Guide*.
- 5 (Conditional) If you are upgrading from GroupWise 8, complete the steps in [“Cleaning Up the WebAccess Server after Updating to GroupWise 2012”](#) and [“Updating Access Control for WebAccess Users”](#) in the *GroupWise 2012 Installation Guide*.
- 6 Continue with [Clearing User Browser Caches to Display GroupWise 18 WebAccess Correctly](#).

Clearing User Browser Caches to Display GroupWise 18 WebAccess Correctly

After you have upgraded the WebAccess Application to GroupWise 18, notify your GroupWise WebAccess users that they should clear their browser caches before logging into their mailboxes with the upgraded version of GroupWise WebAccess. If old GroupWise WebAccess files are used from users' browser caches, they might not be compatible with the upgraded files from the web server. The results can be unpredictable and undesirable.

Upgrading the Calendar Publishing Host

There are no Calendar Publishing Host upgrade issues. You can upgrade the Calendar Publishing Host to GroupWise 18 at any time after the POA that it communicates with has been upgraded. However, in order to use the CalPub Host Admin console, you must change the way it is configured. For instructions, see [Setting Up Calendar Publishing Administration](#).

- ♦ “Installing the GroupWise 18 Calendar Publishing Host Application” on page 205
- ♦ “Clearing User Browser Caches to Display Published Calendars Correctly” on page 206

Installing the GroupWise 18 Calendar Publishing Host Application

- 1 (Conditional) On Linux, stop Tomcat.

```
SLES 11:      rcgrpwise-tomcat8 stop
```

On Windows, the Installation Wizard does this for you.

- 2 To upgrade the Calendar Publishing Host to GroupWise 18, follow the standard installation instructions in [Setting Up the GroupWise Calendar Publishing Host](#).

IMPORTANT: If more than one web-based GroupWise component (WebAccess, Calendar Publishing Host, and/or Monitor) is installed on the same server, you must upgrade all web-based GroupWise components at the same time. After one existing web-based component has been upgraded to GroupWise 18, other web-based components on the server do not work until they also are upgraded to GroupWise 18.

- 3 Reconfigure the CalPub Host Admin console.
For instructions, see [Setting Up Calendar Publishing Administration](#).
- 4 (Conditional) If you are upgrading from GroupWise 8, complete the steps in “[Cleaning Up the Calendar Publishing Host Server after Updating to GroupWise 2012](#)” in the *GroupWise 2012 Installation Guide*.
- 5 Continue with [Clearing User Browser Caches to Display Published Calendars Correctly](#).

Clearing User Browser Caches to Display Published Calendars Correctly

After you have upgraded the Calendar Publishing Host Application to GroupWise 18, notify your GroupWise users that they should clear their browser caches before accessing published calendars. If old Calendar Publishing files are used from users' browser caches, they might not be compatible with the upgraded files from the web server. The results can be unpredictable and undesirable.

External users of published calendars might not see some aspects of the GroupWise 18 Calendar Publishing interface until after they clear their browser caches.

Upgrading GroupWise Monitor

After you have upgraded at least one domain to GroupWise 18, you can upgrade GroupWise Monitor. For information about upgrade issues that you should consider, see [Agent Upgrades](#).

- ♦ [“Preparing to Upgrade GroupWise Monitor” on page 206](#)
- ♦ [“Installing the Monitor Software” on page 206](#)
- ♦ [“Clearing Browser Caches to Display GroupWise 18 Monitor Correctly” on page 207](#)
- ♦ [“Reconfiguring the GroupWise High Availability Service” on page 207](#)

Preparing to Upgrade GroupWise Monitor

GroupWise Monitor is not dependent on any other GroupWise agents, so you can upgrade the Monitor Agent and the Monitor Application to GroupWise 18 at any time.

IMPORTANT: If you are upgrading from GroupWise 8 directly to GroupWise 18, you need to understand that Monitor no longer relies on eDirectory objects for its configuration information. All configuration information is located in the `gwmonitor.cfg` file instead. See [“Understanding Monitor Updates”](#) and [“Updating GroupWise Monitor”](#) in the *GroupWise 2012 Installation Guide* before you upgrade Monitor from GroupWise 8 directly to GroupWise 18.

Installing the Monitor Software

- 1 Stop the existing Monitor Agent.
- 2 (Conditional) On Linux, stop Tomcat.

```
SLES 11:      rcgrpwise-tomcat8 stop
```

On Windows, the Installation Wizard does this for you.

- 3 To upgrade Monitor to GroupWise 18, follow the standard installation instructions in [Setting Up GroupWise Monitor](#).

