Quest

Quest® Coexistence Manager™ for GroupWise 1.7.1

FBC Configuration Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Coexistence Manager for GroupWise FBC Configuration Guide
Updated - March 2019
Software Version - 1.7.1

Contents

1

About the Coexistence Manager for GroupWise Documentation

About this *Configuration Guide*

This *FBC Configuration Guide* provides process instructions and application notes for installing and configuring Coexistence Manager for GroupWise's Free/Busy Connector (FBC) in a variety of environmental scenarios—for various combinations of GroupWise and Exchange environments, in both single (shared) and multiple namespace environments. An introductory chapter explains the environmental variables, and concludes with a short worksheet to help you determine your particular FBC scenario. The next 12 chapters then each describe the complete process for installing and configuring the FBC, GroupWise, Exchange and Active Directory for the particular scenario.

Other Coexistence Manager for GroupWise documentation

The documentation for Quest Coexistence Manager for GroupWise (Coexistence Manager for GroupWise) also includes:

- ***Release Notes*** (printable PDF): Describes the current Coexistence Manager for GroupWise release—any new and enhanced features, resolved issues, and known issues. Also documents minimum installation requirements, and provides Quest contact information.
- ***Quick-Start Guide*** (printable PDF): An orientation to the product's basic purposes, features and capabilities, with a case study showing how its primary components are most commonly used within a typical coexistence scenario. Also documents System Requirements, and explains how to download and install the software.
- ***Coexistence Manager for GroupWise User Guide*** (printable PDF): Overview of features, deployment considerations and typical configurations for the Coexistence Manager for GroupWise Directory Connector, Mail Connector and Free/Busy Connector. Also provides process instructions and application notes for installing, configuring, starting and running the Coexistence Manager for GroupWise Directory Connector and Mail Connector, and explains how to configure the GroupWise and Exchange/AD environments to work with these Coexistence Manager for GroupWise components. (The same information for the F/B Connector is deferred to this separate *FBC Configuration Guide*.) The *User Guide* also provides screen-by-screen field notes for Coexistence Manager for GroupWise's Management Console software tools, for all three Coexistence Manager for GroupWise components.
- ***Management Console Online Help*** (three compiled Windows Help files, one for each Coexistence Manager for GroupWise component): Field notes and application notes for the screens and features of Coexistence Manager for GroupWise's Management Console.

All Coexistence Manager for GroupWise documentation is intended for network administrators, consultants, analysts, and any other IT professionals who will install or use the product components, or who may help plan for their use in a coexistence scenario. All of these documents, including the online Help, are bundled and installed with the product, and all except the Help files are also available separately at Quest's Support Portal.

Where To Look in the Coexistence Manager for GroupWise Documentation

The Coexistence Manager for GroupWise *Quick-Start Guide* is intended to introduce you to the product and familiarize you with its capabilities and typical uses. After that, this table shows where you can find particular types of information about particular Coexistence Manager for GroupWise components:

Table 1.

	for Dir Connector & Mail Connector	for Free/Busy Connector
Introduction and orientation:	— — Coexistence Manager for GroupWise Quick-Start Guide and User Guide — —	
Installation instructions:	— — Coexistence Manager for GroupWise Quick-Start Guide — —	
Configuration instructions:	Coexistence Manager for GroupWise User Guide	Coexistence Manager for GroupWise FBC Configuration Guide
Operating instructions:	— — Coexistence Manager for GroupWise User Guide — —	
Troubleshooting info:	Coexistence Manager for GroupWise User Guide	Coexistence Manager for GroupWise FBC Configuration Guide

The Coexistence Manager for GroupWise application Help files contain the same information as the *User Guide*, but make the information available on-screen at the push of a button (from the Coexistence Manager for GroupWise Management Console).

2

Determine your FBC scenario

Coexistence Manager for GroupWise's F/B Connector supports a broad range of scenarios for different GroupWise and Exchange environments, and for both single (shared) namespace and multi-namespace environments. This *FBC Configuration Guide* provides instructions and guidance for configuring Coexistence Manager for GroupWise's FBC, but the instructions are different for different combinations of environments. The first step in configuring the FBC is therefore to determine your FBC scenario, so you can refer to the correct configuration instructions.

The primary variables that determine your FBC scenario are explained in the FBC Configuration Variables topics below. Various combinations of those variables make up 12 basic FBC scenarios. Review these topics as necessary, then see the FBC Configuration Worksheet following to determine your FBC scenario.

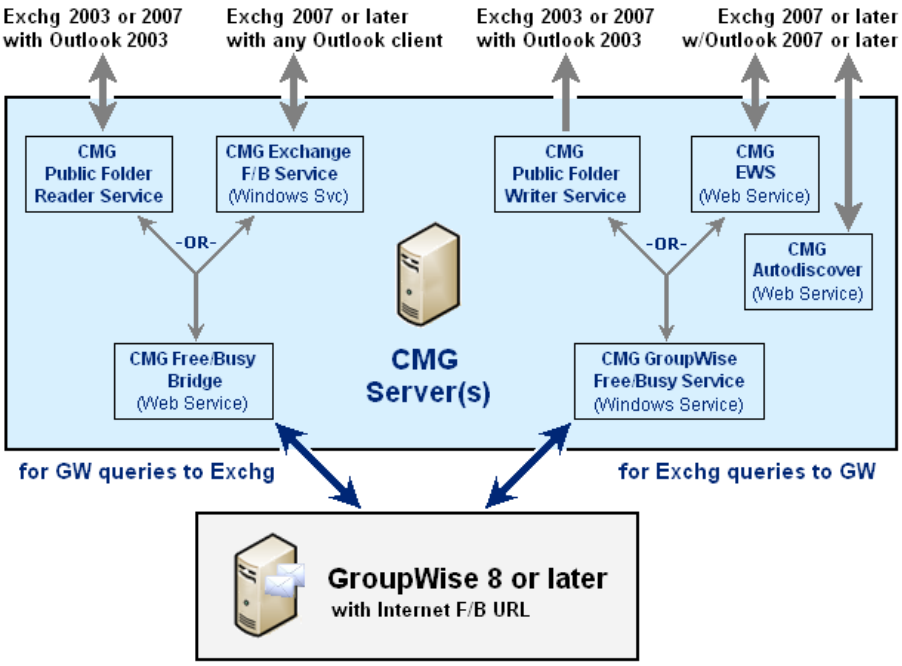
FBC Configuration Variables

These are the primary variables that determine your F/B coexistence scenario:

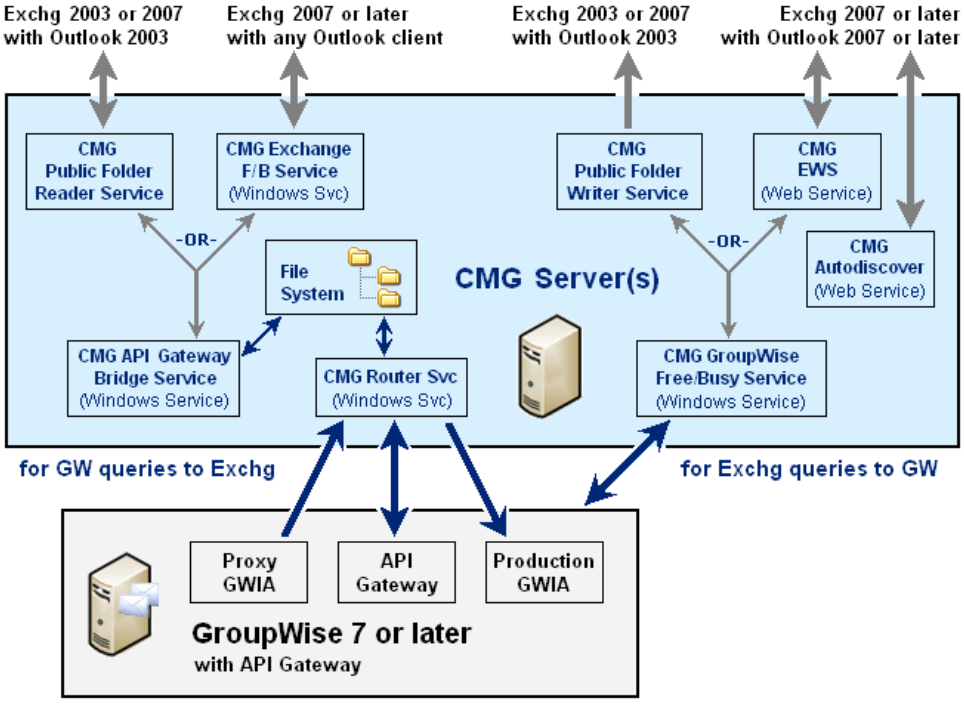
- GroupWise via API vs. via F/B Internet URL
- On-premises Exchange vs. Office 365
- Outlook 2003 clients vs. Outlook 2007 or later (with on-premises Exchange)
- Single (shared) namespace vs. multiple namespaces

GroupWise via API vs. via F/B Internet URL

GroupWise versions 8 and later can communicate with external applications via an Internet URL, as shown here, with the Coexistence Manager for GroupWise components required for configuration with an Internet F/B URL.



GroupWise 7 can communicate with external applications only by an API Gateway, as shown here, also with the Coexistence Manager for GroupWise components necessary for that configuration.



Note that GroupWise versions 8 and later can also be configured with an API Gateway, although configuration with an Internet F/B URL usually delivers better performance.

On-premises Exchange vs. Office 365

Coexistence Manager for GroupWise supports F/B coexistence with an on-premises Exchange, or with a hybrid or non-hybrid Office 365 (“O365”) scenario.

- **Hybrid Office 365:** O365 is synced to an on-premises Exchange, and Coexistence Manager for GroupWise's FBC is configured only between GroupWise and the local on-premises Exchange. Synchronization of the local Exchange to O365 is configured apart from Coexistence Manager for GroupWise, as described in Microsoft's documentation. The configuration of Coexistence Manager for GroupWise's FBC for a hybrid O365 is therefore the same as for a local on-premises Exchange, and we let Microsoft document the instructions for synchronizing the local Exchange with O365.

  IMPORTANT: When configuring for a hybrid O365, remember to configure and test the hybrid connection between your local Exchange and Office 365 *before* configuring Coexistence Manager for GroupWise's FBC.

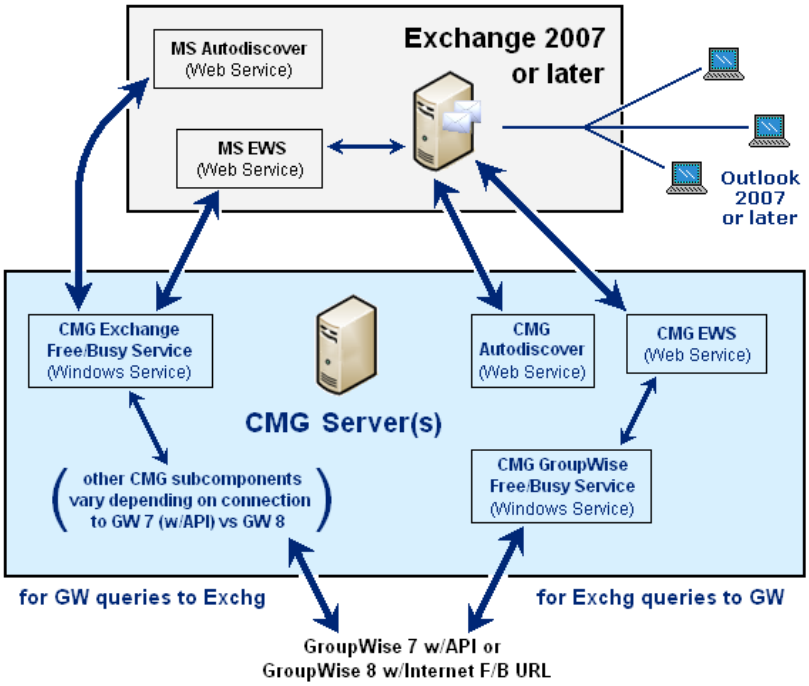
- **Non-hybrid Office 365:** Configuration of Coexistence Manager for GroupWise's FBC for a non-hybrid O365 (where there is no local Exchange) is a qualitatively different scenario, described in chapters 5, 6, 11 and 12 of this *Guide*.

Outlook 2003 clients vs. Outlook 2007 or later (with on-premises Exchange)

Coexistence Manager for GroupWise supports F/B coexistence with Outlook 2007 or later clients connected to Exchange 2007 or later, or with Outlook 2003 clients connected to Exchange 2003 or 2007 (only). These different scenarios require different Coexistence Manager for GroupWise F/B subcomponents, because the implementation of Exchange F/B features changed between Exchange 2003 and Exchange 2007.

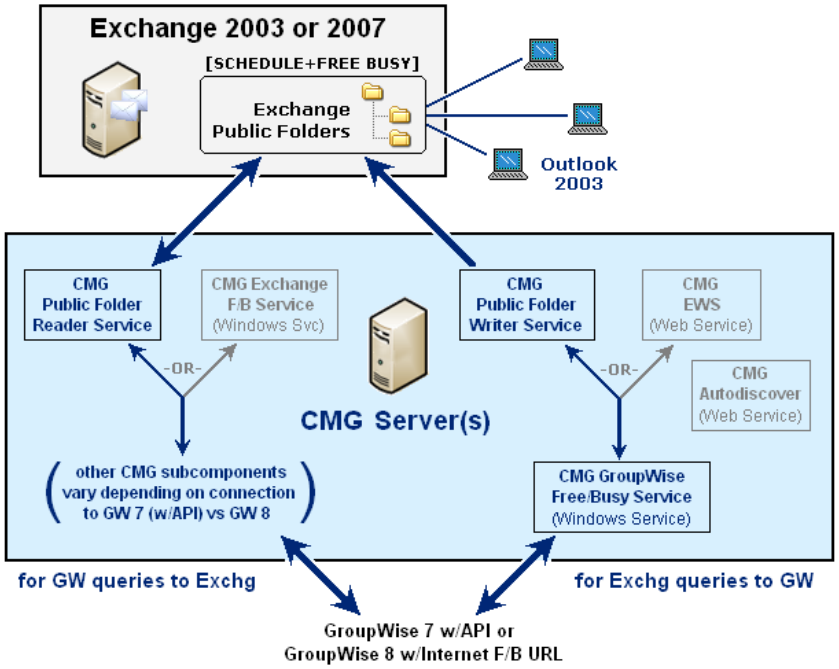
Older versions of Exchange (e.g., Exchange 2000 and 2003) stored free/busy information in system public folders. Beginning with Exchange 2007, F/B information is stored by default in object mailboxes, although Exchange 2007 also lets you store F/B information in public folders, making Exchange 2007 backward-compatible with Outlook 2003 clients.

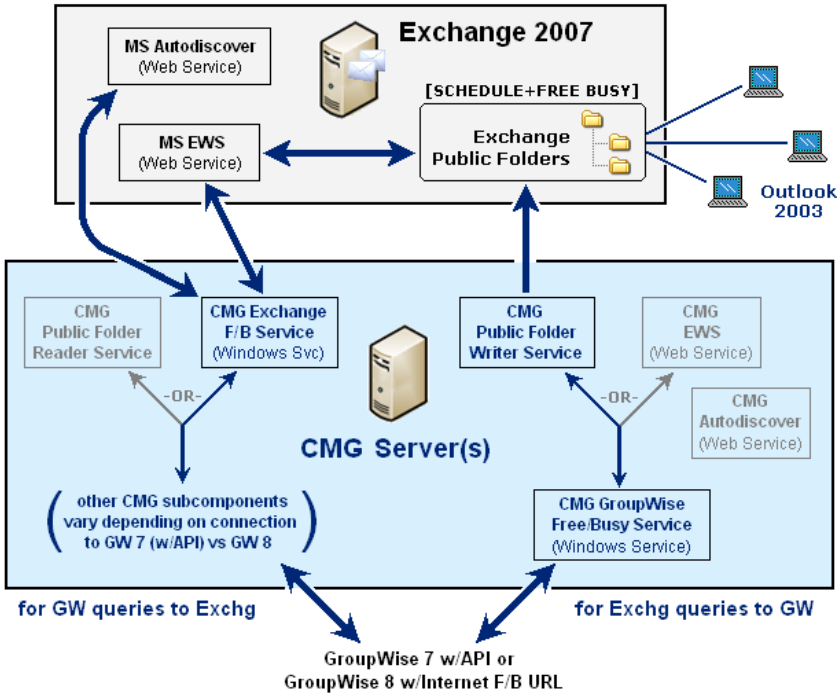
Coexistence Manager for GroupWise's Free/Busy Connector was originally designed to function as a direct, immediate query-and-response system, as shown here for Outlook 2007 and later clients connected to an Exchange 2007 or later server:



In this scenario, Coexistence Manager for GroupWise's FBC facilitates processes where an end-user client in system "A" asks system "B" for the free/busy info for one of its users, and system "B" immediately replies with the requested information. This model, designed for F/B coexistence with Outlook 2007 or later, is also suitable for Microsoft's Office 365. But the same approach does not work for Outlook 2003, which can communicate F/B information with external systems only by relaying it through Exchange public folders.

Coexistence Manager for GroupWise now also supports the public-folders option, by alternate configurations with some different Coexistence Manager for GroupWise subcomponents to facilitate F/B communications with Outlook 2003 clients connected to either Exchange 2003 or Exchange 2007 servers. The illustrations below show these Outlook 2003 configurations. The configuration instructions for scenarios (chapters) 3, 4, 9 and 10 in this *Guide* include more details for using Exchange public folders for F/B coexistence with Outlook 2003 clients.





Implications of F/B coexistence with Outlook 2003 clients

The F/B Connector's public-folders models for Outlook 2003 clients are not direct query-and-response systems when Outlook users seek GroupWise users' F/B info. Exchange public folders instead function like a holding tank that must be repeatedly refreshed with updated data, so at any given moment the public folders data will lag some interval (typically several minutes) behind the true current state of GroupWise F/B data as it exists in the

GroupWise environment. The polling interval is configurable, so the latency period can be minimized by a shorter interval, although an increased polling frequency imposes greater demands on system resources.

The public-folders FBC model does, however, support a direct query-response process in the other direction—when GroupWise users seek Outlook users' F/B info. The Exchange public folders serve as a repository for F/B info for both systems' users, but the information for Outlook users is very nearly current, almost continuously refreshed (internally, by Exchange), whereas the F/B info for GroupWise users must be explicitly obtained and relayed by Coexistence Manager for GroupWise's F/B Connector, at less frequent intervals.

Single (shared) namespace vs. multiple namespaces

Coexistence Manager for GroupWise supports F/B coexistence for either a single (shared) namespace environment (equivalent domain names) or separate (multiple) namespaces. In a single-namespace environment, equivalent domains are mapped to the primary domain in the Exchange server or GroupWise server.

In the FBC Configuration Worksheet table below, the odd-numbered scenarios (chapters) are for single (shared) namespace environments, while the even-numbered scenarios (chapters) are for separate (multiple) namespaces.

FBC Configuration Worksheet

Fill in the blanks in this short worksheet, then check the table below to determine your FBC scenario.

GroupWise environment and connectivity

GroupWise version is _____, and the GroupWise connection to Coexistence Manager for GroupWise will be (pick one):

( ) via API (GW7 or later)

( ) via Internet F/B URL (GW8 or later)

Exchange environment and connectivity

The Exchange side is:

( ) on-premises Exchange version _____, with or without hybrid Office 365 (synced to local Exchange)

... and the local Outlook clients version is:

( ) Outlook 2007 or later, with F/B data flowing via Microsoft Autodiscover and EWS

( ) Outlook 2003, with F/B data flowing via Exchange public folders

( ) non-hybrid Office 365

Single (shared) namespace vs. multiple namespaces

The coexistence environment will be (pick one):

( ) single (shared) namespace

( ) separate (multiple) namespaces

FBC configuration scenarios table

The FBC configuration instructions appear in 12 separate chapters of this *FBC Configuration Guide*, a different chapter for each scenario. The *Chapter* column at the right edge of this table shows which chapter numbers of this *Configuration Guide* provide the configuration instructions for the various scenarios.

IMPORTANT: Only one of these chapters will apply to your particular scenario. Just ignore the other chapters for other scenarios.

Table 2.