IMPORTANT: If more than one web-based GroupWise component (WebAccess, Calendar Publishing Host, and/or Monitor) is installed on the same server, you must upgrade all web-based GroupWise components at the same time. After one existing web-based component has been upgraded to GroupWise 18, other web-based components on the server do not work until they also are upgraded to GroupWise 18.

- 4 Restart all GroupWise services on the server.
- 5 (Conditional) If you are upgrading from GroupWise 8, complete the steps in “[Cleaning Up the Monitor Server after Updating to GroupWise 2012](#)” in the *GroupWise 2012 Installation Guide*.
- 6 Continue with [Clearing Browser Caches to Display GroupWise 18 Monitor Correctly](#).

Clearing Browser Caches to Display GroupWise 18 Monitor Correctly

After you have upgraded the Monitor Application to GroupWise 18, clear your browser cache before accessing the upgraded version of GroupWise Monitor. If old GroupWise Monitor files are used from users’ browser caches, they might not be compatible with the upgraded files from the web server. The results can be unpredictable and undesirable.

Reconfiguring the GroupWise High Availability Service

On Linux, the GroupWise High Availability Service (gwha), that works in conjunction with GroupWise Monitor to automatically restart the Linux GroupWise agents, now requires an additional file. The `gwha.allow` file lists the user that the High Availability Service uses to log in to the Monitor Agent. This file increases the security of the interaction between the High Available Service and the Monitor Agent. For setup instructions, see [Step 3](#) in [Creating a GroupWise High Availability Service User](#).

Implementing TLS Encryption

If you have not yet implemented TLS in your GroupWise system, you can now easily generate GroupWise CA signed certificates by using the native GroupWise certificate authority (CA). For instructions, see “[Configuring Server Certificates and TLS](#)” in the *GroupWise 18 Administration Guide*.

31 Upgrading Users' GroupWise Client Software

After a post office is upgraded to GroupWise 18, users who have accounts in that post office can start using the GroupWise 18 clients. You can give users access to a *GroupWise 18* software on the GroupWise download page, so that they can install the GroupWise client themselves, or you can use the other methods of client software distribution described in “[Distributing the GroupWise Client](#)” in the *GroupWise 18 Administration Guide*.

32 Transitioning from ConsoleOne

Use the table below to learn how to perform familiar ConsoleOne tasks in the GroupWise Admin console.

Task	ConsoleOne Functionality	Admin Console Functionality
Locate a domain or post office to edit its properties.	Use the eDirectory View to browse the eDirectory tree structure to find the Domain or Post Office object.	Click Domains or Post Offices in the Administration panel to list the Domain or Post Office objects in your GroupWise system.
	or	or
	Use the GroupWise View to list the Domain or Post Office objects in your GroupWise system.	Click the domain or post office on the System Overview page. or Type the name of the domain or post office in the Global Search field.
Locate a user to edit its properties.	Use the eDirectory View to browse the eDirectory tree structure to find the User object.	Click Users in the Administration panel to list the User objects in your GroupWise system.
	or	or
	Use the GroupWise View to list the User objects in your GroupWise system.	Type the user's first name, last name, GroupWise user name, email address, or file ID (FID) in the Global Search field.
Locate an agent to edit its properties.	Use the eDirectory View to browse the eDirectory tree structure to find the agent object.	Click the agent type in the Administration panel to list the agent objects of that type in your GroupWise system.
	or	or
	Use the GroupWise View to list the agent objects in your GroupWise system.	Click the agent on the System Overview page. or Type the agent's IP address in the Global Search field.

Task	ConsoleOne Functionality	Admin Console Functionality
Perform GroupWise system operations.	Click Tools > GroupWise System Operations .	Click System in the Administration panel. or Type the name of the GroupWise system tool in the Global Search field.
Run GroupWise utilities.	Click Tools > GroupWise Utilities .	Click System in the Administration panel. or Type the name of the GroupWise system tool in the Global Search field.
Perform database maintenance.	Browse to and select a Domain or Post Office object, and then click Tools > GroupWise Utilities > System Maintenance .	Display the properties of a domain or post office, and then click Maintenance > System Maintenance .
Perform Mailbox/Library Maintenance.	Browse to and select a Post Office or User object, and then click Tools > GroupWise Utilities > System Maintenance .	Display the properties of a post office or user, and then click Maintenance > Mailbox/Library Maintenance .
Set Client Options.	Browse to and select a Domain, Post Office, or User object, and then click Tools > GroupWise Utilities > Client Options .	Display the properties of a domain, post office, or user, and then click Client Options .