GroupWise Environment	Exchange Environment		Single (shared) or Multiple Namespaces?	Chapter
GroupWise via API (GW 7 or later)	On-Premises Exchange (or a hybrid Ofc 365)	Outlook 2007 or later via MS Autodiscover/EWS	Single/shared	1
			Multiple	2
		Outlook 2003 via Exchange Public Folders	Single/shared	3
			Multiple	4
	Office 365 (non-hybrid)		Single/shared	5
			Multiple	6
GroupWise via Internet F/B URL (GW 8 or later)	On-Premises Exchange (or a hybrid Ofc 365)	Outlook 2007 or later via MS Autodiscover/EWS	Single/shared	7
			Multiple	8
		Outlook 2003 via Exchange Public Folders	Single/shared	9
			Multiple	10
	Office 365 (non-hybrid)		Single/shared	11
			Multiple	12

3

FBC Scenario #1

- **GroupWise via API**
- **On-premises Exchange 2007 or later (or hybrid O365)**
- **Outlook 2007 or later**
- **In a single (shared) namespace**

This procedure begins with the assumption that you have already reviewed the introductory chapter of this *FBC Configuration Guide* to Determine your FBC scenario. This chapter explains how to configure the FBC and the coexisting environments for F/B scenario #1, specified above.

Follow these steps, in order as presented here, to install and configure Coexistence Manager for GroupWise's F/B Connector for scenario #1:

- Step 1: Plan your FBC installation and configuration
- Step 2: Configure the GroupWise side
- Step 3: Configure the Exchange side
- Step 4: Configure CMG's FBC Web Server
- Step 5: Configure and test connections among GroupWise, Exchange and CMG's FBC Web Server

Remember that the FBC for a hybrid O365 is configured only between GroupWise and the local on-premises Exchange, while synchronization of the local Exchange to O365 is a connection apart from Coexistence Manager for GroupWise and documented separately by Microsoft. Configuring Coexistence Manager for GroupWise's FBC for a hybrid O365 is therefore the same as configuring for a local on-premises Exchange.

IMPORTANT: For a hybrid Office 365, remember to configure and test the hybrid connection between your local Exchange and O365 (as documented by Microsoft) ***before*** configuring Coexistence Manager for GroupWise's FBC.

Step 1: Plan your FBC installation and configuration

Review the System Requirements (in the Coexistence Manager for GroupWise *Release Notes*), and verify either that your environment conforms to the requirements, or that you will have the necessary hardware and software to meet the requirements.

1.1: Make a configuration map

Scan through the installation and configuration procedures in this chapter, and think through what this process will entail in your own environment, to accommodate your own needs and preferences. Identify any special circumstances or issues, and determine how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers, and how they will connect to the GroupWise and Exchange environments.

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers. If you prefer that all subcomponents reside

on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed below. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit, as described in a later step in this chapter.

The typical deployment of FBC components to two computers for this scenario (GW 7 or later via API Gateway, with Exchange 2007 or later and Outlook 2007 or later) is:

- On Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies):
    - Coexistence Manager for GroupWise Router Service
    - Coexistence Manager for GroupWise API Gateway Bridge Service
    - Coexistence Manager for GroupWise Exchange Free/Busy Service
- On Coexistence Manager for GroupWise Server 2 (for Exchange queries to GroupWise, and GroupWise replies):
    - Coexistence Manager for GroupWise GroupWise Free/Busy Service
    - Coexistence Manager for GroupWise Autodiscover
    - Coexistence Manager for GroupWise EWS

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted just above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

1.2: Complete the Coexistence Manager for GroupWise FBC Planning Worksheet

Use the worksheet in Appendix A of this *FBC Configuration Guide* to gather and organize the information you will need to enter into Coexistence Manager for GroupWise's Management Console application when configuring the Free/Busy Connector. You can print the worksheet to paper, and use a pen or pencil to write the information into the wide right margins.

The actual data-entry work will occur later in this procedure, in step 4.

Step 2: Configure the GroupWise side

Free/busy coexistence with GroupWise 7 requires the GroupWise API Gateway, GroupWise Proxy GWIA, and the GroupWise SOAP web service, as described in the subtopics below.

The API Gateway is also supported (though not recommended) for GroupWise 8 and later. GroupWise 8 admins may choose between the router/postoffice configuration and the original shared-address-book configuration.

NOTE: For F/B coexistence with a mixed GroupWise 7 and 8 environment:

- The GroupWise 8 domain must be the primary domain.
- GroupWise 7 and the API Gateway must be secondary domains.
- GroupWise 7 must be the bridgehead between Coexistence Manager for GroupWise and GroupWise.

A later step of this FBC configuration procedure describes how to configure and test connections among Coexistence Manager for GroupWise FBC components and the GroupWise and Exchange environments.

2.1: Install and configure the GroupWise API Gateway

These components must be installed to support the newer router/postoffice configuration option, required for connection to GroupWise 7. This configuration requires:

- A non-GroupWise domain and non-GroupWise post office.
- A Novell Netware server version 6.0–6.5 running the API Gateway version 4.1v2.

2.2: Enable and configure the GroupWise SOAP web service

FBC coexistence with any supported GroupWise version requires the GroupWise SOAP web service, enabled on the GroupWise Post Office where the Coexistence Manager for GroupWise service account resides. To enable and configure SOAP, see this Novell article, and this one too.

2.3: Create the required proxy GWIA

FBC coexistence with GroupWise version 7 requires a proxy GWIA. In ConsoleOne:

1. Manually create an empty gateway folder called *GWIAFB* (e.g., *..\WPGATE\GWIAFB*).

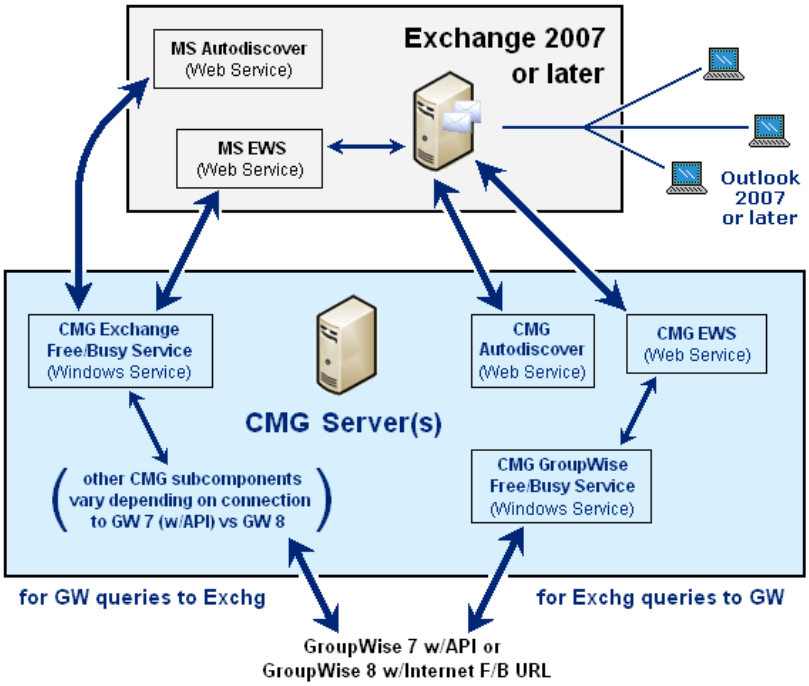
   Copy the entire GWIA folder (the “real” GWIA) to a new proxy GWIA directory, and then delete the *\wpcsout\gwiaXXXX* subfolder (where *XXXX* is the gateway unique ID), and delete the *\wpcsin* subfolder. Do ***not*** start/enable the proxy GWIA, since the FBC must process the files in the proxy GWIA folders.

   > **IMPORTANT:** The proxy GWIA in turn requires:
   >
   > - Account rights with a minimum of *Read*, *Write* and *Delete* rights for all folders in the proxy GWIA. These rights may vary depending on the OS to which the proxy GWIA is installed. For example, the equivalent rights on Netware are *Read*, *Write*, *Create*, *Modify*, *Erase* and *Filescan* [RWCEMF].
   > - A GroupWise mailbox for use with the F/B Connector and associated services.

2. Create a GroupWise Internet Agent called *GWIAFB*, and point it to the *GWIAFB* directory that was just created. (This new GroupWise Internet Agent will need to have a Gateway Type of *Internet Agent*.)
3. Leave the version as 4.x, as this is the only version that is supported by the API Gateway.
4. Change the API agent **Idle Sleep Duration** to 5 seconds.
5. Reconfigure the GW domain to use *GWIAFB* as the default. To do this: Select the Non-GroupWise domain in ConsoleOne and then, on the **Tools** menu: Select **GroupWise System Options** | **Internet Addressing** to open the *Internet Addressing* dialog box. Then select **GWIAFB** from the **Internet Agent for outbound SMTP/MIME messages** drop-down list. Click **OK** to save the changes.

Step 3: Configure the Exchange side

Other than an accommodation for multiple subdomains (see next subtopic below), no additional Exchange configuration is necessary for the FBC to work with an Exchange environment whose Outlook clients are all version 2007 or later, and where Exchange will connect with the FBC by Microsoft’s Autodiscover and EWS (with*out* Exchange public folders). This Exchange-side scenario is illustrated here:



If you are configuring FBC for a hybrid Office 365: Remember that the FBC for a hybrid O365 is configured only between GroupWise and the local on-premises Exchange, while synchronization of the local Exchange to O365 is configured apart from Coexistence Manager for GroupWise (and documented separately by Microsoft). Configuration of Coexistence Manager for GroupWise's FBC for a hybrid O365 is therefore the same as configuring for a local on-premises Exchange—as described here.

To configure the Exchange side for multiple subdomains

Coexistence Manager for GroupWise's Free/Busy Connector can facilitate the flow of free/busy information among multiple subdomains supported by both the Exchange and GroupWise servers. To support this scenario, run the *Add-AvailabilityAddressSpace* cmdlet on the Exchange server or Office 365 for each GroupWise SMTP domain supported.

Step 4: Configure Coexistence Manager for GroupWise's FBC Web Server

To configure Coexistence Manager for GroupWise's FBC Web Server:

- 4.1: Physically install the CMG FBC components
- 4.2: Obtain and install web services certificates
- 4.3: Configure trusted sites for computers hosting F/B components
- 4.4 (optional): Configure logging for F/B components
- 4.5: Configure CMG's FBC for shared/single namespace (equivalent domains)
- 4.6: Run CMG's Management Console to configure FBC components

4.1: Physically install the Coexistence Manager for GroupWise FBC components

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to

warrant separate servers to ensure optimal performance. The installation instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers.

If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed in step 1 above. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit.

See the configuration map you made in step 1 above to determine which components should be installed to which servers for this scenario.

> **IMPORTANT:** ***Before you install,*** on any computer that will host any Coexistence Manager for GroupWise FBC web subcomponent, remove the IIS *DefaultWebSite*: In the navigation tree at left, right-click **DefaultWebSite**, and then select **Remove** from the pop-up menu. Coexistence Manager for GroupWise requires a dedicated server for its own web subcomponents.

Use the AutoRun utility now to install all the necessary Coexistence Manager for GroupWise F/B Connector subcomponents on the computer(s) where you want them installed.

> **IMPORTANT:** ***Remember,*** the Coexistence Manager for GroupWise AutoRun installer must be run on the computer where you want to install a particular subcomponent. If you are deploying the F/B Connector to two different computers, you must run the AutoRun installer twice—once on each computer.

> **NOTE:** The AutoRun installer automatically checks your environment to verify Coexistence Manager for GroupWise prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command string.

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

Remember: For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as listed in step 1 above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

4.2: Obtain and install web services certificates

Coexistence Manager for GroupWise Web Server components must support HTTPS to accept SSL connections. The server on which these components are installed must have a certificate that Exchange trusts. The single certificate must cover the primary domain and all subdomains supported by the GroupWise Server. The certificate covers the Autodiscover and EWS web services.

Coexistence Manager for GroupWise includes an *Autodiscover Certificate Wizard* to automate much of the process of installing this necessary certificate for the Free/Busy Connector. The wizard can be launched from Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*), as described in the procedure documented in the next subtopic below (see Using the Autodiscover Certificate Wizard to Obtain and Install a Certificate). Alternatively you can manually request and install a certificate, as described in the second subtopic below (see To Manually Request and Install a Certificate Using IIS 7.0–8.5).

Using the *Autodiscover Certificate Wizard* to Obtain and Install a Certificate

Even when using the wizard, you will still have to manually request the certificate, and then tell the wizard where the certificate file resides, so the wizard can install it for use with Coexistence Manager for GroupWise.

To use the *Autodiscover Certificate Wizard* to install the necessary web services certificate using IIS 7.0–8.5:

1 In Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*): Click the **Autodiscover Certificate Wizard** button to launch the wizard.

2 Enter the information requested by the wizard until the wizard displays a window of data for you to copy to a certificate request form. Copy (Ctrl+a) the data.

At this point the wizard will remain open, waiting for you to obtain the certificate. You can obtain a certificate from a local certification authority (CA) if you are using an on-premises Exchange server, or from a public CA (like Verisign or Microsoft Active Directory Certificate Services) if you are using Exchange in a hosted environment (e.g., Office 365).

> **NOTE: If you need a multi-domain certificate:** See To Create a SAN Certificate below.

> **NOTE:** You can request a certificate using Web enrollment pages. For more information, see http://support.microsoft.com/kb/931351.

3 Request and obtain the certificate (while the Coexistence Manager for GroupWise wizard waits).

To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate. At some point you will paste into the request form the text you copied from the wizard (in step 2 above).

To request a certificate from a local CA:

a From a web browser, enter ***https://<Local_Certification_Authority_computer>/certsrv***

b Click **Request a certificate**, then click **Advanced certificate request**.

c Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.

d Paste the text you copied from the wizard (in step 2 above) into the certificate request form.

e In the **Certificate Template** box, select **Web Server**.

f Click **Submit**.

g Select **Base 64 Encoded**, then select **Download certificate**.

4 Back in the *Autodiscover Certificate Wizard*: Click **Next**.

5 Specify the path and filename of the certificate file downloaded in step 3 above, and click **Finish** to register the file and dismiss the wizard.

To Manually Request and Install a Certificate Using IIS 7.0–8.5

To manually request a certificate using IIS 7.0–8.5:

1 From Internet Information Services, click **Server Certificates**.

2 From the Actions Pane, select **Create Certificate Request**.

3 Enter **autodiscover.<smtpdomain>** or **<smtpdomain>** for the primary domain and all required subdomains. Then click **Next**.

4 Accept the defaults, and click **Next**.

5 Specify the file name, and click **Finish**.

6 Request a certificate using a local CA or public CA.

To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate.

To request a certificate from a local CA:

a From a web browser, enter **https://<Local_Certification_Authority_computer>/certsrv**

b Click **Request a certificate**, then click **Advanced certificate request**.

c Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.

d Open the text file where you save the certificate request.

e Copy and paste the text from the certificate request into the **Saved Request** box when you selected Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

f In the **Certificate Template** box, select **Web Server**.

g Click **Submit**.

h Select **Base 64 Encoded**, then select **Download certificate**.

To manually install the certificate using IIS 7.0–8.5:

1 From Internet Information Services, click **Server Certificates**.

2 From the Actions Pane, select **Complete Certificate Request**.

3 Select the saved certificate file, and enter a friendly name for the certificate, then click **OK**.

NOTE: To create an https binding for the web site using IIS 7.0–8.5:

1 From the Connection Pane in IIS, select **QuestFreeBusy**.

2 From the Actions Pane, select **Bindings**.

3 Select **Add**. Select **https** as the type for a secure site, and enter the IP address and port number.

4 Select the SSL certificate to pass the certificate into the computer account, and click **View** to view any certificate information.

To Create a SAN Certificate

This procedure lets you configure a single certificate to answer for multiple addresses. This is obviously necessary for a multi-/subdomain configuration, but also, for a single-namespace environment, to create a certificate that will cover both Autodiscover and the root domain.

First, you *must* enable the SAN (Subject Alternate Name) flag on your CA. On the machine running CA services, run these commands at the command prompt to enable the flag:

```
certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
net stop certsvc
net start certsvc
```

When the SAN flag is enabled, you can create the certificate:

1 Open IIS on the machine running F/B and select the server. Scroll to the bottom, open **Server Certificates**, and click on **Create Certificate Request**.

2 For the common name, enter something appropriate for your larger domain. For example, for a domain *alejandro.xyzcorp.com*, the common name on the certificate is **.xyzcorp.com*. (This is somewhat generic, as we will later add specific namespaces to the certificate.)

3 Accept the defaults and enter a name for the request.

4 Open the certificate request you just created, and select and copy ***all*** of the text.

5 Open the certificate web enrollment page for the CA of your domain— e.g., *https://hostname/certsrv*. Then select **Request a Certificate**, and then select **Advanced Certificate Request**.

6 Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.

7 In the **Base-64-encoded certificate request** box, paste all of the text that you copied from the text file in step 4 above.

8 For the **Certificate Template**, select **Web Server**.

9 In the **Additional Attributes** box, enter any alternate-domain information in this format:

san:dns=dns.name[&dns=dns.name]

... with *&dns=dns.name* appended for each alternate domain you want the certificate to handle.

For a single-namespace environment: Enter the autodiscover and root domain, like this:

san:dns=autodiscover.xyzcorp.com&dns=xyzcorp.com

For a multi-/subdomain environment: You can enter as many domains as you like:

san:dns=autodiscover.sub1.xyzcorp.com
&dns=autodiscover.sub2.xyzcorp.com
&dns=autodiscover.sub3.xyzcorp.com
&dns=autodiscover.sub[...].xyzcorp.com
&dns=autodiscover.sub[n].xyzcorp.com

When you are finished, click **Submit**.

10. Select the **DER encoded** radio button, and then select **Download certificate chain**.
11. Enter a name for this.
12. Go back to IIS and click **Complete Certificate Request**.
13. For the **Filename** containing the certification authority's response, click the **Browse** button and select the certificate you just saved. (Be sure to change the file type to *.* instead of *.cer, or you won't see the file you saved—since it is a .P7B extension.) Type a friendly name that is easy to remember and identify so you can find your certificate on the list later. You should then see your new certificate on the list.
14. Select your new certificate and click **View**.
15. Click the **Details** tab, and scroll down to **Subject Alternative Name**. Highlight this field, and you should see all of your domains in the *Details* box.

Now bind your certificate to the HTTPS protocol on the QuestFreeBusy website:

1. On the Coexistence Manager for GroupWise F/B computer, in IIS Manager: Select **QuestFreeBusy**.
2. In the *Actions* pane on the right, select **Bindings**.
3. Select **https** and click **Edit**.
4. In the *Edit Site Binding* window, in the SSL certificate drop-down list: Select the certificate you just created.
5. Click **OK**.

4.3: Configure trusted sites for computers hosting F/B components

Log in as the Coexistence Manager for GroupWise account to be used with the F/B Connector (if you haven't already). Then, in **Internet Options** (via Windows Control Panel or IE **Tools**):

1. Click the *Security* tab, then select **Trusted sites** and click the **Custom level...** button.
2. In **Settings**, scroll down to **User Authentication | Logon**, and click the radio button for *Automatic logon with current user name and password*.
3. Click **OK** to save the selection and return to the *Security* tab.
4. Add the Exchange Server EWS and Autodiscover URLs to the **Trusted Sites**.
5. Click **OK** to save your new **Security** settings and dismiss the **Internet Options** dialog box.

4.4 (optional): Configure logging for F/B components

By default, Coexistence Manager for GroupWise is installed with the *log42net* utility to generate log files of Coexistence Manager for GroupWise components' system activity. This information is critical to diagnosing any problems that may arise. Logging is enabled by default for all Coexistence Manager for GroupWise components.

The default configurations will be suitable for almost all organizations and circumstances, but you can customize logging features if you like. The *log42net* utility may be configured to work a particular way with each Coexistence Manager for GroupWise component. Configuration instructions are nearly identical from one component to another, so we present those details separately, in Appendix C of the Coexistence Manager for GroupWise *User Guide* (not in this *FBC Configuration Guide*).