If parts of your GroupWise system are still running legacy GroupWise agents, you should continue to use the legacy ConsoleOne and its snap-ins to administer the legacy parts of your GroupWise system. For convenience, you can safely run the GroupWise 2012 ConsoleOne and snap-ins on most of the legacy parts of your GroupWise system. However, the GroupWise 2012 snap-ins do not support specific legacy GroupWise functionality, such as the WebAccess Agent and its eDirectory objects, which no longer exist in GroupWise 2012.

When you are in the GroupWise 18 Admin console, you can easily see which agents have not yet been upgraded. Legacy agents that have not yet been upgraded to GroupWise 18 are marked with their GroupWise version.

VI Appendixes

See the appendixes below for additional information about employing GroupWise.

- ♦ [Appendix A, “GroupWise Version Compatibility,” on page 215](#)
- ♦ [Appendix B, “Attributes, Operators, and Values for Object Filters,” on page 221](#)
- ♦ [Appendix C, “Invalid Characters in GroupWise Object Names and Email Addresses,” on page 225](#)
- ♦ [Appendix D, “Cross-Platform Connections,” on page 227](#)

A

GroupWise Version Compatibility

Use the tables in this section to determine compatibility among the following GroupWise versions:

- ♦ [“GroupWise 18 with Earlier GroupWise Versions” on page 215](#)
- ♦ [“GroupWise 18 in a Cross-Platform Environment” on page 218](#)

For each GroupWise version, the tables indicate compatibility for:

- ♦ **Administrative components:** Domain and post office database platforms and versions, eDirectory platforms, and GroupWise snap-ins to ConsoleOne platforms and versions.
- ♦ **Agents:** Domain and post office database platforms and versions, agent platforms and versions.
- ♦ **Clients:** Post office directory platforms and access, POA platforms and versions, client modes.

In the compatibility tables, cells with combinations that are not applicable are marked N/A. For example, the POA never communicates with the Internet Agent, so that table cell is N/A.

For information about what operating system versions are supported for GroupWise 18 on Linux and Windows, refer to [GroupWise System Requirements](#). For information about earlier versions of GroupWise, refer to:

- ♦ [GroupWise 2014 R2 Installation Guide](#)
- ♦ [GroupWise 2012 Installation Guide](#)
- ♦ [GroupWise 8 Installation Guide](#)

GroupWise 18 with Earlier GroupWise Versions

Select the GroupWise version that you want to determine GroupWise 18 compatibility with:

- ♦ [“Compatibility with GroupWise 2012” on page 215](#)
- ♦ [“Compatibility with GroupWise 8” on page 217](#)

Compatibility with GroupWise 2012

Reference the sections below for information about GroupWise 18 compatibility with GroupWise 2012.

- ♦ [“GroupWise 18 Administrative Components with GroupWise 2012” on page 216](#)
- ♦ [“GroupWise 18 Agents with GroupWise 2012” on page 216](#)
- ♦ [“GroupWise 18 Clients and POAs with GroupWise 2012” on page 216](#)

GroupWise 18 Administrative Components with GroupWise 2012

GroupWise 18 Components	GroupWise 2012 Domain and Post Office Databases	GW 2012 Objects in eDirectory	ConsoleOne + GW 2012 Snap-Ins
GW 18 Domain and Post Office Databases	N/A	N/A	Not Supported
GW 18 Admin Console	Supported	Not Supported	Not Supported

Table Summary: The GroupWise Admin console can be used to access GroupWise 2012 databases for domains and post offices, but GroupWise 2012 ConsoleOne with the GroupWise snap-ins should not be used to access GroupWise 18 databases. The Admin console does not access GroupWise eDirectory objects. You must continue to use ConsoleOne with the GroupWise snap-ins to access GroupWise objects in eDirectory.

GroupWise 18 Agents with GroupWise 2012

GroupWise 18 Agents	GroupWise 2012 Domain and Post Office Databases	GW 2012 POA	GW 2012 MTA	GW 2012 GWIA	GW 2012 DVA	GW 2012 Monitor Agent
GW 18 Domain and Post Office Databases	N/A	Not Supported	Not Supported	Not Supported	N/A	N/A
GW 18 POA	Supported	N/A	Supported	N/A	Supported	Supported
GW 18 MTA	Supported	Supported	Supported	N/A	N/A	Supported
GW 18 GWIA	Supported	N/A	Supported	N/A	N/A	Supported
GW 18 DVA	N/A	Supported	N/A	N/A	N/A	N/A
GW 18 Monitor Agent	N/A	Supported	Supported	Supported	N/A	N/A

Table Summary: GroupWise 2012 agents cannot access domain and post office databases that have been upgraded to GroupWise 18. When a GroupWise 18 MTA or POA accesses an earlier GroupWise database, it has no effect on the database. You must use the Installation console to upgrade domain and post office databases to GroupWise 18.