4.5: Configure Coexistence Manager for GroupWise's FBC for shared/single namespace (equivalent domains)

Coexistence Manager for GroupWise supports equivalent domain names (single, shared namespace) for GroupWise mail users and on-premises Exchange mail users. Equivalent domains are mapped to the primary domain in the Exchange server or GroupWise server. You can use a PowerShell cmdlet to perform this mapping:

- At the Coexistence Manager for GroupWise Web Server, open PowerShell and type:
  Set-CmgGroupWiseFreeBusyConfig -SmtpDomainMappings <*equivalentDomain*>=<*primaryDomain*>

And be sure to repeat the cmdlet for each equivalent domain.

4.6: Run Coexistence Manager for GroupWise's Management Console to configure FBC components

Use Coexistence Manager for GroupWise's Management Console to configure the Free/Busy Connector's components—to identify the participating servers and their locations, register the necessary account access credentials, and set other operating parameters and preferences. See chapter 4 of the Coexistence Manager for GroupWise *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

IMPORTANT: For a hybrid Office 365:

1. Be sure to add the O365 suffix (*yourdomain.onmicrosoft.com*) to the UPN (User Principal Name) suffixes in the Active Directory Domains and Trusts MMC. This lets Coexistence Manager for GroupWise sign-on to both O365 and the on-prem Exchange with the same credentials (assuming the passwords are the same). If the credentials are different, the FBC lookups to O365 will fail.
2. Make sure the O365 suffix is assigned as the coexistence admin's user logon name for the on-prem Active Directory.

NOTE: You may use PowerShell commands to configure Coexistence Manager for GroupWise Free/Busy Connector components, instead of Coexistence Manager for GroupWise's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Appendix B in this *Guide*: Appendix: Configuring and troubleshooting the FBC with PowerShell.

Step 5: Configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server

To configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server:

5.1: Synchronize Exchange and GroupWise directories

Before running any of Coexistence Manager for GroupWise's F/B Connector subcomponents, you must synchronize GroupWise users as Exchange contacts, and Exchange users to GroupWise. For best performance, Quest recommends using the Coexistence Manager for GroupWise Directory Connector. The Directory Connector is another Coexistence Manager for GroupWise component that you may have already installed and configured, or you can install it now. For complete information about the Coexistence Manager for GroupWise Directory Connector, see *User Guide* chapter 2.

If you are configuring the FBC for a local, on-premises Exchange environment (with or without a hybrid O365), use Coexistence Manager for GroupWise's Directory Connector to define a bidirectional update (a pair of single-direction updates, in opposite directions, run sequentially). Most admins schedule the pair to run automatically at regular intervals to keep both directories current throughout the coexistence period. Be sure that at least one bidirectional update has completed before continuing.

Coexistence Manager for GroupWise's Directory Connector does not support directory synchronizations directly between GroupWise and Office 365. In a hybrid O365 scenario, you can facilitate that directory synchronization by this "two-step" approach:

1. Configure the Coexistence Manager for GroupWise Directory Connector for bidirectional updates between GroupWise and the local, proprietary Active Directory, and then
2. Configure Microsoft's AD Sync tool to synchronize the local AD with the hosted (Office 365) AD.

The combination of the two, run in tandem, would configure an effective directory coexistence between GroupWise and Office 365.

Whatever method you choose to synchronize directories, make sure that the GroupWise SOAP web service is enabled (step 2.2 above), since that is also an environmental requirement for Coexistence Manager for GroupWise's Free/Busy Connector.

NOTE: GroupWise sometimes mistakenly generates F/B queries for addresses in the form *user-domain-com@domain.com* (instead of *user@domain.com*). Queries to such addresses will fail if AD does not recognize the address, so be sure to add that address form as an alias in AD for each Exchange user.

5.2: Configure Exchange server connections

Configure and verify the link from the Exchange server to the domains/subdomains supported by the GroupWise server. This procedure tests whether the certificate on the Coexistence Manager for GroupWise Web Server is trusted by the Exchange server.

To configure the Exchange Server link to the Coexistence Manager for GroupWise Web Server and verify that certificates are trusted by Exchange:

1. At the Exchange Server, open Exchange Management Shell and enter the following cmdlet:

   Add-AvailabilityAddressSpace -ForestName <*smtpdomain*> -AccessMethod OrgWideFB

   ... where <*smtpdomain*> is the name of the GroupWise domain.

2. Open a web browser and enter the URL **http://autodiscover.<domain>/autodiscover/autodiscover.xml** to ensure that the Exchange server resolves it to the Coexistence Manager for GroupWise FBC EWS without any certification errors.
3. Ensure the certificate created earlier is trusted by Exchange. If it is not, see 4.2: Obtain and install web services certificates.

4 For a multiple-domain or subdomains environment, repeat the above steps for each domain.

NOTE: If you created a self-signed certificate and a certification error appears in the Web browser:

1. Click the **SSL** button in the Web browser, then click **View Certificates**.
2. Right-click the certificate to open the **Import Certificate Wizard**.
3. Install the certificate in Trusted Root Certification Authorities, and click **Next**.
4. Click **Import**, then **Finish**.

If you requested a certificate from a public CA, the certificate is already trusted by Exchange.

For F/B coexistence with an Exchange 2013 in a single-namespace environment: On all servers running a mailbox role, modify the hostfile to add the IP address and host name of the Coexistence Manager for GroupWise Autodiscover.

To enable shared SMTP namespace F/B lookups in the Exchange-to-GroupWise direction, add the Coexistence Manager for GroupWise F/B Web Services IP address to the host file on the Exchange CAS server.

If Exchange has sites that are handled by Exchange 2003:

- These domains must be added to the 2007/2010/2013 servers' availability address space as *PublicFolders* (not *OrgWideFB*).

5.3: Configure DNS

Configure network load balancing (optional)

You can use Network Load Balancing to permit multiple web servers to handle Autodiscover requests. This is optional, *not* required to deploy Coexistence Manager for GroupWise. For more information, see this Microsoft article.

Configure DNS (Domain Name System)

Configure DNS to point *autodiscover.<smtpdomain.com>* to the computer where Coexistence Manager for GroupWise's Autodiscover service is installed. For each domain, Exchange connects to predefined Autodiscover URLs using DNS host entries.

For Exchange to get free/busy information from the domain supported by a GroupWise server, through the Coexistence Manager for GroupWise Free/Busy Connector, you must make the Coexistence Manager for GroupWise Autodiscover Web Service resolvable to this URL:

https://[autodiscover.]<smtpdomain>/autodiscover/autodiscover.xml

4

FBC Scenario #2

- **GroupWise via API**
- **On-premises Exchange 2007 or later (or hybrid O365)**
- **Outlook 2007 or later**
- **In a multi-namespace environment**

This procedure begins with the assumption that you have already reviewed the introductory chapter of this *FBC Configuration Guide* to Determine your FBC scenario. This chapter explains how to configure the FBC and the coexisting environments for F/B scenario #2, specified above.

Follow these steps, in order as presented here, to install and configure Coexistence Manager for GroupWise's F/B Connector for scenario #2:

- Step 1: Plan your FBC installation and configuration
- Step 2: Configure the GroupWise side
- Step 3: Configure the Exchange side
- Step 4: Configure CMG's FBC Web Server
- Step 5: Configure and test connections among GroupWise, Exchange and CMG's FBC Web Server

Remember that the FBC for a hybrid O365 is configured only between GroupWise and the local on-premises Exchange, while synchronization of the local Exchange to O365 is a connection apart from Coexistence Manager for GroupWise and documented separately by Microsoft. Configuring Coexistence Manager for GroupWise's FBC for a hybrid O365 is therefore the same as configuring for a local on-premises Exchange.

IMPORTANT: For a hybrid Office 365, remember to configure and test the hybrid connection between your local Exchange and O365 (as documented by Microsoft) ***before*** configuring Coexistence Manager for GroupWise's FBC.

Step 1: Plan your FBC installation and configuration

Review the System Requirements (in the Coexistence Manager for GroupWise *Release Notes*), and verify either that your environment conforms to the requirements, or that you will have the necessary hardware and software to meet the requirements.

1.1: Make a configuration map

Scan through the installation and configuration procedures in this chapter, and think through what this process will entail in your own environment, to accommodate your own needs and preferences. Identify any special circumstances or issues, and determine how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers, and how they will connect to the GroupWise and Exchange environments.

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers. If you prefer that all subcomponents reside

on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed below. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit, as described in a later step in this chapter.

The typical deployment of FBC components to two computers for this scenario (GW 7 or later via API Gateway, with Exchange 2007 or later and Outlook 2007 or later) is:

- On Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies):
    - Coexistence Manager for GroupWise Router Service
    - Coexistence Manager for GroupWise API Gateway Bridge Service
    - Coexistence Manager for GroupWise Exchange Free/Busy Service
- On Coexistence Manager for GroupWise Server 2 (for Exchange queries to GroupWise, and GroupWise replies):
    - Coexistence Manager for GroupWise GroupWise Free/Busy Service
    - Coexistence Manager for GroupWise Autodiscover
    - Coexistence Manager for GroupWise EWS

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as listed just above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

1.2: Complete the Coexistence Manager for GroupWise FBC Planning Worksheet

Use the worksheet in Appendix A of this *FBC Configuration Guide* to gather and organize the information you will need to enter into Coexistence Manager for GroupWise's Management Console application when configuring the Free/Busy Connector. You can print the worksheet to paper, and use a pen or pencil to write the information into the wide right margins.

The actual data-entry work will occur later in this procedure, in step 4.

Step 2: Configure the GroupWise side

Free/busy coexistence with GroupWise 7 requires the GroupWise API Gateway, GroupWise Proxy GWIA, and the GroupWise SOAP web service, as described in the subtopics below.

The API Gateway is also supported (though not recommended) for GroupWise 8 and later. GroupWise 8 admins may choose between the router/postoffice configuration and the original shared-address-book configuration.

NOTE: For F/B coexistence with a mixed GroupWise 7 and 8 environment:

- The GroupWise 8 domain must be the primary domain.
- GroupWise 7 and the API Gateway must be secondary domains.
- GroupWise 7 must be the bridgehead between Coexistence Manager for GroupWise and GroupWise.

A later step of this FBC configuration procedure describes how to configure and test connections among Coexistence Manager for GroupWise FBC components and the GroupWise and Exchange environments.

2.1: Install and configure the GroupWise API Gateway

These components must be installed to support the newer router/postoffice configuration option, required for connection to GroupWise 7. This configuration requires:

- A non-GroupWise domain and non-GroupWise post office.
- A Novell Netware server version 6.0–6.5 running the API Gateway version 4.1v2.

2.2: Enable and configure the GroupWise SOAP web service

FBC coexistence with any supported GroupWise version requires the GroupWise SOAP web service, enabled on the GroupWise Post Office where the Coexistence Manager for GroupWise service account resides. To enable and configure SOAP, see this Novell article, and this one too.

2.3: Create the required proxy GWIA

FBC coexistence with GroupWise version 7 requires a proxy GWIA. In ConsoleOne:

1. Manually create an empty gateway folder called *GWIAFB* (e.g., *..\WPGATE\GWIAFB*).

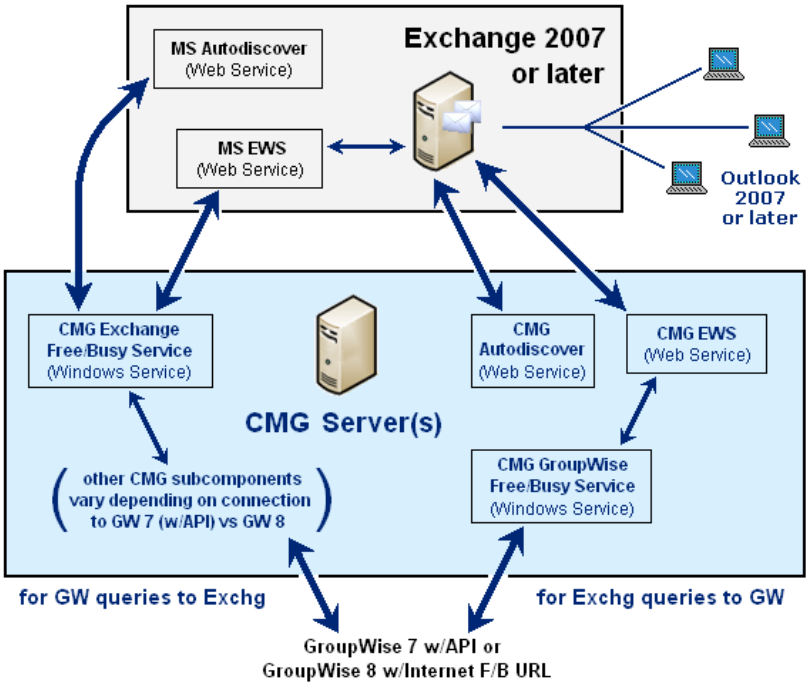
   Copy the entire GWIA folder (the “real” GWIA) to a new proxy GWIA directory, and then delete the *\wpcsout\gwiaXXXX* subfolder (where *XXXX* is the gateway unique ID), and delete the *\wpcsin* subfolder. Do ***not*** start/enable the proxy GWIA, since the FBC must process the files in the proxy GWIA folders.

   > **IMPORTANT:** The proxy GWIA in turn requires:
   >
   > - Account rights with a minimum of *Read*, *Write* and *Delete* rights for all folders in the proxy GWIA. These rights may vary depending on the OS to which the proxy GWIA is installed. For example, the equivalent rights on Netware are *Read*, *Write*, *Create*, *Modify*, *Erase* and *Filescan* [RWCEMF].
   > - A GroupWise mailbox for use with the F/B Connector and associated services.

2. Create a GroupWise Internet Agent called *GWIAFB*, and point it to the *GWIAFB* directory that was just created. (This new GroupWise Internet Agent will need to have a Gateway Type of *Internet Agent*.)
3. Leave the version as 4.x, as this is the only version that is supported by the API Gateway.
4. Change the API agent **Idle Sleep Duration** to 5 seconds.
5. Reconfigure the GW domain to use *GWIAFB* as the default. To do this: Select the Non-GroupWise domain in ConsoleOne and then, on the **Tools** menu: Select **GroupWise System Options** | **Internet Addressing** to open the *Internet Addressing* dialog box. Then select **GWIAFB** from the **Internet Agent for outbound SMTP/MIME messages** drop-down list. Click **OK** to save the changes.

Step 3: Configure the Exchange side

Other than an accommodation for multiple subdomains (see next subtopic below), no additional Exchange configuration is necessary for the FBC to work with an Exchange environment whose Outlook clients are all version 2007 or later, and where Exchange will connect with the FBC by Microsoft’s Autodiscover and EWS (with*out* Exchange public folders). This Exchange-side scenario is illustrated here:



If you are configuring FBC for a hybrid Office 365: Remember that the FBC for a hybrid O365 is configured only between GroupWise and the local on-premises Exchange, while synchronization of the local Exchange to O365 is configured apart from Coexistence Manager for GroupWise (and documented separately by Microsoft). Configuration of Coexistence Manager for GroupWise's FBC for a hybrid O365 is therefore the same as configuring for a local on-premises Exchange—as described here.

To configure the Exchange side for multiple subdomains

Coexistence Manager for GroupWise's Free/Busy Connector can facilitate the flow of free/busy information among multiple subdomains supported by both the Exchange and GroupWise servers. To support this scenario, run the *Add-AvailabilityAddressSpace* cmdlet on the Exchange server or Office 365 for each GroupWise SMTP domain supported.

Step 4: Configure Coexistence Manager for GroupWise's FBC Web Server

To configure Coexistence Manager for GroupWise's FBC Web Server:

- 4.1: Physically install the CMG FBC components
- 4.2: Obtain and install web services certificates
- 4.3: Configure trusted sites for computers hosting F/B components
- 4.4 (optional): Configure logging for F/B components
- 4.5: Run CMG's Management Console to configure FBC components

4.1: Physically install the Coexistence Manager for GroupWise FBC components

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The installation instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers.

If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed in step 1 above. All Coexistence Manager for GroupWise Free/BusyConnector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit.

See the configuration map you made in step 1 above to determine which components should be installed to which servers for this scenario.

> **IMPORTANT:** ***Before you install,*** on any computer that will host any Coexistence Manager for GroupWise FBC web subcomponent, remove the IIS *DefaultWebSite*: In the navigation tree at left, right-click **DefaultWebSite**, and then select **Remove** from the pop-up menu. Coexistence Manager for GroupWise requires a dedicated server for its own web subcomponents.

Use the AutoRun utility now to install all the necessary Coexistence Manager for GroupWise F/B Connector subcomponents on the computer(s) where you want them installed.

> **IMPORTANT:** ***Remember,*** the Coexistence Manager for GroupWise AutoRun installer must be run on the computer where you want to install a particular subcomponent. If you are deploying the F/B Connector to two different computers, you must run the AutoRun installer twice—once on each computer.

> **NOTE:** The AutoRun installer automatically checks your environment to verify Coexistence Manager for GroupWise prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command string.

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

Remember: For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as configured in step 1 above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

4.2: Obtain and install web services certificates

Coexistence Manager for GroupWise Web Server components must support HTTPS to accept SSL connections. The server on which these components are installed must have a certificate that Exchange trusts. The single certificate must cover the primary domain and all subdomains supported by the GroupWise Server. The certificate covers the Autodiscover and EWS web services.

Coexistence Manager for GroupWise includes an *Autodiscover Certificate Wizard* to automate much of the process of installing this necessary certificate for the Free/Busy Connector. The wizard can be launched from Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*), as described in the procedure documented in the next subtopic below (see Using the Autodiscover Certificate Wizard to Obtain and Install a Certificate). Alternatively you can manually request and install a certificate, as described in the second subtopic below (see To Manually Request and Install a Certificate Using IIS 7.0–8.5).

Using the *Autodiscover Certificate Wizard* to Obtain and Install a Certificate

Even when using the wizard, you will still have to manually request the certificate, and then tell the wizard where the certificate file resides, so the wizard can install it for use with Coexistence Manager for GroupWise.

To use the *Autodiscover Certificate Wizard* to install the necessary web services certificate using IIS 7.0–8.5:

1. In Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*): Click the **Autodiscover Certificate Wizard** button to launch the wizard.

2 Enter the information requested by the wizard until the wizard displays a window of data for you to copy to a certificate request form. Copy (Ctrl+a) the data.

   At this point the wizard will remain open, waiting for you to obtain the certificate. You can obtain a certificate from a local certification authority (CA) if you are using an on-premises Exchange server, or from a public CA (like Verisign or Microsoft Active Directory Certificate Services) if you are using Exchange in a hosted environment (e.g., Office 365).

   NOTE: If you need a multi-domain certificate: See To Create a SAN Certificate below.

   NOTE: You can request a certificate using Web enrollment pages. For more information, see http://support.microsoft.com/kb/931351.

3 Request and obtain the certificate (while the Coexistence Manager for GroupWise wizard waits).

   To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate. At some point you will paste into the request form the text you copied from the wizard (in step 2 above).

   To request a certificate from a local CA:

   a From a web browser, enter ***https://<Local_Certification_Authority_computer>/certsrv***

   b Click **Request a certificate**, then click **Advanced certificate request**.

   c Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.

   d Paste the text you copied from the wizard (in step 2 above) into the certificate request form.

   e In the **Certificate Template** box, select **Web Server**.

   f Click **Submit**.

   g Select **Base 64 Encoded**, then select **Download certificate**.

4 Back in the *Autodiscover Certificate Wizard*: Click **Next**.

5 Specify the path and filename of the certificate file downloaded in step 3 above, and click **Finish** to register the file and dismiss the wizard.

To Manually Request and Install a Certificate Using IIS 7.0–8.5

To manually request a certificate using IIS 7.0–8.5:

1 From Internet Information Services, click **Server Certificates**.

2 From the Actions Pane, select **Create Certificate Request**.

3 Enter **autodiscover.<smtpdomain>** or **<smtpdomain>** for the primary domain and all required subdomains. Then click **Next**.

4 Accept the defaults, and click **Next**.

5 Specify the file name, and click **Finish**.

6 Request a certificate using a local CA or public CA.

   To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate.

   To request a certificate from a local CA:

   a From a web browser, enter **https://<Local_Certification_Authority_computer>/certsrv**

   b Click **Request a certificate**, then click **Advanced certificate request**.

   c Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.

   d Open the text file where you save the certificate request.

e Copy and paste the text from the certificate request into the **Saved Request** box when you selected Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

f In the **Certificate Template** box, select **Web Server**.

g Click **Submit**.

h Select **Base 64 Encoded**, then select **Download certificate**.

To manually install the certificate using IIS 7.0–8.5:

1 From Internet Information Services, click **Server Certificates**.

2 From the Actions Pane, select **Complete Certificate Request**.

3 Select the saved certificate file, and enter a friendly name for the certificate, then click **OK**.

NOTE: To create an https binding for the web site using IIS 7.0–8.5:

1 From the Connection Pane in IIS, select **QuestFreeBusy**.

2 From the Actions Pane, select **Bindings**.

3 Select **Add**. Select **https** as the type for a secure site, and enter the IP address and port number.

4 Select the SSL certificate to pass the certificate into the computer account, and click **View** to view any certificate information.

To Create a SAN Certificate

This procedure lets you configure a single certificate to answer for multiple addresses. This is obviously necessary for a multi-/subdomain configuration, but also, for a single-namespace environment, to create a certificate that will cover both Autodiscover and the root domain.

First, you *must* enable the SAN (Subject Alternate Name) flag on your CA. On the machine running CA services, run these commands at the command prompt to enable the flag:

```
certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
net stop certsvc
net start certsvc
```

When the SAN flag is enabled, you can create the certificate:

1 Open IIS on the machine running F/B and select the server. Scroll to the bottom, open **Server Certificates**, and click on **Create Certificate Request**.

2 For the common name, enter something appropriate for your larger domain. For example, for a domain *alejandro.xyzcorp.com*, the common name on the certificate is **.xyzcorp.com*. (This is somewhat generic, as we will later add specific namespaces to the certificate.)

3 Accept the defaults and enter a name for the request.

4 Open the certificate request you just created, and select and copy ***all*** of the text.

5 Open the certificate web enrollment page for the CA of your domain— e.g., *https://hostname/certsrv*. Then select **Request a Certificate**, and then select **Advanced Certificate Request**.

6 Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.

7 In the **Base-64-encoded certificate request** box, paste all of the text that you copied from the text file in step 4 above.

8 For the **Certificate Template**, select **Web Server**.

9 In the **Additional Attributes** box, enter any alternate-domain information in this format:

```
san:dns=dns.name[&dns=dns.name]
```

... with *&dns=dns.name* appended for each alternate domain you want the certificate to handle.

For a single-namespace environment: Enter the autodiscover and root domain, like this:

san:dns=autodiscover.xyzcorp.com&dns=xyzcorp.com

For a multi-/subdomain environment: You can enter as many domains as you like:

san:dns=autodiscover.sub1.xyzcorp.com
&dns=autodiscover.sub2.xyzcorp.com
&dns=autodiscover.sub3.xyzcorp.com
&dns=autodiscover.sub[...].xyzcorp.com
&dns=autodiscover.sub[n].xyzcorp.com

When you are finished, click **Submit**.

10. Select the **DER encoded** radio button, and then select **Download certificate chain**.
11. Enter a name for this.
12. Go back to IIS and click **Complete Certificate Request**.
13. For the **Filename** containing the certification authority's response, click the **Browse** button and select the certificate you just saved. (Be sure to change the file type to *.* instead of *.cer, or you won't see the file you saved—since it is a .P7B extension.) Type a friendly name that is easy to remember and identify so you can find your certificate on the list later. You should then see your new certificate on the list.
14. Select your new certificate and click **View**.
15. Click the **Details** tab, and scroll down to **Subject Alternative Name**. Highlight this field, and you should see all of your domains in the *Details* box.

Now bind your certificate to the HTTPS protocol on the QuestFreeBusy website:

1. On the Coexistence Manager for GroupWise F/B computer, in IIS Manager: Select **QuestFreeBusy**.
2. In the *Actions* pane on the right, select **Bindings**.
3. Select **https** and click **Edit**.
4. In the *Edit Site Binding* window, in the SSL certificate drop-down list: Select the certificate you just created.
5. Click **OK**.

4.3: Configure trusted sites for computers hosting F/B components

Log in as the Coexistence Manager for GroupWise account to be used with the F/B Connector (if you haven't already). Then, in **Internet Options** (via Windows Control Panel or IE **Tools**):

1. Click the *Security* tab, then select **Trusted sites** and click the **Custom level...** button.
2. In **Settings**, scroll down to **User Authentication | Logon**, and click the radio button for *Automatic logon with current user name and password*.
3. Click **OK** to save the selection and return to the *Security* tab.
4. Add the Exchange Server EWS and Autodiscover URLs to the **Trusted Sites**.
5. Click **OK** to save your new **Security** settings and dismiss the **Internet Options** dialog box.

4.4 (optional): Configure logging for F/B components

By default, Coexistence Manager for GroupWise is installed with the *log42net* utility to generate log files of Coexistence Manager for GroupWise components' system activity. This information is critical to diagnosing any problems that may arise. Logging is enabled by default for all Coexistence Manager for GroupWise components.

The default configurations will be suitable for almost all organizations and circumstances, but you can customize logging features if you like. The *log42net* utility may be configured to work a particular way with each Coexistence Manager for GroupWise component. Configuration instructions are nearly identical from one component to another, so we present those details separately, in Appendix C of the Coexistence Manager for GroupWise *User Guide* (not in this *FBC Configuration Guide*).

4.5: Run Coexistence Manager for GroupWise's Management Console to configure FBC components

Use Coexistence Manager for GroupWise's Management Console to configure the Free/Busy Connector's components—to identify the participating servers and their locations, register the necessary account access credentials, and set other operating parameters and preferences. See chapter 4 of the Coexistence Manager for GroupWise *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

IMPORTANT: For a hybrid Office 365:

1. Be sure to add the O365 suffix (*yourdomain.onmicrosoft.com*) to the UPN (User Principal Name) suffixes in the Active Directory Domains and Trusts MMC. This lets Coexistence Manager for GroupWise sign-on to both O365 and the on-prem Exchange with the same credentials (assuming the passwords are the same). If the credentials are different, the FBC lookups to O365 will fail.
2. Make sure the O365 suffix is assigned as the coexistence admin's user logon name for the on-prem Active Directory.

NOTE: You may use PowerShell commands to configure Coexistence Manager for GroupWise Free/Busy Connector components, instead of Coexistence Manager for GroupWise's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Appendix B in this *Guide*: Appendix: Configuring and troubleshooting the FBC with PowerShell.

Step 5: Configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server

To configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server:

5.1: Synchronize Exchange and GroupWise directories

Before running any of Coexistence Manager for GroupWise's F/B Connector subcomponents, you must synchronize GroupWise users as Exchange contacts, and Exchange users to GroupWise. For best performance, Quest recommends using the Coexistence Manager for GroupWise Directory Connector. The Directory Connector is another Coexistence Manager for GroupWise component that you may have already installed and configured, or you can install it now. For complete information about the Coexistence Manager for GroupWise Directory Connector, see *User Guide* chapter 2.

If you are configuring the FBC for a local, on-premises Exchange environment (with or without a hybrid O365), use Coexistence Manager for GroupWise's Directory Connector to define a bidirectional update (a pair of single-direction updates, in opposite directions, run sequentially). Most admins schedule the pair to run automatically at regular intervals to keep both directories current throughout the coexistence period. Be sure that at least one bidirectional update has completed before continuing.

Coexistence Manager for GroupWise's Directory Connector does not support directory synchronizations directly between GroupWise and Office 365. In a hybrid O365 scenario, you can facilitate that directory synchronization by this "two-step" approach:

1. Configure the Coexistence Manager for GroupWise Directory Connector for bidirectional updates between GroupWise and the local, proprietary Active Directory, and then
2. Configure Microsoft's AD Sync tool to synchronize the local AD with the hosted (Office 365) AD.

The combination of the two, run in tandem, would configure an effective directory coexistence between GroupWise and Office 365.

Whatever method you choose to synchronize directories, make sure that the GroupWise SOAP web service is enabled (step 2.2 above), since that is also an environmental requirement for Coexistence Manager for GroupWise's Free/Busy Connector.

> **NOTE:** GroupWise sometimes mistakenly generates F/B queries for addresses in the form *user-domain-com@domain.com* (instead of *user@domain.com*). Queries to such addresses will fail if AD does not recognize the address, so be sure to add that address form as an alias in AD for each Exchange user.

5.2: Configure Exchange server connections

Configure and verify the link from the Exchange server to the domains/subdomains supported by the GroupWise server. This procedure tests whether the certificate on the Coexistence Manager for GroupWise Web Server is trusted by the Exchange server.

To configure the Exchange Server link to the Coexistence Manager for GroupWise Web Server and verify that certificates are trusted by Exchange:

1. At the Exchange Server, open Exchange Management Shell and enter the following cmdlet:

   Add-AvailabilityAddressSpace -ForestName <*smtpdomain*> -AccessMethod OrgWideFB

   ... where <*smtpdomain*> is the name of the GroupWise domain.
2. Open a web browser and enter the URL **http://autodiscover.<domain>/autodiscover/autodiscover.xml** to ensure that the Exchange server resolves it to the Coexistence Manager for GroupWise FBC EWS without any certification errors.
3. Ensure the certificate created earlier is trusted by Exchange. If it is not, see 4.2: Obtain and install web services certificates.
4. For a multiple-domain or subdomains environment, repeat the above steps for each domain.

> **NOTE:** If you created a self-signed certificate and a certification error appears in the Web browser:
>
> 1. Click the **SSL** button in the Web browser, then click **View Certificates**.
> 2. Right-click the certificate to open the **Import Certificate Wizard**.
> 3. Install the certificate in Trusted Root Certification Authorities, and click **Next**.
> 4. Click **Import**, then **Finish**.
>
> If you requested a certificate from a public CA, the certificate is already trusted by Exchange.

For F/B coexistence with an Exchange 2013 in a single-namespace environment: On all servers running a mailbox role, modify the hostfile to add the IP address and host name of the Coexistence Manager for GroupWise Autodiscover.

To enable shared SMTP namespace F/B lookups in the Exchange-to-GroupWise direction, add the Coexistence Manager for GroupWise F/B Web Services IP address to the host file on the Exchange CAS server.

If Exchange has sites that are handled by Exchange 2003:

- These domains must be added to the 2007/2010/2013 servers' availability address space as *PublicFolders* (not *OrgWideFB*).

5.3: Configure DNS

Configure network load balancing (optional)

You can use Network Load Balancing to permit multiple web servers to handle Autodiscover requests. This is optional, *not* required to deploy Coexistence Manager for GroupWise. For more information, see

this Microsoft article.

Configure DNS (Domain Name System)

Configure DNS to point *autodiscover.<smtpdomain.com>* to the computer where Coexistence Manager for GroupWise's Autodiscover service is installed. For each domain, Exchange connects to predefined Autodiscover URLs using DNS host entries.

For Exchange to get free/busy information from the domain supported by a GroupWise server, through the Coexistence Manager for GroupWise Free/Busy Connector, you must make the Coexistence Manager for GroupWise Autodiscover Web Service resolvable to this URL:

https://[autodiscover.]<smtpdomain>/autodiscover/autodiscover.xml

5

FBC Scenario #3

- **GroupWise via API**
- **On-premises Exchange 2007 or 2003**
- **Outlook 2003 (using Exchange public folders)**
- **In a single (shared) namespace**

This procedure begins with the assumption that you have already reviewed the introductory chapter of this *FBC Configuration Guide* to Determine your FBC scenario. This chapter explains how to configure the FBC and the coexisting environments for F/B scenario #3, specified above.

Follow these steps, in order as presented here, to install and configure Coexistence Manager for GroupWise's F/B Connector for scenario #3:

Step 1: Plan your FBC installation and configuration

Review the System Requirements (in the Coexistence Manager for GroupWise *Release Notes*), and verify either that your environment conforms to the requirements, or that you will have the necessary hardware and software to meet the requirements.

1.1: Make a configuration map

Scan through the installation and configuration procedures in this chapter, and think through what this process will entail in your own environment, to accommodate your own needs and preferences. Identify any special circumstances or issues, and determine how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers, and how they will connect to the GroupWise and Exchange environments.

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers. If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed below.

The typical deployment of FBC components to two computers for this scenario (GW 7 or later via API Gateway, and connections to Outlook 2003 via Exchange public folders) depends on how the public folders will connect to the Coexistence Manager for GroupWise components for GroupWise queries to Exchange. With Exchange 2003, that half of the process must be routed through Coexistence Manager for GroupWise's Public Folder Reader Service, and the typical deployment is:

- On Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies):
    - Coexistence Manager for GroupWise Router Service
    - Coexistence Manager for GroupWise API Gateway Bridge Service
    - Coexistence Manager for GroupWise Public Folder Reader Service
- On Coexistence Manager for GroupWise Server 2 (for Exchange queries to GroupWise, and GroupWise replies):
    - Coexistence Manager for GroupWise GroupWise Free/Busy Service
    - Coexistence Manager for GroupWise Public Folder Writer Service

With Exchange 2007, GroupWise queries to Exchange may be routed through Coexistence Manager for GroupWise's Public Folder Reader Service, by the same deployment as shown above, or may instead be routed through Microsoft's Autodiscover and EWS. In the latter case, the typical deployment for Coexistence Manager for GroupWise Server 2 is the same as shown above, but Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies) contains:

- Coexistence Manager for GroupWise Router Service
- Coexistence Manager for GroupWise API Gateway Bridge Service
- Coexistence Manager for GroupWise Exchange Free/Busy Service

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as listed just above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

1.2: Complete the Coexistence Manager for GroupWise FBC Planning Worksheet

Use the worksheet in Appendix A of this *FBC Configuration Guide* to gather and organize the information you will need to enter into Coexistence Manager for GroupWise's Management Console application when configuring the Free/Busy Connector. You can print the worksheet to paper, and use a pen or pencil to write the information into the wide right margins.

The actual data-entry work will occur later in this procedure, in step 4.

Step 2: Configure the GroupWise side

Free/busy coexistence with GroupWise 7 requires the GroupWise API Gateway, GroupWise Proxy GWIA, and the GroupWise SOAP web service, as described in the subtopics below.

The API Gateway is also supported (though not recommended) for GroupWise 8 and later. GroupWise 8 admins may choose between the router/postoffice configuration and the original shared-address-book configuration.

NOTE: For F/B coexistence with a mixed GroupWise 7 and 8 environment:

- The GroupWise 8 domain must be the primary domain.
- GroupWise 7 and the API Gateway must be secondary domains.
- GroupWise 7 must be the bridgehead between Coexistence Manager for GroupWise and GroupWise.

A later step of this FBC configuration procedure describes how to configure and test connections among Coexistence Manager for GroupWise FBC components and the GroupWise and Exchange environments.

2.1: Install and configure the GroupWise API Gateway

These components must be installed to support the newer router/postoffice configuration option, required for connection to GroupWise 7. This configuration requires:

- A non-GroupWise domain and non-GroupWise post office.
- A Novell Netware server version 6.0–6.5 running the API Gateway version 4.1v2.

2.2: Enable and configure the GroupWise SOAP web service

FBC coexistence with any supported GroupWise version requires the GroupWise SOAP web service, enabled on the GroupWise Post Office where the Coexistence Manager for GroupWise service account resides. To enable and configure SOAP, see this Novell article, and this one too.

2.3: Create the required proxy GWIA

FBC coexistence with GroupWise version 7 requires a proxy GWIA. In ConsoleOne:

1. Manually create an empty gateway folder called *GWIAFB* (e.g., *..\WPGATE\GWIAFB*).

   Copy the entire GWIA folder (the “real” GWIA) to a new proxy GWIA directory, and then delete the *\wpcsout\gwiaXXXX* subfolder (where *XXXX* is the gateway unique ID), and delete the *\wpcsin* subfolder. Do ***not*** start/enable the proxy GWIA, since the FBC must process the files in the proxy GWIA folders.

   > **IMPORTANT:** The proxy GWIA in turn requires:
   >
   > - Account rights with a minimum of *Read*, *Write* and *Delete* rights for all folders in the proxy GWIA. These rights may vary depending on the OS to which the proxy GWIA is installed. For example, the equivalent rights on Netware are *Read*, *Write*, *Create*, *Modify*, *Erase* and *Filescan* [RWCEMF].
   > - A GroupWise mailbox for use with the F/B Connector and associated services.

2. Create a GroupWise Internet Agent called *GWIAFB*, and point it to the *GWIAFB* directory that was just created. (This new GroupWise Internet Agent will need to have a Gateway Type of *Internet Agent*.)
3. Leave the version as 4.x, as this is the only version that is supported by the API Gateway.
4. Change the API agent **Idle Sleep Duration** to 5 seconds.
5. Reconfigure the GW domain to use *GWIAFB* as the default. To do this: Select the Non-GroupWise domain in ConsoleOne and then, on the **Tools** menu: Select **GroupWise System Options** | **Internet Addressing** to open the *Internet Addressing* dialog box. Then select **GWIAFB** from the **Internet Agent for outbound SMTP/MIME messages** drop-down list. Click **OK** to save the changes.

Step 3: Configure the Exchange side

Configure domains, permissions and other server parameters and attributes so they will be able to work with Coexistence Manager for GroupWise’s Free/Busy Connector.

To configure the Exchange side for multiple subdomains

Coexistence Manager for GroupWise’s Free/Busy Connector can facilitate the flow of free/busy information among multiple subdomains supported by both the Exchange and GroupWise servers. To support this scenario, run the *Add-AvailabilityAddressSpace* cmdlet on the Exchange server for each GroupWise SMTP domain supported.

Configure Exchange 2003 or 2007 to use Exchange public folders

In these scenarios, Exchange queries for GroupWise F/B data (see the right halves of the Coexistence Manager for GroupWise servers in the diagrams below) are not sent to GroupWise, but rather are routed internally to Exchange's own public folders, which Coexistence Manager for GroupWise regularly refreshes by its Coexistence Manager for GroupWise Public Folder Writer Service. For GroupWise queries to Exchange, however, Coexistence Manager for GroupWise supports two options (described in the next two subtopics below):

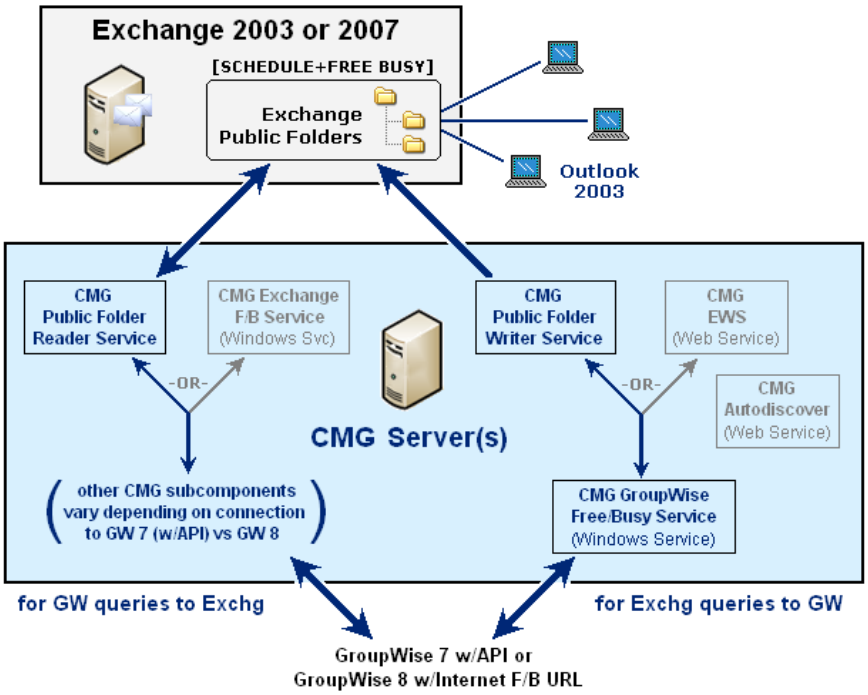
- with Outlook 2003 via Coexistence Manager for GroupWise's Public Folder Reader Service
- with Outlook 2003 and Exchange 2007 (only) via Microsoft's Autodiscover and EWS

FBC with Outlook 2003 via Coexistence Manager for GroupWise's Public Folder Reader Service

For either Exchange 2003 or 2007, GroupWise queries for Exchange F/B data (the left halves of the Coexistence Manager for GroupWise servers in the diagrams below) can pass through Coexistence Manager for GroupWise's Public Folder Reader Service. The Public Folder Reader Service relays GroupWise F/B queries to Exchange public folders, and then relays the F/B info back to GroupWise.