GroupWise 18 Clients and POAs with GroupWise 2012

	GroupWise 2012 Client	GroupWise 2012 POA
GroupWise 18 Client	N/A	Not Supported
GroupWise 18 POA	Supported	N/A

Table Summary: The GroupWise 2012 client can communicate with the GroupWise 18 POA, but the GroupWise 18 client cannot communicate with the GroupWise 2012 POA. The general rule is that earlier GroupWise clients can always communicate with later POAs, but later GroupWise clients cannot communicate with earlier POAs. GroupWise clients include the Windows client and WebAccess.

Compatibility with GroupWise 8

IMPORTANT: Support for GroupWise 8 has ended. The information below is provided for your convenience. Some of the options listed below may not work as expected. Use at your own risk.

- ♦ [“GroupWise 18 Administrative Components with GroupWise 8” on page 217](#)
- ♦ [“GroupWise 18 Agents with GroupWise 8” on page 218](#)
- ♦ [“GroupWise 18 Client with GroupWise 8” on page 218](#)

GroupWise 18 Administrative Components with GroupWise 8

GroupWise 18 Components	GroupWise 8 Domain and Post Office Databases	GW 8 Objects in eDirectory	ConsoleOne + GW 8 Snap-Ins
GW 18 Domain and Post Office Databases	N/A	N/A	Not Supported
GW 18 Admin Console	Supported	Not Supported	Not Supported

Table Summary: The GroupWise Admin console can be used to access GroupWise 8 databases for domains and post offices, but GroupWise 8 ConsoleOne with the GroupWise snap-ins should not be used to access GroupWise 18 databases. The Admin console does not access GroupWise eDirectory objects. You must continue to use ConsoleOne with the GroupWise snap-ins to access GroupWise objects in eDirectory.

GroupWise 18 Agents with GroupWise 8

GroupWise 18 Agents	GroupWise 8 Domain and Post Office Databases	GW 8 POA	GW 8 MTA	GW 8 GWIA	GW 8 WebAccess Agent	GW 8 Monitor Agent
GW 18 Domain and Post Office Databases	N/A	Not Supported	Not Supported	Not Supported	N/A	N/A
GW 18 POA	Supported	N/A	Supported	N/A	N/A	Supported
GW 18 MTA	Supported	Supported	Supported	Supported	N/A	Supported
GW 18 GWIA	Supported	N/A	Supported	N/A	N/A	Supported
GW 18 DVA	N/A	N/A	N/A	N/A	N/A	N/A
GW 18 Monitor Agent	N/A	Supported	Supported	Supported	N/A	N/A

Table Summary: GroupWise 8 agents cannot access domain and post office databases that have been upgraded to GroupWise 18. When a GroupWise 18 MTA or POA accesses an earlier GroupWise database, it has no effect on the database. You must use the Installation console to upgrade domain and post office databases to GroupWise 18.

The Document Viewer Agent (DVA) was introduced in GroupWise 2012 and so does not interact with any GroupWise 8 agents. The WebAccess Agent that was part of GroupWise 8 was eliminated in GroupWise 2012.

GroupWise 18 Client with GroupWise 8

	GroupWise 8 Client	GroupWise 8 POA
GroupWise 18 Client	N/A	Not Supported
GroupWise 18 POA	Supported	N/A

Table Summary: The GroupWise 8 Windows client can communicate with the GroupWise 18 POA, but the GroupWise 18 client cannot communicate with the GroupWise 8 POA. The general rule is that earlier GroupWise clients can always communicate with later POAs, but later GroupWise clients cannot communicate with earlier POAs. GroupWise clients include the Windows client and WebAccess.

GroupWise 18 in a Cross-Platform Environment

Reference these sections for information running GroupWise in a cross-platform environment.

- ♦ [“GroupWise 18 Administrative Components and Databases” on page 219](#)
- ♦ [“GroupWise 18 Agents on Linux and Windows” on page 219](#)

GroupWise 18 Administrative Components and Databases

Thanks to the web-based nature of the GroupWise Admin console, it does not matter what platform GroupWise databases and agents are on, or where your browser is running, they successfully communicate.