Outlook users' queries for GroupWise F/B info (the right halves of the Coexistence Manager for GroupWise servers in these diagrams) are routed directly to Exchange public folders (internally within the Exchange environment). The public folders reply by transmitting their F/B info directly to the Outlook users. No Coexistence Manager for GroupWise components are used for that query-reply portion of the F/B process. But the Exchange public folders must regularly be refreshed with GroupWise users' current F/B info, and that function is performed by Coexistence Manager for GroupWise's Public Folder Writer Service.

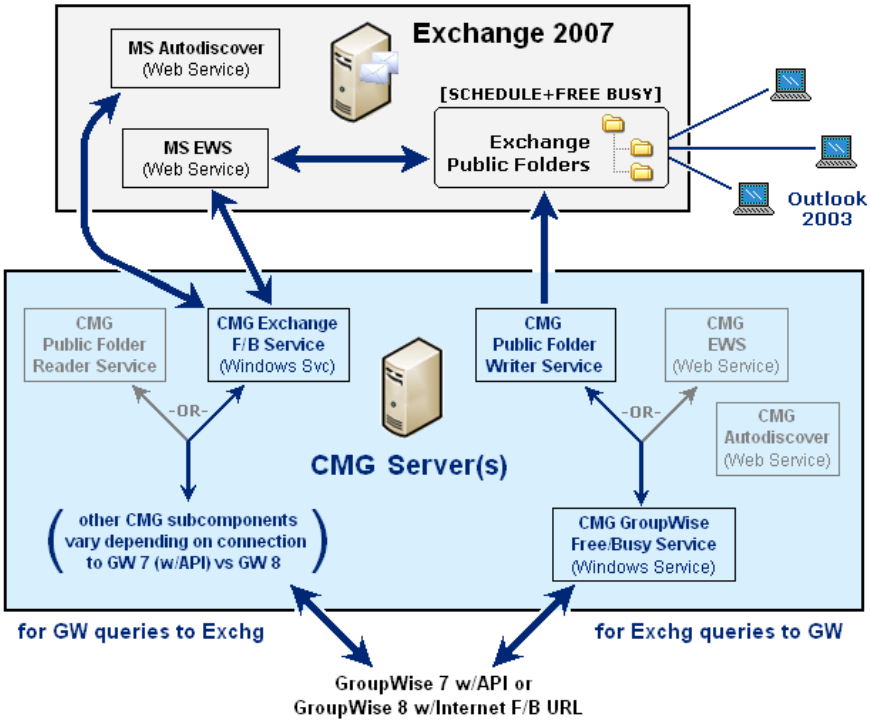
Coexistence Manager for GroupWise's Public Folder Writer Service collects GroupWise users' current F/B info from GroupWise to refresh the Exchange public folders, and also communicates with Active Directory to get and maintain a current list of GroupWise contacts in the Exchange system.



FBC with Outlook 2003 and Exchange 2007 via Microsoft's Autodiscover and EWS

Coexistence Manager for GroupWise can connect to Exchange 2007 public folders either via its Public Folder Reader Service (as described above), or via Microsoft's Autodiscover and EWS, as described here and illustrated in the diagram below. Connecting via the Microsoft services is not an option with Exchange 2003.

This configuration uses Coexistence Manager for GroupWise's Exchange Free/Busy Connector Service to relay GroupWise F/B queries to Microsoft's Autodiscover and EWS on the Exchange server, and relay the F/B info back from MS Autodiscover and EWS to GroupWise. (Microsoft's Autodiscover and EWS in turn relay GroupWise F/B queries to Exchange public folders, and receive the public folders' F/B info.)



Coexistence Manager for GroupWise uses its Public Folder Writer Service to get GroupWise users' current F/B info from GroupWise and, at regular intervals, to refresh the corresponding F/B info held in the Exchange public folders. The Public Folder Writer Service also communicates with Active Directory to get and maintain a current list of GroupWise contacts in the Exchange system. Outlook users' queries for GroupWise F/B info are routed directly to Exchange public folders (internally within the Exchange environment), while the public folders transmit the F/B info directly to the Outlook users.

Step 4: Configure Coexistence Manager for GroupWise's FBC Web Server

To configure Coexistence Manager for GroupWise's FBC Web Server:

- 4.1: Physically install the CMG FBC components
- 4.2: Configure trusted sites for computers hosting F/B components
- 4.3 (optional): Configure logging for F/B components
- 4.4: Configure CMG's FBC for shared/single namespace (equivalent domains)
- 4.5: Run CMG's Management Console to configure FBC components

4.1: Physically install the Coexistence Manager for GroupWise FBC components

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The installation instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers.

If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed in step 1 above. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit.

See the configuration map you made in step 1 above to determine which components should be installed to which servers for this scenario.

IMPORTANT: ***Before you install,*** on any computer that will host any Coexistence Manager for GroupWise FBC web subcomponent, remove the IIS *DefaultWebSite*: In the navigation tree at left, right-click **DefaultWebSite**, and then select **Remove** from the pop-up menu. Coexistence Manager for GroupWise requires a dedicated server for its own web subcomponents.

Use the AutoRun utility now to install all the necessary Coexistence Manager for GroupWise F/B Connector subcomponents on the computer(s) where you want them installed.

IMPORTANT: ***Remember,*** the Coexistence Manager for GroupWise AutoRun installer must be run on the computer where you want to install a particular subcomponent. If you are deploying the F/B Connector to two different computers, you must run the AutoRun installer twice—once on each computer.

NOTE: Coexistence Manager for GroupWise's Public Folder Writer Service and Public Folder Reader Service are available only via the *Custom Setup* option of Coexistence Manager for GroupWise's F/B Connector *Setup* utility.

NOTE: The AutoRun installer automatically checks your environment to verify Coexistence Manager for GroupWise prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command string.

NOTE: ***If you are configuring F/B for Exchange 2003:*** Exchange 2003 does not support Coexistence Manager for GroupWise's F/B Bridge subcomponent or PowerShell. The AutoRun installer installs these subcomponents anyway, because it doesn't know how you intend to configure your F/B services, but the Coexistence Manager for GroupWise F/B Bridge and PowerShell will not be used in your configuration.

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

Remember: For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted in step 1 above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

4.2: Configure trusted sites for computers hosting F/B components

NOTE: This step applies only if you are configuring the FBC to use Microsoft's Autodiscover and EWS for an Exchange 2007 server with Outlook 2003 clients.

Log in as the Coexistence Manager for GroupWise account to be used with the F/B Connector (if you haven't already). Then, in **Internet Options** (via Windows Control Panel or IE **Tools**):

1. Click the *Security* tab, then select **Trusted sites** and click the **Custom level...** button.
2. In **Settings**, scroll down to **User Authentication | Logon**, and click the radio button for *Automatic logon with current user name and password*.
3. Click **OK** to save the selection and return to the *Security* tab.
4. Add the Exchange Server EWS and Autodiscover URLs to the **Trusted Sites**.
5. Click **OK** to save your new **Security** settings and dismiss the **Internet Options** dialog box.

4.3 (optional): Configure logging for F/B components

By default, Coexistence Manager for GroupWise is installed with the *log42net* utility to generate log files of Coexistence Manager for GroupWise components' system activity. This information is critical to diagnosing any problems that may arise. Logging is enabled by default for all Coexistence Manager for GroupWise components.

The default configurations will be suitable for almost all organizations and circumstances, but you can customize logging features if you like. The *log42net* utility may be configured to work a particular way with each Coexistence Manager for GroupWise component. Configuration instructions are nearly identical from one component to another, so we present those details separately, in Appendix C of the Coexistence Manager for GroupWise *User Guide* (not in this *FBC Configuration Guide*).

4.4: Configure Coexistence Manager for GroupWise's FBC for shared/single namespace (equivalent domains)

Coexistence Manager for GroupWise supports equivalent domain names (single, shared namespace) for GroupWise mail users and on-premises Exchange mail users. Equivalent domains are mapped to the primary domain in the Exchange server or GroupWise server. You can use a PowerShell cmdlet to perform this mapping:

- At the Coexistence Manager for GroupWise Web Server, open PowerShell and type:
  Set-CmgGroupWiseFreeBusyConfig -SmtpDomainMappings <*equivalentDomain*>=<*primaryDomain*>

And be sure to repeat the cmdlet for each equivalent domain.

4.5: Run Coexistence Manager for GroupWise's Management Console to configure FBC components

Use Coexistence Manager for GroupWise's Management Console to configure the Free/Busy Connector's components—to identify the participating servers and their locations, register the necessary account access credentials, and set other operating parameters and preferences. See chapter 4 of the Coexistence Manager for GroupWise *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

NOTE: You may use PowerShell commands to configure Coexistence Manager for GroupWise Free/Busy Connector components, instead of Coexistence Manager for GroupWise's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Appendix A in this *Guide*: Appendix: Configuring and troubleshooting the FBC with PowerShell.

Step 5: Configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server

5.1: Configure Coexistence Manager for GroupWise's Directory Connector for the FBC

The public-folders configuration for the FBC requires the corresponding DC connector to be configured, for both the *Provision* and *Update* functions, with an attribute assignment that matches the AD *extensionAttribute* you designate for this purpose. (The attribute and its value are designated in the F/B Connector Management Console, in the *Exchange Public Folder Writer-AD Contacts* screen, as described in the *User Guide*.)

5.2: Synchronize Exchange and GroupWise directories

Before running any of Coexistence Manager for GroupWise's F/B Connector subcomponents, you must synchronize GroupWise users as Exchange contacts, and Exchange users to GroupWise. For best performance, Quest recommends using the Coexistence Manager for GroupWise Directory Connector. The Directory Connector is another Coexistence Manager for GroupWise component that you may have already installed and configured, or you can install it now. For complete information about the Coexistence Manager for GroupWise Directory Connector, see *User Guide* chapter 2.

Use Coexistence Manager for GroupWise's Directory Connector to define a bidirectional update (a pair of single-direction updates, in opposite directions, run sequentially). Most admins schedule the pair to run automatically at regular intervals to keep both directories current throughout the coexistence period. Be sure that at least one bidirectional update has completed before continuing.

Whatever method you choose to synchronize directories, make sure that the GroupWise SOAP web service is enabled (step 2.2 above), since that is also an environmental requirement for Coexistence Manager for GroupWise's Free/Busy Connector.

NOTE: GroupWise sometimes mistakenly generates F/B queries for addresses in the form *user-domain-com@domain.com* (instead of *user@domain.com*). Queries to such addresses will fail if AD does not recognize the address, so be sure to add that address form as an alias in AD for each Exchange user.

6

FBC Scenario #4

- **GroupWise via API**
- **On-premises Exchange 2007 or 2003**
- **Outlook 2003 (using Exchange public folders)**
- **In a multi-namespace environment**

This procedure begins with the assumption that you have already reviewed the introductory chapter of this *FBC Configuration Guide* to Determine your FBC scenario. This chapter explains how to configure the FBC and the coexisting environments for F/B scenario #4, specified above.

Follow these steps, in order as presented here, to install and configure Coexistence Manager for GroupWise's F/B Connector for scenario #4:

Step 1: Plan your FBC installation and configuration

Review the System Requirements (in the Coexistence Manager for GroupWise *Release Notes*), and verify either that your environment conforms to the requirements, or that you will have the necessary hardware and software to meet the requirements.

1.1: Make a configuration map

Scan through the installation and configuration procedures in this chapter, and think through what this process will entail in your own environment, to accommodate your own needs and preferences. Identify any special circumstances or issues, and determine how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers, and how they will connect to the GroupWise and Exchange environments.

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers. If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed below. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit, as described in a later step in this chapter.

The typical deployment of FBC components to two computers for this scenario (GW 7 or later via API Gateway, and connections to Outlook 2003 via Exchange public folders) depends on how the public folders will connect to the Coexistence Manager for GroupWise components for GroupWise queries to Exchange. With Exchange 2003,

that half of the process must be routed through Coexistence Manager for GroupWise's Public Folder Reader Service, and the typical deployment is:

- On Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies):
    - Coexistence Manager for GroupWise Router Service
    - Coexistence Manager for GroupWise API Gateway Bridge Service
    - Coexistence Manager for GroupWise Public Folder Reader Service
- On Coexistence Manager for GroupWise Server 2 (for Exchange queries to GroupWise, and GroupWise replies):
    - Coexistence Manager for GroupWise GroupWise Free/Busy Service
    - Coexistence Manager for GroupWise Public Folder Writer Service

With Exchange 2007, GroupWise queries to Exchange may be routed through Coexistence Manager for GroupWise's Public Folder Reader Service, by the same deployment as shown above, or may instead be routed through Microsoft's Autodiscover and EWS. In the latter case, the typical deployment for Coexistence Manager for GroupWise Server 2 is the same as shown above, but Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies) contains:

- Coexistence Manager for GroupWise Router Service
- Coexistence Manager for GroupWise API Gateway Bridge Service
- Coexistence Manager for GroupWise Exchange Free/Busy Service

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted just above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

1.2: Complete the Coexistence Manager for GroupWise FBC Planning Worksheet

Use the worksheet in Appendix A of this *FBC Configuration Guide* to gather and organize the information you will need to enter into Coexistence Manager for GroupWise's Management Console application when configuring the Free/Busy Connector. You can print the worksheet to paper, and use a pen or pencil to write the information into the wide right margins.

The actual data-entry work will occur later in this procedure, in step 4.

Step 2: Configure the GroupWise side

Free/busy coexistence with GroupWise 7 requires the GroupWise API Gateway, GroupWise Proxy GWIA, and the GroupWise SOAP web service, as described in the subtopics below.

The API Gateway is also supported (though not recommended) for GroupWise 8 and later. GroupWise 8 admins may choose between the router/postoffice configuration and the original shared-address-book configuration.

NOTE: For F/B coexistence with a mixed GroupWise 7 and 8 environment:

- The GroupWise 8 domain must be the primary domain.
- GroupWise 7 and the API Gateway must be secondary domains.
- GroupWise 7 must be the bridgehead between Coexistence Manager for GroupWise and GroupWise.

A later step of this FBC configuration procedure describes how to configure and test connections among Coexistence Manager for GroupWise FBC components and the GroupWise and Exchange environments.

2.1: Install and configure the GroupWise API Gateway

These components must be installed to support the newer router/postoffice configuration option, required for connection to GroupWise 7. This configuration requires:

- A non-GroupWise domain and non-GroupWise post office.
- A Novell Netware server version 6.0–6.5 running the API Gateway version 4.1v2.

2.2: Enable and configure the GroupWise SOAP web service

FBC coexistence with any supported GroupWise version requires the GroupWise SOAP web service, enabled on the GroupWise Post Office where the Coexistence Manager for GroupWise service account resides. To enable and configure SOAP, see this Novell article, and this one too.

2.3: Create the required proxy GWIA

FBC coexistence with GroupWise version 7 requires a proxy GWIA. In ConsoleOne:

1. Manually create an empty gateway folder called *GWIAFB* (e.g., *..\WPGATE\GWIAFB*).

   Copy the entire GWIA folder (the “real” GWIA) to a new proxy GWIA directory, and then delete the *\wpcsout\gwiaXXXX* subfolder (where *XXXX* is the gateway unique ID), and delete the *\wpcsin* subfolder. Do ***not*** start/enable the proxy GWIA, since the FBC must process the files in the proxy GWIA folders.

   > **IMPORTANT:** The proxy GWIA in turn requires:
   > - Account rights with a minimum of *Read*, *Write* and *Delete* rights for all folders in the proxy GWIA. These rights may vary depending on the OS to which the proxy GWIA is installed. For example, the equivalent rights on Netware are *Read*, *Write*, *Create*, *Modify*, *Erase* and *Filescan* [RWCEMF].
   > - A GroupWise mailbox for use with the F/B Connector and associated services.

2. Create a GroupWise Internet Agent called *GWIAFB*, and point it to the *GWIAFB* directory that was just created. (This new GroupWise Internet Agent will need to have a Gateway Type of *Internet Agent*.)
3. Leave the version as 4.x, as this is the only version that is supported by the API Gateway.
4. Change the API agent **Idle Sleep Duration** to 5 seconds.
5. Reconfigure the GW domain to use *GWIAFB* as the default. To do this: Select the Non-GroupWise domain in ConsoleOne and then, on the **Tools** menu: Select **GroupWise System Options** | **Internet Addressing** to open the *Internet Addressing* dialog box. Then select **GWIAFB** from the **Internet Agent for outbound SMTP/MIME messages** drop-down list. Click **OK** to save the changes.

Step 3: Configure the Exchange side

Configure domains, permissions and other server parameters and attributes so they will be able to work with Coexistence Manager for GroupWise’s Free/Busy Connector.

To configure the Exchange side for multiple subdomains

Coexistence Manager for GroupWise’s Free/Busy Connector can facilitate the flow of free/busy information among multiple subdomains supported by both the Exchange and GroupWise servers. To support this scenario, run the *Add-AvailabilityAddressSpace* cmdlet on the Exchange server for each GroupWise SMTP domain supported.

Configure Exchange 2003 or 2007 to use Exchange public folders

In these scenarios, Exchange queries for GroupWise F/B data (see the right halves of the Coexistence Manager for GroupWise servers in the diagrams below) are not sent to GroupWise, but rather are routed internally to Exchange's own public folders, which Coexistence Manager for GroupWise regularly refreshes by its Coexistence Manager for GroupWise Public Folder Writer Service. For GroupWise queries to Exchange, however, Coexistence Manager for GroupWise supports two options (described in the next two subtopics below):

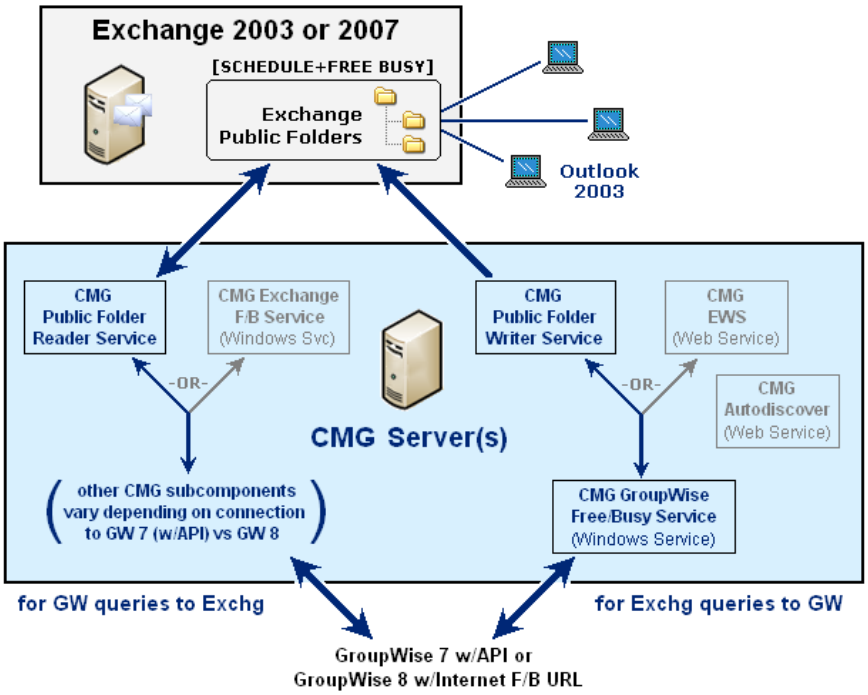
- with Outlook 2003 via Coexistence Manager for GroupWise's Public Folder Reader Service
- with Outlook 2003 and Exchange 2007 (only) via Microsoft's Autodiscover and EWS

FBC with Outlook 2003 via Coexistence Manager for GroupWise's Public Folder Reader Service

For either Exchange 2003 or 2007, GroupWise queries for Exchange F/B data (the left halves of the Coexistence Manager for GroupWise servers in the diagrams below) can pass through Coexistence Manager for GroupWise's Public Folder Reader Service. The Public Folder Reader Service relays GroupWise F/B queries to Exchange public folders, and then relays the F/B info back to GroupWise.

Outlook users' queries for GroupWise F/B info (the right halves of the Coexistence Manager for GroupWise servers in these diagrams) are routed directly to Exchange public folders (internally within the Exchange environment). The public folders reply by transmitting their F/B info directly to the Outlook users. No Coexistence Manager for GroupWise components are used for that query-reply portion of the F/B process. But the Exchange public folders must regularly be refreshed with GroupWise users' current F/B info, and that function is performed by Coexistence Manager for GroupWise's Public Folder Writer Service.

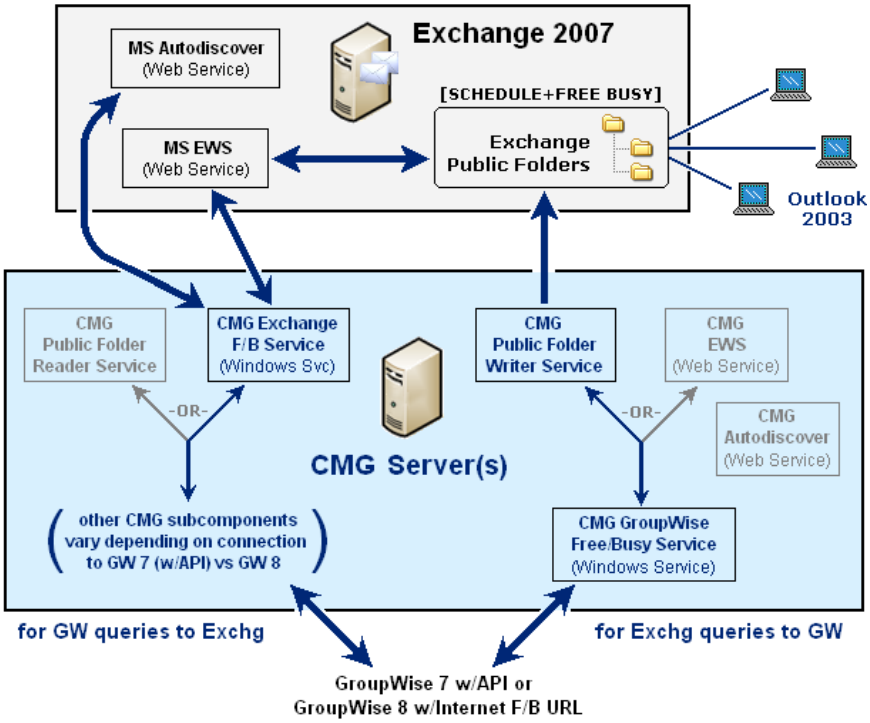
Coexistence Manager for GroupWise's Public Folder Writer Service collects GroupWise users' current F/B info from GroupWise to refresh the Exchange public folders, and also communicates with Active Directory to get and maintain a current list of GroupWise contacts in the Exchange system.



FBC with Outlook 2003 and Exchange 2007 via Microsoft's Autodiscover and EWS

Coexistence Manager for GroupWise can connect to Exchange 2007 public folders either via its Public Folder Reader Service (as described above), or via Microsoft's Autodiscover and EWS, as described here and illustrated in the diagram below. Connecting via the Microsoft services is not an option with Exchange 2003.

This configuration uses Coexistence Manager for GroupWise's Exchange Free/Busy Connector Service to relay GroupWise F/B queries to Microsoft's Autodiscover and EWS on the Exchange server, and relay the F/B info back from MS Autodiscover and EWS to GroupWise. (Microsoft's Autodiscover and EWS in turn relay GroupWise F/B queries to Exchange public folders, and receive the public folders' F/B info.)



Coexistence Manager for GroupWise uses its Public Folder Writer Service to get GroupWise users' current F/B info from GroupWise and, at regular intervals, to refresh the corresponding F/B info held in the Exchange public folders. The Public Folder Writer Service also communicates with Active Directory to get and maintain a current list of GroupWise contacts in the Exchange system. Outlook users' queries for GroupWise F/B info are routed directly to Exchange public folders (internally within the Exchange environment), while the public folders transmit the F/B info directly to the Outlook users.

Step 4: Configure Coexistence Manager for GroupWise's FBC Web Server

To configure Coexistence Manager for GroupWise's FBC Web Server:

- 4.1: Physically install the CMG FBC components
- 4.2: Configure trusted sites for computers hosting F/B components
- 4.3 (optional): Configure logging for F/B components
- 4.4: Run CMG's Management Console to configure FBC components

4.1: Physically install the Coexistence Manager for GroupWise FBC components

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The installation instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers.

If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed in step 1 above. All Coexistence Manager for GroupWise Free/BusyConnector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit.

See the configuration map you made in step 1 above to determine which components should be installed to which servers for this scenario.

IMPORTANT: ***Before you install,*** on any computer that will host any Coexistence Manager for GroupWise FBC web subcomponent, remove the IIS *DefaultWebSite*: In the navigation tree at left, right-click **DefaultWebSite**, and then select **Remove** from the pop-up menu. Coexistence Manager for GroupWise requires a dedicated server for its own web subcomponents.

Use the AutoRun utility now to install all the necessary Coexistence Manager for GroupWise F/B Connector subcomponents on the computer(s) where you want them installed.

IMPORTANT: ***Remember,*** the Coexistence Manager for GroupWise AutoRun installer must be run on the computer where you want to install a particular subcomponent. If you are deploying the F/B Connector to two different computers, you must run the AutoRun installer twice—once on each computer.

NOTE: Coexistence Manager for GroupWise's Public Folder Writer Service and Public Folder Reader Service are available only via the *Custom Setup* option of Coexistence Manager for GroupWise's F/B Connector *Setup* utility.

NOTE: The AutoRun installer automatically checks your environment to verify Coexistence Manager for GroupWise prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command string.

NOTE: ***If you are configuring F/B for Exchange 2003:*** Exchange 2003 does not support Coexistence Manager for GroupWise's F/B Bridge subcomponent or PowerShell. The AutoRun installer installs these subcomponents anyway, because it doesn't know how you intend to configure your F/B services, but the Coexistence Manager for GroupWise F/B Bridge and PowerShell will not be used in your configuration.

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

Remember: For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted in step 1 above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

4.2: Configure trusted sites for computers hosting F/B components

NOTE: This step applies only if you are configuring the FBC to use Microsoft's Autodiscover and EWS for an Exchange 2007 server with Outlook 2003 clients.

Log in as the Coexistence Manager for GroupWise account to be used with the F/B Connector (if you haven't already). Then, in **Internet Options** (via Windows Control Panel or IE **Tools**):

1. Click the *Security* tab, then select **Trusted sites** and click the **Custom level...** button.
2. In **Settings**, scroll down to **User Authentication | Logon**, and click the radio button for *Automatic logon with current user name and password*.
3. Click **OK** to save the selection and return to the *Security* tab.
4. Add the Exchange Server EWS and Autodiscover URLs to the **Trusted Sites**.
5. Click **OK** to save your new **Security** settings and dismiss the **Internet Options** dialog box.

4.3 (optional): Configure logging for F/B components

By default, Coexistence Manager for GroupWise is installed with the *log42net* utility to generate log files of Coexistence Manager for GroupWise components' system activity. This information is critical to diagnosing any problems that may arise. Logging is enabled by default for all Coexistence Manager for GroupWise components.

The default configurations will be suitable for almost all organizations and circumstances, but you can customize logging features if you like. The *log42net* utility may be configured to work a particular way with each Coexistence Manager for GroupWise component. Configuration instructions are nearly identical from one component to another, so we present those details separately, in Appendix C of the Coexistence Manager for GroupWise *User Guide* (not in this *FBC Configuration Guide*).

4.4: Run Coexistence Manager for GroupWise's Management Console to configure FBC components

Use Coexistence Manager for GroupWise's Management Console to configure the Free/Busy Connector's components—to identify the participating servers and their locations, register the necessary account access credentials, and set other operating parameters and preferences. See chapter 4 of the Coexistence Manager for GroupWise *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

NOTE: You may use PowerShell commands to configure Coexistence Manager for GroupWise Free/Busy Connector components, instead of Coexistence Manager for GroupWise's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Appendix A in this *Guide*: Appendix: Configuring and troubleshooting the FBC with PowerShell.

Step 5: Configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server

5.1: Configure Coexistence Manager for GroupWise's Directory Connector for the FBC

The public-folders configuration for the FBC requires the corresponding DC connector to be configured, for both the *Provision* and *Update* functions, with an attribute assignment that matches the AD *extensionAttribute* you designate for this purpose. (The attribute and its value are designated in the F/B Connector Management Console, in the *Exchange Public Folder Writer-AD Contacts* screen, as described in the *User Guide*.)

5.2: Synchronize Exchange and GroupWise directories

Before running any of Coexistence Manager for GroupWise's F/B Connector subcomponents, you must synchronize GroupWise users as Exchange contacts, and Exchange users to GroupWise. For best performance, Quest recommends using the Coexistence Manager for GroupWise Directory Connector. The Directory Connector is another Coexistence Manager for GroupWise component that you may have already installed and configured, or you can install it now. For complete information about the Coexistence Manager for GroupWise Directory Connector, see *User Guide* chapter 2.

Use Coexistence Manager for GroupWise's Directory Connector to define a bidirectional update (a pair of single-direction updates, in opposite directions, run sequentially). Most admins schedule the pair to run automatically at regular intervals to keep both directories current throughout the coexistence period. Be sure that at least one bidirectional update has completed before continuing.

Whatever method you choose to synchronize directories, make sure that the GroupWise SOAP web service is enabled (step 2.2 above), since that is also an environmental requirement for Coexistence Manager for GroupWise's Free/Busy Connector.

NOTE: GroupWise sometimes mistakenly generates F/B queries for addresses in the form *user-domain-com@domain.com* (instead of *user@domain.com*). Queries to such addresses will fail if AD does not recognize the address, so be sure to add that address form as an alias in AD for each Exchange user.

7

FBC Scenario #5

• GroupWise via API
• Office 365 (non-hybrid)
• In a single (shared) namespace

This procedure begins with the assumption that you have already reviewed the introductory chapter of this *FBC Configuration Guide* to Determine your FBC scenario. This chapter explains how to configure the FBC and the coexisting environments for F/B scenario #5, specified above.

Follow these steps, in order as presented here, to install and configure Coexistence Manager for GroupWise's F/B Connector for scenario #5:

Step 1: Plan your FBC installation and configuration

Review the System Requirements (in the Coexistence Manager for GroupWise *Release Notes*), and verify either that your environment conforms to the requirements, or that you will have the necessary hardware and software to meet the requirements.

1.1: Make a configuration map

Scan through the installation and configuration procedures in this chapter, and think through what this process will entail in your own environment, to accommodate your own needs and preferences. Identify any special circumstances or issues, and determine how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers, and how they will connect to the GroupWise and Exchange environments.

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers. If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed below. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit, as described in a later step in this chapter.

The typical deployment of FBC components to two computers for this scenario (GW 7 or later via API Gateway, with non-hybrid Office 365) is:

- On Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies):

    - Coexistence Manager for GroupWise Router Service
    - Coexistence Manager for GroupWise API Gateway Bridge Service
    - Coexistence Manager for GroupWise Exchange Free/Busy Service
- On Coexistence Manager for GroupWise Server 2 (for Exchange queries to GroupWise, and GroupWise replies):
    - Coexistence Manager for GroupWise GroupWise Free/Busy Service
    - Coexistence Manager for GroupWise Autodiscover
    - Coexistence Manager for GroupWise EWS

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted just above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

1.2: Complete the Coexistence Manager for GroupWise FBC Planning Worksheet

Use the worksheet in Appendix A of this *FBC Configuration Guide* to gather and organize the information you will need to enter into Coexistence Manager for GroupWise's Management Console application when configuring the Free/Busy Connector. You can print the worksheet to paper, and use a pen or pencil to write the information into the wide right margins.

The actual data-entry work will occur later in this procedure, in step 4.

Step 2: Configure the GroupWise side

Free/busy coexistence with GroupWise 7 requires the GroupWise API Gateway, GroupWise Proxy GWIA, and the GroupWise SOAP web service, as described in the subtopics below.

The API Gateway is also supported (though not recommended) for GroupWise 8 and later. GroupWise 8 admins may choose between the router/postoffice configuration and the original shared-address-book configuration.

NOTE: For F/B coexistence with a mixed GroupWise 7 and 8 environment:

- The GroupWise 8 domain must be the primary domain.
- GroupWise 7 and the API Gateway must be secondary domains.
- GroupWise 7 must be the bridgehead between Coexistence Manager for GroupWise and GroupWise.

A later step of this FBC configuration procedure describes how to configure and test connections among Coexistence Manager for GroupWise FBC components and the GroupWise and Exchange environments.

2.1: Install and configure the GroupWise API Gateway

These components must be installed to support the newer router/postoffice configuration option, required for connection to GroupWise 7. This configuration requires:

- A non-GroupWise domain and non-GroupWise post office.
- A Novell Netware server version 6.0–6.5 running the API Gateway version 4.1v2.

2.2: Enable and configure the GroupWise SOAP web service

FBC coexistence with any supported GroupWise version requires the GroupWise SOAP web service, enabled on the GroupWise Post Office where the Coexistence Manager for GroupWise service account resides. To enable and configure SOAP, see this Novell article, and this one too.

2.3: Create the required proxy GWIA

FBC coexistence with GroupWise version 7 requires a proxy GWIA. In ConsoleOne:

1. Manually create an empty gateway folder called *GWIAFB* (e.g., ..*WPGATE**GWIAFB*).

   Copy the entire GWIA folder (the “real” GWIA) to a new proxy GWIA directory, and then delete the *wpcsout**gwiaXXXX* subfolder (where *XXXX* is the gateway unique ID), and delete the *wpcsin* subfolder. Do ***not*** start/enable the proxy GWIA, since the FBC must process the files in the proxy GWIA folders.

   > **IMPORTANT:** The proxy GWIA in turn requires:
   >
   > - Account rights with a minimum of *Read*, *Write* and *Delete* rights for all folders in the proxy GWIA. These rights may vary depending on the OS to which the proxy GWIA is installed. For example, the equivalent rights on Netware are *Read*, *Write*, *Create*, *Modify*, *Erase* and *Filescan* [RWCEMF].
   > - A GroupWise mailbox for use with the F/B Connector and associated services.

2. Create a GroupWise Internet Agent called *GWIAFB*, and point it to the *GWIAFB* directory that was just created. (This new GroupWise Internet Agent will need to have a Gateway Type of *Internet Agent*.)
3. Leave the version as 4.x, as this is the only version that is supported by the API Gateway.
4. Change the API agent **Idle Sleep Duration** to 5 seconds.
5. Reconfigure the GW domain to use *GWIAFB* as the default. To do this: Select the Non-GroupWise domain in ConsoleOne and then, on the **Tools** menu: Select **GroupWise System Options** | **Internet Addressing** to open the *Internet Addressing* dialog box. Then select **GWIAFB** from the **Internet Agent for outbound SMTP/MIME messages** drop-down list. Click **OK** to save the changes.

Step 3: Configure the Office 365 side

To configure a non-hybrid Office 365 for Coexistence Manager for GroupWise’s F/B Connector in a single/shared namespace environment:

1. In O365, configure an outbound send connector to point to Coexistence Manager for GroupWise’s Mail Connector, to facilitate mail flow apart from free/busy.
2. Configure an Autodiscover website for Coexistence Manager for GroupWise that is **not** *Autodiscover.x.y*—since that name is reserved for Outlook use. (In these examples, the "*x.y*" domain is the SMTP address to the right of the @ symbol.) The Coexistence Manager for GroupWise website could be, for example, *coexist.x.y*. The Coexistence Manager for GroupWise website must also have a matching certificate. (To obtain and install a matching certificate, see 4.2: Obtain and install web services certificates.)
3. Run the O365 A*dd-AvailabilityAddressSpace* cmdlet for the Coexistence Manager for GroupWise Autodiscover address ("*coexist.x.y*") configured in step 2 above.
4. In DNS, make sure the *coexist* domain has an A record pointing to Coexistence Manager for GroupWise.
5. Test the configuration: Open a web browser and enter the URL ("*https://coexist.x.y/autodiscover/autodiscover.xml*") to verify that it resolves it correctly and without any certification errors.

To configure Office 365 for multiple subdomains

Coexistence Manager for GroupWise's Free/Busy Connector can facilitate the flow of free/busy information among multiple subdomains supported by both Office 365 and the GroupWise servers. To support this scenario, run the *Add-AvailabilityAddressSpace* cmdlet on Office 365 for each GroupWise SMTP domain supported.

Step 4: Configure Coexistence Manager for GroupWise's FBC Web Server

To configure Coexistence Manager for GroupWise's FBC Web Server:

4.1: Physically install the Coexistence Manager for GroupWise FBC components

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The installation instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers.

See the configuration map you made in step 1 above to determine which components should be installed to which servers for this scenario.

If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed in step 1 above. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit.

IMPORTANT: ***Before you install,*** on any computer that will host any Coexistence Manager for GroupWise FBC web subcomponent, remove the IIS *DefaultWebSite*: In the navigation tree at left, right-click **DefaultWebSite**, and then select **Remove** from the pop-up menu. Coexistence Manager for GroupWise requires a dedicated server for its own web subcomponents.

Use the AutoRun utility now to install all the necessary Coexistence Manager for GroupWise F/B Connector subcomponents on the computer(s) where you want them installed.

IMPORTANT: ***Remember,*** the Coexistence Manager for GroupWise AutoRun installer must be run on the computer where you want to install a particular subcomponent. If you are deploying the F/B Connector to two different computers, you must run the AutoRun installer twice—once on each computer.

NOTE: The AutoRun installer automatically checks your environment to verify Coexistence Manager for GroupWise prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command string.

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

Remember: For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted in step 1 above, for Exchange queries to

GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

4.2: Obtain and install web services certificates

Coexistence Manager for GroupWise Web Server components must support HTTPS to accept SSL connections. The server on which these components are installed must have a certificate that Exchange trusts. The single certificate must cover the primary domain and all subdomains supported by the GroupWise Server. The certificate covers the Autodiscover and EWS web services.

Coexistence Manager for GroupWise includes an *Autodiscover Certificate Wizard* to automate much of the process of installing this necessary certificate for the Free/Busy Connector. The wizard can be launched from Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*), as described in the procedure documented in the next subtopic below (see Using the Autodiscover Certificate Wizard to Obtain and Install a Certificate). Alternatively you can manually request and install a certificate, as described in the second subtopic below (see To Manually Request and Install a Certificate Using IIS 7.0–8.5).

Using the *Autodiscover Certificate Wizard* to Obtain and Install a Certificate

Even when using the wizard, you will still have to manually request the certificate, and then tell the wizard where the certificate file resides, so the wizard can install it for use with Coexistence Manager for GroupWise.

To use the *Autodiscover Certificate Wizard* to install the necessary web services certificate using IIS 7.0–8.5:

1 In Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*): Click the **Autodiscover Certificate Wizard** button to launch the wizard.

2 Enter the information requested by the wizard until the wizard displays a window of data for you to copy to a certificate request form. Copy (Ctrl+a) the data.

At this point the wizard will remain open, waiting for you to obtain the certificate. You can obtain a certificate from a local certification authority (CA) if you are using an on-premises Exchange server, or from a public CA (like Verisign or Microsoft Active Directory Certificate Services) if you are using Exchange in a hosted environment (e.g., Office 365).

> **NOTE: If you need a multi-domain certificate:** See To Create a SAN Certificate below.

> **NOTE:** You can request a certificate using Web enrollment pages. For more information, see http://support.microsoft.com/kb/931351.

3 Request and obtain the certificate (while the Coexistence Manager for GroupWise wizard waits).

To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate. At some point you will paste into the request form the text you copied from the wizard (in step 2 above).

To request a certificate from a local CA:

a From a web browser, enter ***https://<Local_Certification_Authority_computer>/certsrv***

b Click **Request a certificate**, then click **Advanced certificate request**.

c Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.

d Paste the text you copied from the wizard (in step 2 above) into the certificate request form.

e In the **Certificate Template** box, select **Web Server**.

f Click **Submit**.

g Select **Base 64 Encoded**, then select **Download certificate**.