GroupWise 18 Agents on Linux and Windows

GroupWise 18 on Linux Agents	GroupWise 18 Domain or Post Office Databases on Windows	GW 18 POA on Windows	GW 18 MTA on Windows	GW 18 GWIA on Windows	GW 18 DVA on Windows	GW 18 Monitor Agent on Windows
GW 18 Domain and Post Office Databases on Linux	N/A	Not Supported	Not Supported	N/A	N/A	N/A
GW 18 POA on Linux	Not Supported	N/A	Supported	N/A	Supported	Supported
GW 18 MTA on Linux	Not Supported	Supported	Supported	Supported	N/A	Supported
GW 18 GWIA on Linux	N/A	N/A	Supported	N/A	N/A	Supported
GW 18 DVA on Linux	N/A	Supported	N/A	N/A	N/A	N/A
GW 18 Monitor Agent on Linux	N/A	Supported	Supported	Supported	N/A	N/A

Table Summary: Domains and post offices can be located on Linux or Windows. Run the version of the GroupWise agents that matches the platform where the domains and post offices are located. Agents on either platform can communicate with other agents regardless of platform.

B Attributes, Operators, and Values for Object Filters

In general terms, a filter selects data. In any list of objects, you can use a filter in the **Search** field to select and list GroupWise object data based on object attributes and operators.

- ♦ [“Attributes” on page 221](#)
- ♦ [“Logical Operators” on page 222](#)
- ♦ [“Grouping Operators” on page 223](#)
- ♦ [“Wildcard Characters” on page 223](#)
- ♦ [“Literal Values” on page 223](#)
- ♦ [“Date Specifications” on page 224](#)

Attributes

To list the attributes that you can filter on for any object type, press Ctrl-Spacebar in the **Search** field of the object list. Common attributes that you might want to filter on include the following:

Object	Common Attributes
Domain	domainversion lockoutoldadmin minimumadminreleasedate minimumadminreleaseversion
Post Office	clientlockout clientlockoutdate clientlockoutversion disabledlogins intruderdetection postofficeversion
User	allowedaddressformats lastclientlogintime logindisabled mailboxicensetype mailboxsizemb preferredemailid visibility

Object	Common Attributes
POA	clientserverthreads imapenabled maintenancehandlerthreads messagehandlerthreads soapenabled
MTA	defaultroutingdomain loglevel platform synclapservername trackadminmessages

For an exhaustive list of attributes and their possible values, display the following URL on the Admin Service server:

`https://admin_service_address:9710/gwadmin-service/list/object_type/schema`

Replace *admin_service_address* with the IP address or DNS hostname of a server where the Admin Service is installed.

Replace *object_type* with any of the following object types, depending on what you want to list:

- ♦ domain
- ♦ post_office
- ♦ user
- ♦ group
- ♦ resource
- ♦ nickname
- ♦ poa
- ♦ mta
- ♦ gwia
- ♦ library
- ♦ ldap_server

Logical Operators

Spaces around the operators are optional.

Operator	Meaning	Example
=	Equal	lastname = smith
!=	Not equal	visibility != system
>	Greater than	mailboxsizemb > 500

Operator	Meaning	Example
<	Less than	mtpport < 2000
>=	Greater than or equal to	soapthreads >= 10
<=	Less than or equal to	physicalconnections <= 1000

Grouping Operators

Spaces around the operators are optional.

Operator	Meaning	Example
&, and	Conjunction	firstname = john & lastname = smith firstname = john and lastname = smith
, or	Disjunction	lastname = smith lastname = jones lastname = smith or lastname = jones
!, not	Inversion	! (lastname = smith lastname = jones) not (lastname = smith or lastname = jones)
()	Parentheses	lastname = smith & (firstname = john firstname = jill) lastname = smith and (firstname = john or firstname = jill)

Wildcard Characters

The match operator must be used with wildcard characters. The string to match must be surrounded by single quote marks.

Characters	Meaning	Example
*	Zero or more characters	lastname match 'sm*'
?	One character	lastname match 'sm?th'

Literal Values

Spaces around the operators are optional.

Value	Explanation	Example
null	Empty	internetdomainname != null minimumadminreleasedate != null preferredaddressformat != null
true, 1	Enabled or set	logindisabled = true logindisabled = 1

Value	Explanation	Example
false, 0	Disabled or not set	soapenabled = false soapenabled = 0

Date Specifications

You can filter on one specific date or on a range of dates that are relative to today.

Format	Explanation	Example
<i>yyyy-mm-ddTmm:ss</i>	Literal date	18-01-01T00:00
<code>timelastmod > now(<i>time_unit</i>)</code>	Modified now (current time stamp on server)	<code>timelastmod > now()</code>
	Modified in the last day	<code>timelastmod > now(-1)</code>
	Modified in the last 2 weeks	<code>timelastmod > now(-2, weeks)</code>
	Modified in the last three months	<code>timelastmod > now(-3, months)</code>
	Modified in the last year	<code>timelastmod > now(-1, year)</code>

C Invalid Characters in GroupWise Object Names and Email Addresses

Although most characters in the languages supported by GroupWise can be used in GroupWise object names and Internet email addresses, some cannot.