4 Back in the *Autodiscover Certificate Wizard*: Click **Next**.

5 Specify the path and filename of the certificate file downloaded in step 3 above, and click **Finish** to register the file and dismiss the wizard.

To Manually Request and Install a Certificate Using IIS 7.0–8.5

To manually request a certificate using IIS 7.0–8.5:

1 From Internet Information Services, click **Server Certificates**.

2 From the Actions Pane, select **Create Certificate Request**.

3 Enter **autodiscover.<smtpdomain>** or **<smtpdomain>** for the primary domain and all required subdomains. Then click **Next**.

4 Accept the defaults, and click **Next**.

5 Specify the file name, and click **Finish**.

6 Request a certificate using a local CA or public CA.

To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate.

To request a certificate from a local CA:

a From a web browser, enter **https://<Local_Certification_Authority_computer>/certsrv**

b Click **Request a certificate**, then click **Advanced certificate request**.

c Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.

d Open the text file where you save the certificate request.

e Copy and paste the text from the certificate request into the **Saved Request** box when you selected Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

f In the **Certificate Template** box, select **Web Server**.

g Click **Submit**.

h Select **Base 64 Encoded**, then select **Download certificate**.

To manually install the certificate using IIS 7.0–8.5:

1 From Internet Information Services, click **Server Certificates**.

2 From the Actions Pane, select **Complete Certificate Request**.

3 Select the saved certificate file, and enter a friendly name for the certificate, then click **OK**.

NOTE: To create an https binding for the web site using IIS 7.0–8.5:

1 From the Connection Pane in IIS, select **QuestFreeBusy**.

2 From the Actions Pane, select **Bindings**.

3 Select **Add**. Select **https** as the type for a secure site, and enter the IP address and port number.

4 Select the SSL certificate to pass the certificate into the computer account, and click **View** to view any certificate information.

To Create a SAN Certificate

This procedure lets you configure a single certificate to answer for multiple addresses. This is obviously necessary for a multi-/subdomain configuration, but also, for a single-namespace environment, to create a certificate that will cover both Autodiscover and the root domain.

First, you *must* enable the SAN (Subject Alternate Name) flag on your CA. On the machine running CA services, run these commands at the command prompt to enable the flag:

```
certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
net stop certsvc
net start certsvc
```

When the SAN flag is enabled, you can create the certificate:

1. Open IIS on the machine running F/B and select the server. Scroll to the bottom, open **Server Certificates**, and click on **Create Certificate Request**.
2. For the common name, enter something appropriate for your larger domain. For example, for a domain *alejandro.xyzcorp.com*, the common name on the certificate is **.xyzcorp.com*. (This is somewhat generic, as we will later add specific namespaces to the certificate.)
3. Accept the defaults and enter a name for the request.
4. Open the certificate request you just created, and select and copy ***all*** of the text.
5. Open the certificate web enrollment page for the CA of your domain— e.g., *https://hostname/certsrv*. Then select **Request a Certificate**, and then select **Advanced Certificate Request**.
6. Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.
7. In the **Base-64-encoded certificate request** box, paste all of the text that you copied from the text file in step 4 above.
8. For the **Certificate Template**, select **Web Server**.
9. In the **Additional Attributes** box, enter any alternate-domain information in this format:

   ```
   san:dns=dns.name[&dns=dns.name]
   ```

   ... with *&dns=dns.name* appended for each alternate domain you want the certificate to handle.

   For a single-namespace environment: Enter the autodiscover and root domain, like this:

   ```
   san:dns=autodiscover.xyzcorp.com&dns=xyzcorp.com
   ```

   For a multi-/subdomain environment: You can enter as many domains as you like:

   ```
   san:dns=autodiscover.sub1.xyzcorp.com
   &dns=autodiscover.sub2.xyzcorp.com
   &dns=autodiscover.sub3.xyzcorp.com
   &dns=autodiscover.sub[...].xyzcorp.com
   &dns=autodiscover.sub[n].xyzcorp.com
   ```

   When you are finished, click **Submit**.
10. Select the **DER encoded** radio button, and then select **Download certificate chain**.
11. Enter a name for this.
12. Go back to IIS and click **Complete Certificate Request**.
13. For the **Filename** containing the certification authority's response, click the **Browse** button and select the certificate you just saved. (Be sure to change the file type to *.* instead of *.cer, or you won't see the file you saved—since it is a .P7B extension.) Type a friendly name that is easy to remember and identify so you can find your certificate on the list later. You should then see your new certificate on the list.
14. Select your new certificate and click **View**.
15. Click the **Details** tab, and scroll down to **Subject Alternative Name**. Highlight this field, and you should see all of your domains in the *Details* box.

Now bind your certificate to the HTTPS protocol on the QuestFreeBusy website:

1. On the Coexistence Manager for GroupWise F/B computer, in IIS Manager: Select **QuestFreeBusy**.
2. In the *Actions* pane on the right, select **Bindings**.
3. Select **https** and click **Edit**.

4 In the *Edit Site Binding* window, in the SSL certificate drop-down list: Select the certificate you just created.

5 Click **OK**.

4.3: Configure trusted sites for computers hosting F/B components

Log in as the Coexistence Manager for GroupWise account to be used with the F/B Connector (if you haven't already). Then, in **Internet Options** (via Windows Control Panel or IE **Tools**):

1 Click the *Security* tab, then select **Trusted sites** and click the **Custom level...** button.

2 In **Settings**, scroll down to **User Authentication | Logon**, and click the radio button for *Automatic logon with current user name and password*.

3 Click **OK** to save the selection and return to the *Security* tab.

4 Add the Exchange Server EWS and Autodiscover URLs to the **Trusted Sites**.

5 Click **OK** to save your new **Security** settings and dismiss the **Internet Options** dialog box.

4.4 (optional): Configure logging for F/B components

By default, Coexistence Manager for GroupWise is installed with the *log42net* utility to generate log files of Coexistence Manager for GroupWise components' system activity. This information is critical to diagnosing any problems that may arise. Logging is enabled by default for all Coexistence Manager for GroupWise components.

The default configurations will be suitable for almost all organizations and circumstances, but you can customize logging features if you like. The *log42net* utility may be configured to work a particular way with each Coexistence Manager for GroupWise component. Configuration instructions are nearly identical from one component to another, so we present those details separately, in Appendix C of the Coexistence Manager for GroupWise *User Guide* (not in this *FBC Configuration Guide*).

4.5: Configure Coexistence Manager for GroupWise's FBC for shared/single namespace (equivalent domains)

Coexistence Manager for GroupWise supports equivalent domain names (single, shared namespace) for GroupWise mail users and on-premises Exchange mail users. Equivalent domains are mapped to the primary domain in the Exchange server or GroupWise server. You can use a PowerShell cmdlet to perform this mapping:

- At the Coexistence Manager for GroupWise Web Server, open PowerShell and type:
  Set-CmgGroupWiseFreeBusyConfig -SmtpDomainMappings <*equivalentDomain*>=<*primaryDomain*>

And be sure to repeat the cmdlet for each equivalent domain.

4.6: Run Coexistence Manager for GroupWise's Management Console to configure FBC components

Use Coexistence Manager for GroupWise's Management Console to configure the Free/Busy Connector's components—to identify the participating servers and their locations, register the necessary account access credentials, and set other operating parameters and preferences. See chapter 4 of the Coexistence Manager for GroupWise *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

NOTE: You may use PowerShell commands to configure Coexistence Manager for GroupWise Free/Busy Connector components, instead of Coexistence Manager for GroupWise's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Appendix B in this *Guide*: Appendix: Configuring and troubleshooting the FBC with PowerShell.

Step 5: Configure and test connections among GroupWise, O365 and Coexistence Manager for GroupWise's FBC Web Server

5.1: Synchronize Office 365 and GroupWise directories

Before running any of Coexistence Manager for GroupWise's F/B Connector subcomponents, you must synchronize GroupWise users as Office 365 contacts, and Exchange users to GroupWise. Coexistence Manager for GroupWise's Directory Connector does not support directory synchronizations directly between GroupWise and Office 365. In this non-hybrid O365 scenario, however, you can configure Microsoft's *Azure AD Sync* synchronization tool to synchronize a local AD with Office 365. See Microsoft's *Azure AD Sync* tool documentation for instructions and guidance in configuring the *Azure AD Sync* tool for this purpose.

Make sure that the GroupWise SOAP web service is enabled (step 2 above), since that is also an environmental requirement for Coexistence Manager for GroupWise's Free/Busy Connector.

NOTE: GroupWise sometimes mistakenly generates F/B queries for addresses in the form *user-domain-com@domain.com* (instead of *user@domain.com*). Queries to such addresses will fail if AD does not recognize the address, so be sure to add that address form as an alias in AD for each Exchange user.

5.2: Configure Office 365 connections

Configure and verify the link from Office 365 to the domains/subdomains supported by the GroupWise server. This procedure tests whether the certificate on the Coexistence Manager for GroupWise Web Server is trusted by O365.

For FBC coexistence with Office 365, run *Enable-OrganizationCustomization*, and then create the availability address space by opening a PowerShell session and using the following commands:

```
$Credential = Get-Credential

$Session = New-PSSession -Credential $Credential -AllowRedirection -ConnectionUri
https://ps.outlook.com/PowerShell -Authentication Basic -ConfigurationName Microsoft.Exchange

Import-PSSession $Session

New-AvailabilityConfig –OrgWideAccount <username@domain.onmicrosoft.com>
[replace <username@domain.onmicrosoft.com> with your O365 admin account]

$domain = "<domain.onmicrosoft.com>"
[replace <domain.onmicrosoft.com> with your SMTP domain name in Office 365]

$adminUserId = "<username@domain.onmicrosoft.com>"
[replace <username@domain.onmicrosoft.com> with your O365 admin account]

$adminCredsId = "<username@domain.onmicrosoft.com>"
[replace <username@domain.onmicrosoft.com> with your O365 admin account]

$adminCredsPassword = "<YourPassword>"
[replace <YourPassword> with your Office 365 admin password]

$securePassword = ConvertTo-SecureString $adminCredsPassword -AsPlainText -Force

$adminCreds = New-Object
System.Management.Automation.PSCredential($adminCredsId,$securePassword)

Add-AvailabilityAddressSpace -AccessMethod OrgWideFB -ForestName <domain.com> -Credentials
$adminCreds –TargetAutodiscoverEpr 'https://autodiscover.<domain.com>/autodiscover/autodiscover.xml'
[replace <domain.com> with your SMTP domain name]
```

5.3: Configure DNS

Configure network load balancing (optional)

You can use Network Load Balancing to permit multiple web servers to handle Autodiscover requests. This is optional, *not* required to deploy Coexistence Manager for GroupWise. For more information, see this Microsoft article.

Configure DNS (Domain Name System)

Configure DNS to point *autodiscover.<smtpdomain.com>* to the computer where Coexistence Manager for GroupWise's Autodiscover service is installed. For each domain, Exchange connects to predefined Autodiscover URLs using DNS host entries.

For Exchange to get free/busy information from the domain supported by a GroupWise server, through the Coexistence Manager for GroupWise Free/Busy Connector, you must make the Coexistence Manager for GroupWise Autodiscover Web Service resolvable to this URL:

https://[autodiscover.]<smtpdomain>/autodiscover/autodiscover.xml

8

FBC Scenario #6

• GroupWise via API
• Office 365 (non-hybrid)
• In a multi-namespace environment

This procedure begins with the assumption that you have already reviewed the introductory chapter of this *FBC Configuration Guide* to Determine your FBC scenario. This chapter explains how to configure the FBC and the coexisting environments for F/B scenario #6, specified above.

Follow these steps, in order as presented here, to install and configure Coexistence Manager for GroupWise's F/B Connector for scenario #6:

Step 1: Plan your FBC installation and configuration

Review the System Requirements (in the Coexistence Manager for GroupWise *Release Notes*), and verify either that your environment conforms to the requirements, or that you will have the necessary hardware and software to meet the requirements.

1.1: Make a configuration map

Scan through the installation and configuration procedures in this chapter, and think through what this process will entail in your own environment, to accommodate your own needs and preferences. Identify any special circumstances or issues, and determine how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers, and how they will connect to the GroupWise and Exchange environments.

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers. If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed below. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit, as described in a later step in this chapter.

The typical deployment of FBC components to two computers for this scenario (GW 7 or later via API Gateway, with non-hybrid Office 365) is:

- On Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies):

    - Coexistence Manager for GroupWise Router Service
    - Coexistence Manager for GroupWise API Gateway Bridge Service
    - Coexistence Manager for GroupWise Exchange Free/Busy Service
- On Coexistence Manager for GroupWise Server 2 (for Exchange queries to GroupWise, and GroupWise replies):
    - Coexistence Manager for GroupWise GroupWise Free/Busy Service
    - Coexistence Manager for GroupWise Autodiscover
    - Coexistence Manager for GroupWise EWS

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted just above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

1.2: Complete the Coexistence Manager for GroupWise FBC Planning Worksheet

Use the worksheet in Appendix A of this *FBC Configuration Guide* to gather and organize the information you will need to enter into Coexistence Manager for GroupWise's Management Console application when configuring the Free/Busy Connector. You can print the worksheet to paper, and use a pen or pencil to write the information into the wide right margins.

The actual data-entry work will occur later in this procedure, in step 4.

Step 2: Configure the GroupWise side

Free/busy coexistence with GroupWise 7 requires the GroupWise API Gateway, GroupWise Proxy GWIA, and the GroupWise SOAP web service, as described in the subtopics below.

The API Gateway is also supported (though not recommended) for GroupWise 8 and later. GroupWise 8 admins may choose between the router/postoffice configuration and the original shared-address-book configuration.

NOTE: For F/B coexistence with a mixed GroupWise 7 and 8 environment:

- The GroupWise 8 domain must be the primary domain.
- GroupWise 7 and the API Gateway must be secondary domains.
- GroupWise 7 must be the bridgehead between Coexistence Manager for GroupWise and GroupWise.

A later step of this FBC configuration procedure describes how to configure and test connections among Coexistence Manager for GroupWise FBC components and the GroupWise and Exchange environments.

2.1: Install and configure the GroupWise API Gateway

These components must be installed to support the newer router/postoffice configuration option, required for connection to GroupWise 7. This configuration requires:

- A non-GroupWise domain and non-GroupWise post office.
- A Novell Netware server version 6.0–6.5 running the API Gateway version 4.1v2.

2.2: Enable and configure the GroupWise SOAP web service

FBC coexistence with any supported GroupWise version requires the GroupWise SOAP web service, enabled on the GroupWise Post Office where the Coexistence Manager for GroupWise service account resides. To enable and configure SOAP, see this Novell article, and this one too.

2.3: Create the required proxy GWIA

FBC coexistence with GroupWise version 7 requires a proxy GWIA. In ConsoleOne:

1 Manually create an empty gateway folder called *GWIAFB* (e.g., ..*WPGATE**GWIAFB*).

Copy the entire GWIA folder (the “real” GWIA) to a new proxy GWIA directory, and then delete the *wpcsout**gwiaXXXX* subfolder (where *XXXX* is the gateway unique ID), and delete the *wpcsin* subfolder. Do ***not*** start/enable the proxy GWIA, since the FBC must process the files in the proxy GWIA folders.

> **IMPORTANT:** The proxy GWIA in turn requires:
>
> - Account rights with a minimum of *Read*, *Write* and *Delete* rights for all folders in the proxy GWIA. These rights may vary depending on the OS to which the proxy GWIA is installed. For example, the equivalent rights on Netware are *Read*, *Write*, *Create*, *Modify*, *Erase* and *Filescan* [RWCEMF].
> - A GroupWise mailbox for use with the F/B Connector and associated services.

2 Create a GroupWise Internet Agent called *GWIAFB*, and point it to the *GWIAFB* directory that was just created. (This new GroupWise Internet Agent will need to have a Gateway Type of *Internet Agent*.)

3 Leave the version as 4.x, as this is the only version that is supported by the API Gateway.

4 Change the API agent **Idle Sleep Duration** to 5 seconds.

5 Reconfigure the GW domain to use *GWIAFB* as the default. To do this: Select the Non-GroupWise domain in ConsoleOne and then, on the **Tools** menu: Select **GroupWise System Options** | **Internet Addressing** to open the *Internet Addressing* dialog box. Then select **GWIAFB** from the **Internet Agent for outbound SMTP/MIME messages** drop-down list. Click **OK** to save the changes.

Step 3: Configure the Office 365 side

To configure a non-hybrid Office 365 for Coexistence Manager for GroupWise’s F/B Connector in a separate/multiple namespace environment:

1 In DNS, make sure the *coexist* domain has an A record pointing to Coexistence Manager for GroupWise.

2 Configure an Autodiscover website for Coexistence Manager for GroupWise (for example, *Autodiscover.x.y*, where the "*x.y*" domain is the SMTP address to the right of the @ symbol). The Coexistence Manager for GroupWise website must also have a matching certificate. (To obtain and install a matching certificate, see 4.2: Obtain and install web services certificates.)

3 Run the O365 A*dd-AvailabilityAddressSpace* cmdlet for the Coexistence Manager for GroupWise Autodiscover address.

4 Test the configuration: Open a web browser and enter the URL ("*https://Autodiscover.x.y/autodiscover/autodiscover.xml*") to verify that it resolves it correctly and without any certification errors.

To configure Office 365 for multiple subdomains

Coexistence Manager for GroupWise’s Free/Busy Connector can facilitate the flow of free/busy information among multiple subdomains supported by both Office 365 and the GroupWise servers. To support this scenario, run the *Add-AvailabilityAddressSpace* cmdlet on Office 365 for each GroupWise SMTP domain supported.

Step 4: Configure Coexistence Manager for GroupWise's FBC Web Server

To configure Coexistence Manager for GroupWise's FBC Web Server:

4.1: Physically install the Coexistence Manager for GroupWise FBC components

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The installation instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers.

See the configuration map you made in step 1 above to determine which components should be installed to which servers for this scenario.

If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed in step 1 above. All Coexistence Manager for GroupWise Free/BusyConnector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit.

IMPORTANT: ***Before you install,*** on any computer that will host any Coexistence Manager for GroupWise FBC web subcomponent, remove the IIS *DefaultWebSite*: In the navigation tree at left, right-click **DefaultWebSite**, and then select **Remove** from the pop-up menu. Coexistence Manager for GroupWise requires a dedicated server for its own web subcomponents.

Use the AutoRun utility now to install all the necessary Coexistence Manager for GroupWise F/B Connector subcomponents on the computer(s) where you want them installed.

IMPORTANT: ***Remember,*** the Coexistence Manager for GroupWise AutoRun installer must be run on the computer where you want to install a particular subcomponent. If you are deploying the F/B Connector to two different computers, you must run the AutoRun installer twice—once on each computer.

NOTE: The AutoRun installer automatically checks your environment to verify Coexistence Manager for GroupWise prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command string.

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

Remember: For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted in step 1 above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

4.2: Obtain and install web services certificates

Coexistence Manager for GroupWise Web Server components must support HTTPS to accept SSL connections. The server on which these components are installed must have a certificate that Exchange trusts. The single certificate must cover the primary domain and all subdomains supported by the GroupWise Server. The certificate covers the Autodiscover and EWS web services.

Coexistence Manager for GroupWise includes an *Autodiscover Certificate Wizard* to automate much of the process of installing this necessary certificate for the Free/Busy Connector. The wizard can be launched from Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*), as described in the procedure documented in the next subtopic below (see Using the Autodiscover Certificate Wizard to Obtain and Install a Certificate). Alternatively you can manually request and install a certificate, as described in the second subtopic below (see To Manually Request and Install a Certificate Using IIS 7.0–8.5).

Using the *Autodiscover Certificate Wizard* to Obtain and Install a Certificate

Even when using the wizard, you will still have to manually request the certificate, and then tell the wizard where the certificate file resides, so the wizard can install it for use with Coexistence Manager for GroupWise.

To use the *Autodiscover Certificate Wizard* to install the necessary web services certificate using IIS 7.0–8.5:

1. In Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*): Click the **Autodiscover Certificate Wizard** button to launch the wizard.
2. Enter the information requested by the wizard until the wizard displays a window of data for you to copy to a certificate request form. Copy (Ctrl+a) the data.

   At this point the wizard will remain open, waiting for you to obtain the certificate. You can obtain a certificate from a local certification authority (CA) if you are using an on-premises Exchange server, or from a public CA (like Verisign or Microsoft Active Directory Certificate Services) if you are using Exchange in a hosted environment (e.g., Office 365).

   > **NOTE: If you need a multi-domain certificate:** See To Create a SAN Certificate below.

   > **NOTE:** You can request a certificate using Web enrollment pages. For more information, see http://support.microsoft.com/kb/931351.

3. Request and obtain the certificate (while the Coexistence Manager for GroupWise wizard waits).

   To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate. At some point you will paste into the request form the text you copied from the wizard (in step 2 above).

   To request a certificate from a local CA:

   a. From a web browser, enter ***https://<Local_Certification_Authority_computer>/certsrv***
   b. Click **Request a certificate**, then click **Advanced certificate request**.
   c. Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.
   d. Paste the text you copied from the wizard (in step 2 above) into the certificate request form.
   e. In the **Certificate Template** box, select **Web Server**.
   f. Click **Submit**.
   g. Select **Base 64 Encoded**, then select **Download certificate**.
4. Back in the *Autodiscover Certificate Wizard*: Click **Next**.
5. Specify the path and filename of the certificate file downloaded in step 3 above, and click **Finish** to register the file and dismiss the wizard.

To Manually Request and Install a Certificate Using IIS 7.0–8.5

To manually request a certificate using IIS 7.0–8.5:

1. From Internet Information Services, click **Server Certificates**.
2. From the Actions Pane, select **Create Certificate Request**.
3. Enter **autodiscover.<smtpdomain>** or **<smtpdomain>** for the primary domain and all required subdomains. Then click **Next**.
4. Accept the defaults, and click **Next**.
5. Specify the file name, and click **Finish**.
6. Request a certificate using a local CA or public CA.

   To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate.

   To request a certificate from a local CA:

   a. From a web browser, enter **https://<Local_Certification_Authority_computer>/certsrv**
   b. Click **Request a certificate**, then click **Advanced certificate request**.
   c. Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.
   d. Open the text file where you save the certificate request.
   e. Copy and paste the text from the certificate request into the **Saved Request** box when you selected Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
   f. In the **Certificate Template** box, select **Web Server**.
   g. Click **Submit**.
   h. Select **Base 64 Encoded**, then select **Download certificate**.

To manually install the certificate using IIS 7.0–8.5:

1. From Internet Information Services, click **Server Certificates**.
2. From the Actions Pane, select **Complete Certificate Request**.
3. Select the saved certificate file, and enter a friendly name for the certificate, then click **OK**.

NOTE: To create an https binding for the web site using IIS 7.0–8.5:

1. From the Connection Pane in IIS, select **QuestFreeBusy**.
2. From the Actions Pane, select **Bindings**.
3. Select **Add**. Select **https** as the type for a secure site, and enter the IP address and port number.
4. Select the SSL certificate to pass the certificate into the computer account, and click **View** to view any certificate information.

To Create a SAN Certificate

This procedure lets you configure a single certificate to answer for multiple addresses. This is obviously necessary for a multi-/subdomain configuration, but also, for a single-namespace environment, to create a certificate that will cover both Autodiscover and the root domain.

First, you *must* enable the SAN (Subject Alternate Name) flag on your CA. On the machine running CA services, run these commands at the command prompt to enable the flag:

```
certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
net stop certsvc
net start certsvc
```

When the SAN flag is enabled, you can create the certificate:

1. Open IIS on the machine running F/B and select the server. Scroll to the bottom, open **Server Certificates**, and click on **Create Certificate Request**.
2. For the common name, enter something appropriate for your larger domain. For example, for a domain *alejandro.xyzcorp.com*, the common name on the certificate is **.xyzcorp.com*. (This is somewhat generic, as we will later add specific namespaces to the certificate.)
3. Accept the defaults and enter a name for the request.
4. Open the certificate request you just created, and select and copy ***all*** of the text.
5. Open the certificate web enrollment page for the CA of your domain— e.g., *https://hostname/certsrv*. Then select **Request a Certificate**, and then select **Advanced Certificate Request**.
6. Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.
7. In the **Base-64-encoded certificate request** box, paste all of the text that you copied from the text file in step 4 above.
8. For the **Certificate Template**, select **Web Server**.
9. In the **Additional Attributes** box, enter any alternate-domain information in this format:

   san:dns=dns.name[&dns=dns.name]

   ... with *&dns=dns.name* appended for each alternate domain you want the certificate to handle.

   For a single-namespace environment: Enter the autodiscover and root domain, like this:

   san:dns=autodiscover.xyzcorp.com&dns=xyzcorp.com

   For a multi-/subdomain environment: You can enter as many domains as you like:

   san:dns=autodiscover.sub1.xyzcorp.com
   &dns=autodiscover.sub2.xyzcorp.com
   &dns=autodiscover.sub3.xyzcorp.com
   &dns=autodiscover.sub[...].xyzcorp.com
   &dns=autodiscover.sub[n].xyzcorp.com

   When you are finished, click **Submit**.
10. Select the **DER encoded** radio button, and then select **Download certificate chain**.
11. Enter a name for this.
12. Go back to IIS and click **Complete Certificate Request**.
13. For the **Filename** containing the certification authority's response, click the **Browse** button and select the certificate you just saved. (Be sure to change the file type to *.* instead of *.cer, or you won't see the file you saved—since it is a .P7B extension.) Type a friendly name that is easy to remember and identify so you can find your certificate on the list later. You should then see your new certificate on the list.
14. Select your new certificate and click **View**.
15. Click the **Details** tab, and scroll down to **Subject Alternative Name**. Highlight this field, and you should see all of your domains in the *Details* box.

Now bind your certificate to the HTTPS protocol on the QuestFreeBusy website:

1. On the Coexistence Manager for GroupWise F/B computer, in IIS Manager: Select **QuestFreeBusy**.
2. In the *Actions* pane on the right, select **Bindings**.
3. Select **https** and click **Edit**.
4. In the *Edit Site Binding* window, in the SSL certificate drop-down list: Select the certificate you just created.
5. Click **OK**.

4.3: Configure trusted sites for computers hosting F/B components

Log in as the Coexistence Manager for GroupWise account to be used with the F/B Connector (if you haven't already). Then, in **Internet Options** (via Windows Control Panel or IE **Tools**):

1. Click the *Security* tab, then select **Trusted sites** and click the **Custom level...** button.
2. In **Settings**, scroll down to **User Authentication | Logon**, and click the radio button for *Automatic logon with current user name and password*.
3. Click **OK** to save the selection and return to the *Security* tab.
4. Add the Exchange Server EWS and Autodiscover URLs to the **Trusted Sites**.
5. Click **OK** to save your new **Security** settings and dismiss the **Internet Options** dialog box.

4.4 (optional): Configure logging for F/B components

By default, Coexistence Manager for GroupWise is installed with the *log42net* utility to generate log files of Coexistence Manager for GroupWise components' system activity. This information is critical to diagnosing any problems that may arise. Logging is enabled by default for all Coexistence Manager for GroupWise components.

The default configurations will be suitable for almost all organizations and circumstances, but you can customize logging features if you like. The *log42net* utility may be configured to work a particular way with each Coexistence Manager for GroupWise component. Configuration instructions are nearly identical from one component to another, so we present those details separately, in Appendix C of the Coexistence Manager for GroupWise *User Guide* (not in this *FBC Configuration Guide*).

4.5: Run Coexistence Manager for GroupWise's Management Console to configure FBC components

Use Coexistence Manager for GroupWise's Management Console to configure the Free/Busy Connector's components—to identify the participating servers and their locations, register the necessary account access credentials, and set other operating parameters and preferences. See chapter 4 of the Coexistence Manager for GroupWise *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

> **NOTE:** You may use PowerShell commands to configure Coexistence Manager for GroupWise Free/Busy Connector components, instead of Coexistence Manager for GroupWise's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Appendix B in this *Guide*: Appendix: Configuring and troubleshooting the FBC with PowerShell.

Step 5: Configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server

5.1: Synchronize Exchange and GroupWise directories

Before running any of Coexistence Manager for GroupWise's F/B Connector subcomponents, you must synchronize GroupWise users as Office 365 contacts, and Exchange users to GroupWise. Coexistence Manager for GroupWise's Directory Connector does not support directory synchronizations directly between GroupWise and Office 365. In this non-hybrid O365 scenario, however, you can configure Microsoft's *Azure AD Sync* synchronization tool to synchronize a local AD with Office 365. See Microsoft's *Azure AD Sync* tool documentation for instructions and guidance in configuring the *Azure AD Sync* tool for this purpose.

Make sure that the GroupWise SOAP web service is enabled (step 2 above), since that is also an environmental requirement for Coexistence Manager for GroupWise's Free/Busy Connector.

NOTE: GroupWise sometimes mistakenly generates F/B queries for addresses in the form *user-domain-com@domain.com* (instead of *user@domain.com*). Queries to such addresses will fail if AD does not recognize the address, so be sure to add that address form as an alias in AD for each Exchange user.

5.2: Configure Office 365 connections

Configure and verify the link from Office 365 to the domains/subdomains supported by the GroupWise server. This procedure tests whether the certificate on the Coexistence Manager for GroupWise Web Server is trusted by O365.

For FBC coexistence with Office 365, run *Enable-OrganizationCustomization*, and then create the availability address space by opening a PowerShell session and using the following commands:

$Credential = Get-Credential

$Session = New-PSSession -Credential $Credential -AllowRedirection -ConnectionUri https://ps.outlook.com/PowerShell -Authentication Basic -ConfigurationName Microsoft.Exchange

Import-PSSession $Session

New-AvailabilityConfig –OrgWideAccount <username@domain.onmicrosoft.com>
[replace <username@domain.onmicrosoft.com> with your O365 admin account]

$domain = "<domain.onmicrosoft.com>"
[replace <domain.onmicrosoft.com> with your SMTP domain name in Office 365]

$adminUserId = "<username@domain.onmicrosoft.com>"
[replace <username@domain.onmicrosoft.com> with your O365 admin account]

$adminCredsId = "<username@domain.onmicrosoft.com>"
[replace <username@domain.onmicrosoft.com> with your O365 admin account]

$adminCredsPassword = "<YourPassword>"
[replace <YourPassword> with your Office 365 admin password]

$securePassword = ConvertTo-SecureString $adminCredsPassword -AsPlainText -Force

$adminCreds = New-Object System.Management.Automation.PSCredential($adminCredsId,$securePassword)

Add-AvailabilityAddressSpace -AccessMethod OrgWideFB -ForestName <domain.com> -Credentials $adminCreds –TargetAutodiscoverEpr 'https://autodiscover.<domain.com>/autodiscover/autodiscover.xml'
[replace <domain.com> with your SMTP domain name]

5.3: Configure DNS

Configure network load balancing (optional)

You can use Network Load Balancing to permit multiple web servers to handle Autodiscover requests. This is optional, *not* required to deploy Coexistence Manager for GroupWise. For more information, see this Microsoft article.

Configure DNS (Domain Name System)

Configure DNS to point *autodiscover.<smtpdomain.com>* to the computer where Coexistence Manager for GroupWise's Autodiscover service is installed. For each domain, Exchange connects to predefined Autodiscover URLs using DNS host entries.

For Exchange to get free/busy information from the domain supported by a GroupWise server, through the Coexistence Manager for GroupWise Free/Busy Connector, you must make the Coexistence Manager for GroupWise Autodiscover Web Service resolvable to this URL:

https://[autodiscover.]<smtpdomain>/autodiscover/autodiscover.xml

9

FBC Scenario #7

- **GroupWise 8 or later via F/B Internet URL**
- **On-premises Exchange 2007 or later (or hybrid O365)**
- **Outlook 2007 or later**
- **In a single (shared) namespace**

This procedure begins with the assumption that you have already reviewed the introductory chapter of this *FBC Configuration Guide* to Determine your FBC scenario. This chapter explains how to configure the FBC and the coexisting environments for F/B scenario #7, specified above.

Follow these steps, in order as presented here, to install and configure Coexistence Manager for GroupWise's F/B Connector for scenario #7:

- Step 1: Plan your FBC installation and configuration
- Step 2: Configure the GroupWise side
- Step 3: Configure the Exchange side
- Step 4: Configure CMG's FBC Web Server
- Step 5: Configure and test connections among GroupWise, Exchange and CMG's FBC Web Server

Remember that the FBC for a hybrid O365 is configured only between GroupWise and the local on-premises Exchange, while synchronization of the local Exchange to O365 is a connection apart from Coexistence Manager for GroupWise and documented separately by Microsoft. Configuring Coexistence Manager for GroupWise's FBC for a hybrid O365 is therefore the same as configuring for a local on-premises Exchange.

IMPORTANT: For a hybrid Office 365, remember to configure and test the hybrid connection between your local Exchange and O365 (as documented by Microsoft) ***before*** configuring Coexistence Manager for GroupWise's FBC.

Step 1: Plan your FBC installation and configuration

Review the System Requirements (in the Coexistence Manager for GroupWise *Release Notes*), and verify either that your environment conforms to the requirements, or that you will have the necessary hardware and software to meet the requirements.

1.1: Make a configuration map

Scan through the installation and configuration procedures in this chapter, and think through what this process will entail in your own environment, to accommodate your own needs and preferences. Identify any special circumstances or issues, and determine how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers, and how they will connect to the GroupWise and Exchange environments.

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers. If you prefer that all subcomponents reside

on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed below. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit, as described in a later step in this chapter.

The typical deployment of FBC components to two computers for this scenario (GW 8 or later via F/B URL, with Exchange 2007 or later and Outlook 2007 or later) is:

- On Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies):
  - Coexistence Manager for GroupWise Free/Busy Bridge
  - Coexistence Manager for GroupWise Exchange Free/Busy Service
- On Coexistence Manager for GroupWise Server 2 (for Exchange queries to GroupWise, and GroupWise replies):
  - Coexistence Manager for GroupWise GroupWise Free/Busy Service
  - Coexistence Manager for GroupWise Autodiscover
  - Coexistence Manager for GroupWise EWS

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted just above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

1.2: Complete the Coexistence Manager for GroupWise FBC Planning Worksheet

Use the worksheet in Appendix A of this *FBC Configuration Guide* to gather and organize the information you will need to enter into Coexistence Manager for GroupWise's Management Console application when configuring the Free/Busy Connector. You can print the worksheet to paper, and use a pen or pencil to write the information into the wide right margins.

The actual data-entry work will occur later in this procedure, in step 4.

Step 2: Configure the GroupWise side

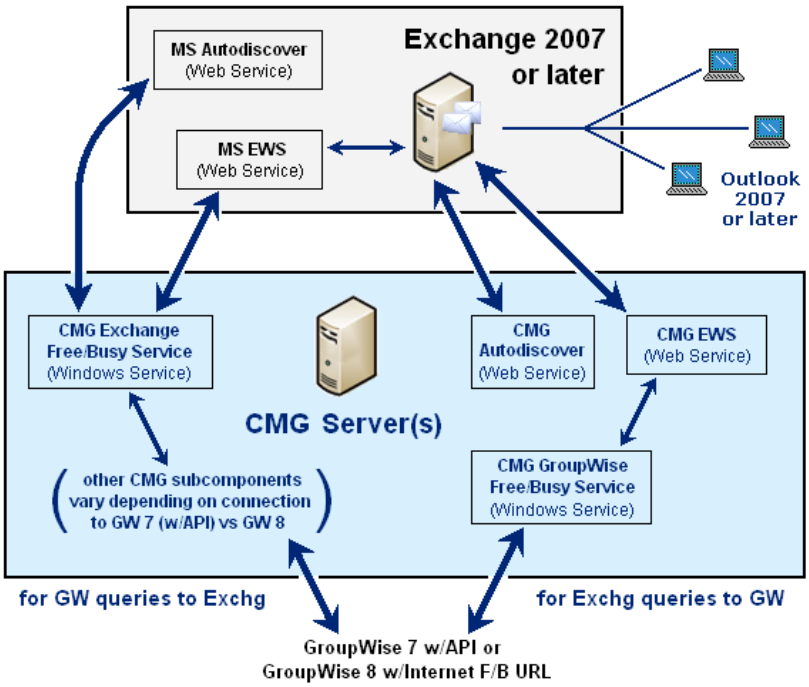
GroupWise versions 8 and later can connect to Coexistence Manager for GroupWise's Free/Busy Connector via a F/B Internet URL.

FBC coexistence with any supported GroupWise version requires the GroupWise SOAP web service, enabled on the GroupWise Post Office where the Coexistence Manager for GroupWise service account resides. To enable and configure SOAP, see this Novell article, and this one too.

A later step of this FBC configuration procedure describes how to configure and test connections among Coexistence Manager for GroupWise FBC components and the GroupWise and Exchange environments.

Step 3: Configure the Exchange side

Other than an accommodation for multiple subdomains (see next subtopic below), no additional Exchange configuration is necessary for the FBC to work with an Exchange environment whose Outlook clients are all version 2007 or later, and where Exchange will connect with the FBC by Microsoft's Autodiscover and EWS (with*out* Exchange public folders). This Exchange-side scenario is illustrated here:



If you are configuring FBC for a hybrid Office 365: Remember that the FBC for a hybrid O365 is configured only between GroupWise and the local on-premises Exchange, while synchronization of the local Exchange to O365 is configured apart from Coexistence Manager for GroupWise (and documented separately by Microsoft). Configuration of Coexistence Manager for GroupWise's FBC for a hybrid O365 is therefore the same as configuring for a local on-premises Exchange—as described here.

To configure the Exchange side for multiple subdomains

Coexistence Manager for GroupWise's Free/Busy Connector can facilitate the flow of free/busy information among multiple subdomains supported by both the Exchange and GroupWise servers. To support this scenario, run the *Add-AvailabilityAddressSpace* cmdlet on the Exchange server or Office 365 for each GroupWise SMTP domain supported.

Step 4: Configure Coexistence Manager for GroupWise's FBC Web Server

To configure Coexistence Manager for GroupWise's FBC Web Server:

- 4.1: Physically install the CMG FBC components
- 4.2: Obtain and install web services certificates
- 4.3: Configure trusted sites for computers hosting F/B components
- 4.4 (optional): Configure logging for F/B components
- 4.5: Configure CMG's FBC for shared/single namespace (equivalent domains)
- 4.6: Run CMG's Management Console to configure FBC components

4.1: Physically install the Coexistence Manager for GroupWise FBC components

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The installation instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers.

If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed in step 1 above. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit.

See the configuration map you made in step 1 above to determine which components should be installed to which servers for this scenario.

IMPORTANT: ***Before you install,*** on any computer that will host any Coexistence Manager for GroupWise FBC web subcomponent, remove the IIS *DefaultWebSite*: In the navigation tree at left, right-click **DefaultWebSite**, and then select **Remove** from the pop-up menu. Coexistence Manager for GroupWise requires a dedicated server for its own web subcomponents.

Use the AutoRun utility now to install all the necessary Coexistence Manager for GroupWise F/B Connector subcomponents on the computer(s) where you want them installed.

IMPORTANT: ***Remember,*** the Coexistence Manager for GroupWise AutoRun installer must be run on the computer where you want to install a particular subcomponent. If you are deploying the F/B Connector to two different computers, you must run the AutoRun installer twice—once on each computer.

NOTE: The AutoRun installer automatically checks your environment to verify Coexistence Manager for GroupWise prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command string.

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

Remember: For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted in step 1 above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

4.2: Obtain and install web services certificates

Coexistence Manager for GroupWise Web Server components must support HTTPS to accept SSL connections. The server on which these components are installed must have a certificate that Exchange trusts. The single certificate must cover the primary domain and all subdomains supported by the GroupWise Server. The certificate covers the Autodiscover and EWS web services.

Coexistence Manager for GroupWise includes an *Autodiscover Certificate Wizard* to automate much of the process of installing this necessary certificate for the Free/Busy Connector. The wizard can be launched from Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*), as described in the procedure documented in the next subtopic below (see Using the Autodiscover Certificate