- ♦ [“Invalid Characters in GroupWise Object Names” on page 225](#)
- ♦ [“Invalid Characters in Internet Email Addresses” on page 225](#)

Invalid Characters in GroupWise Object Names

Do not use any of the following invalid characters in GroupWise object names:

- ♦ ASCII characters 0-31
- ♦ Extended ASCII characters that are graphical or typographical symbols
Accented characters in the extended range can be used in GroupWise object names.
- ♦ Asterisk *
- ♦ At sign @
- ♦ Backslash \
- ♦ Braces { }
- ♦ Colon :
- ♦ Comma ,
- ♦ Double quote "
- ♦ Parentheses ()
- ♦ Period .

In addition to the characters listed above, do not use any of the following invalid characters in Agent objects names:

- ♦ Exclamation mark !
- ♦ Semicolon ;
- ♦ Single quote '

Invalid Characters in Internet Email Addresses

Characters that are valid and even desirable in the name of a user, group, or resource might not be valid in an email address. Such invalid characters include spaces and certain accented and special characters. (Providing a definitive list of such invalid characters is beyond the scope of the GroupWise product documentation.)

In the names of users, groups, and resources, use underscores (_) rather than spaces as separators between words in order to facilitate addressing across the Internet.

When an object name includes any character that is not valid in an email address, that object cannot receive messages. For such an object, you must set up a preferred email ID in order to ensure that it has a valid email address.

D Cross-Platform Connections

If you want users to be able to install the GroupWise client software to Windows workstations from a location on a Linux server, you must make the Linux server look like a Windows server from the point of view of the workstations. There are a variety of ways to accomplish this. Samba is one of them.

This section provides examples of how to use Samba to install the GroupWise client software from a Linux server.

- ♦ [“Setting up Samba on OES” on page 227](#)
- ♦ [“Mapping a Drive to a Samba Share on an OES Server” on page 230](#)
- ♦ [“Setting Up Samba on SLES” on page 231](#)
- ♦ [“Mapping a Drive to a Samba Share on a SLES Server” on page 233](#)

Setting up Samba on OES

In order to access the GroupWise client software on a Linux server, you can set up a Samba share to the client folder, either in the downloaded *GroupWise 18* software or in the software distribution folder, if you have created one on the Linux server.

- ♦ [“Configuring NetWare Core Protocol \(NCP\)” on page 227](#)
- ♦ [“Installing Samba” on page 228](#)
- ♦ [“Logging In to iManager” on page 228](#)
- ♦ [“Creating a User to Manage the Samba Share” on page 228](#)
- ♦ [“Configuring the eDirectory Universal Password for Samba” on page 229](#)
- ♦ [“Setting the eDirectory Universal Password for the Samba Administrator User” on page 229](#)
- ♦ [“Creating a Samba Share” on page 229](#)
- ♦ [“Setting the eDirectory Rights for the Samba Share” on page 230](#)
- ♦ [“Testing Samba on the OES Server” on page 230](#)

Configuring NetWare Core Protocol (NCP)

To configure NetWare Core Protocol:

- 1 In a terminal window on the OES server, become `root` by entering `su -` and the `root` password.
- 2 Enter the following command to create the NCP volume:

```
ncpcon create volume volume_name /folder
```

2a Replace *volume_name* with a unique name for the location of the GroupWise client software.

2b Replace *folder* with the full path to the GroupWise client software, for example:

```
/opt/novell/groupwise/software/client
```

3 Verify that the volume has been created:

```
more /etc/opt/novell/ncpserv.conf
```

The new volume should be listed at the end of the NCP server configuration file.

4 Restart the Micro Focus eDirectory daemon:

```
rcnstd restart
```

5 Continue with [Installing Samba](#).

Installing Samba

If you installed Samba when you installed OES, continue with [Logging In to iManager](#).

If you did not install Samba when you installed OES, install it now:

- 1 Start YaST.
- 2 Under **Groups**, click **Open Enterprise Server**, and then click **OES Install and Configuration**.
- 3 Under **OES Services**, select **Micro Focus Samba**, and click **Accept**.
- 4 Follow the prompts to install Micro Focus Samba.
- 5 Continue with [Logging In to iManager](#).

Logging In to iManager

To log in to iManager:

- 1 Access the following URL:

```
https://ip_address/nps/servlet/webacc?taskid=fw Startup
```

Replace *ip_address* with the IP address of the OES server.

- 2 Specify the eDirectory administrator user name, such as `admin.users.novell`, the password for the user name, and the IP address of the eDirectory tree, and then click **Login**.
- 3 Continue with [Creating a User to Manage the Samba Share](#).

Creating a User to Manage the Samba Share

To create a user for managing the Samba share:

- 1 In iManager, click **Users > Create User**.
- 2 In the **Username** field, specify a unique user name for accessing the Samba share from Windows, such as `gwclient`.

- 3 In the **Last name** field, provide a last name (this is a required field).
- 4 In the **Context** field, browse to and click the eDirectory context where you want to create the new User object.
- 5 Type and confirm the password for the new user.

IMPORTANT: Any users who map a drive to the Samba share need to know this user name and password in order to map the drive.

- 6 Click **OK** to create the Samba user for the GroupWise client Samba share.
- 7 Click **Users** to close the **Users** menu.
- 8 Continue with [Configuring the eDirectory Universal Password for Samba](#).

Configuring the eDirectory Universal Password for Samba

To configure the eDirectory universal password for Samba:

- 1 Click **Passwords > Password Policies**.
- 2 Click **Samba Default Password Policy**.
- 3 On the **Policy Assignment** tab, browse to and click the name of the Samba User object that you created in [Creating a User to Manage the Samba Share](#), and then click **OK** to add the user to the list.
- 4 Click **OK** to complete the process.
- 5 Continue with [Setting the eDirectory Universal Password for the Samba Administrator User](#).

Setting the eDirectory Universal Password for the Samba Administrator User

To set the eDirectory universal password for the Samba Administrator user:

- 1 Under **Passwords**, click **Set Universal Password**.
- 2 Browse to and click the name of the Samba User object, and then click **OK**.
- 3 Specify the password for the Samba user, retype the password for confirmation, and click **OK**.
- 4 Click **Passwords** to close the **Passwords** menu.
- 5 Continue with [Creating a Samba Share](#).

Creating a Samba Share

To create a Samba share:

- 1 Click **File Protocols**, and then click **Samba**.
- 2 Browse to and click the name of the Server object where you are setting up the Samba share.
- 3 On the **Shares** tab, create a new Samba share for the `client` folder on the Linux server:
 - 3a Click **New**.
 - 3b Specify a unique name for the Samba share, such as `gwclient`.

3c Specify the full path name to the `client` folder on the Linux server, for example:

`/opt/novell/groupwise/software/client`

3d Select **Read-Only**.

Write access is not required in order to install the GroupWise client software from the Linux server.

3e Click **OK** to add the location to the list of Samba shares, and then click **Close**.

3f Click **File Protocols** to close the **File Protocols** menu.

4 Continue with [Setting the eDirectory Universal Password for the Samba Administrator User](#).


Setting the eDirectory Rights for the Samba Share

To set the eDirectory rights for the Samba share:

- 1 Click **Files and Folders**, and then click **Properties**.
- 2 Browse to and click the name of the Linux partition or folder where you created the new share, and then click **OK**.
- 3 Click **Rights**.
- 4 In the **Add Trustee** field, browse to and click the name of the Samba User object, and then click **OK**.
- 5 Under **Inherited Rights Filter**, select **Read** and click **OK**.
- 6 Continue with [Testing Samba on the OES Server](#).

Testing Samba on the OES Server

To test Samba on the OES server:

- 1 Double-click the Home Directory icon on the Linux desktop.
- 2 Click .
- 3 In the Location field, type `smb://user_name@ip_address`
 - 3a** Replace `user_name` with the user name of the Samba administrator user.
 - 3b** Replace `ip_address` with the IP address of the Linux server.The File Browser should display all Samba shares, including the new one that you created for the GroupWise client software.
- 4 Return to [Step 3](#) in [Installing the GroupWise Client](#).

Mapping a Drive to a Samba Share on an OES Server

To map a drive to a Samba share on an OES server:

- 1 On the Windows server, right-click **N** on the Windows taskbar, and then click **Micro Focus Map Network Drive**.
- 2 Select the drive letter to map to the NCP volume on the OES server.

- 3 Specify the network path to the NCP volume in the following format:

`\\linux_hostname\ncp_volume`

3a Replace *linux_hostname* with the hostname of the OES server.

3b Replace *ncp_volume* with the name of the NCP volume that you just created.

- 4 For the network user name, specify the fully qualified Samba user name for eDirectory, such as `gwclient.users.novell`.

- 5 Click **Map**.

- 6 Click **OK**.

The mapped drive to the OES server opens in Windows Explorer and can now be accessed from Windows.

- 7 Return to [Step 4](#) in [Installing the GroupWise Client](#).

Setting Up Samba on SLES

In order to access the GroupWise client software on a Linux server, you can set up a Samba share on the Linux server to the `client` folder, either in the downloaded *GroupWise 18* software or in the software distribution folder, if you have created one on the Linux server.

- ♦ [“Preparing Your Firewall to Allow Samba Connections” on page 231](#)
- ♦ [“Configuring the Samba Server” on page 231](#)
- ♦ [“Configuring the Samba Web Administration Tool \(SWAT\)” on page 232](#)
- ♦ [“Accessing SWAT” on page 232](#)
- ♦ [“Setting the Samba User Name and Password” on page 232](#)
- ♦ [“Creating a Samba Share” on page 233](#)

Preparing Your Firewall to Allow Samba Connections

To prepare your firewall to allow Samba connections:

- 1 In YaST, click **Firewall**, and then click **Interfaces**.
- 2 Click **Change**, select **Internal Zone**, and then click **OK**.
- 3 Click **Next** to view the summary, and then click **Finish**.
- 4 Continue with [Configuring the Samba Server](#).

Configuring the Samba Server

To configure the Samba server:

- 1 In YaST, click **Network Services > Samba Server**.
- 2 Specify a workgroup or domain name and click **Next**.

For use in your GroupWise system, the Samba server does not need to be part of a workgroup or domain, so it does not matter what you put in this field. For example, you could use `GWCLIENT`.

- 3 Select **Not a Domain Controller**, and then click **Next**.
For use in your GroupWise system, the Samba server does not need to be a domain controller.
- 4 Under **Service Start**, select **During Boot**.
Because you prepared the firewall in [Preparing Your Firewall to Allow Samba Connections](#), the **Firewall Settings** section shows that the firewall port for Samba is already open.
- 5 Click **OK** to finish the basic configuration of the Samba server.
- 6 Continue with [Configuring the Samba Web Administration Tool \(SWAT\)](#).

Configuring the Samba Web Administration Tool (SWAT)

To configure the Samba Web Administration Tool:

- 1 In YaST, click **Network Services** > **Network Services (xinetd)**.
- 2 Select **Enable**.
- 3 In the **Currently Available Services** list, select `swat`, and then click **Toggle Status (On or Off)**.
SWAT is off by default; this turns it on.
- 4 Click **Finish**.
- 5 Continue with [Accessing SWAT](#).

Accessing SWAT

To access SWAT:

- 1 Display SWAT in your web browser with the following URL:
`http://localhost:901`
- 2 Specify the `root` user name and password, and then click **OK**.
- 3 On the SWAT toolbar, click **Status** to verify that `smbd` and `nmbd` are running.
It is not necessary for `winbindd` to be running.
- 4 Continue with [Setting the Samba User Name and Password](#).

Setting the Samba User Name and Password

To set a Samba user name and password:

- 1 On the SWAT toolbar, click **Password**.
- 2 In the **User Name** field, specify a unique user name for use when mapping a drive to the Samba share, such as `gwclient`.
- 3 Type and confirm the password for the new user, and then click **Add User**.

IMPORTANT: Any users who map a drive to the Samba share need to know this user name and password in order to map the drive.

- 4 Continue with [Creating a Samba Share](#).

Creating a Samba Share

To create a Samba share:

- 1 On the SWAT toolbar, click **Shares**.
- 2 In the **Create Share** field, type a unique name for the share, such as `gwclient`, and then click **Create Share**.
- 3 In the **Path** field, specify the full path name to the `client` folder on the Linux server.
- 4 Leave the **Read Only** field set to the default of **Yes**.
Write access is not required in order to install the GroupWise client software from the Linux server.
- 5 In the **Available** field, select **Yes**.
- 6 Click **Commit Changes**.
The Samba share on the Linux server is now ready for access from a Windows workstation.
- 7 Return to [Step 3](#) in [Installing the GroupWise Client](#).

Mapping a Drive to a Samba Share on a SLES Server

To map a drive to the Samba share on an SLES server:

- 1 In Windows Explorer, right-click the Computer object, and then click **Map network drive**.
- 2 In the **Drive** field, select the drive letter for the new Samba share.
- 3 In the **Folder** field, specify the location of the Samba share in the following format:
`\\ip_address\share_name`
 - 3a Replace `ip_address` with the IP address of the Linux server.
 - 3b Replace `share_name` with the name of the new Samba share where the GroupWise client software is available.
- 4 Deselect **Reconnect to logon**.
- 5 Select **Connect using different credentials**.
- 6 Specify the Samba share user name and password, and then click **OK**.
The Samba share for the OES file system opens in Windows Explorer and can now be accessed from Windows.
- 7 Return to [Step 4](#) in [Installing the GroupWise Client](#).

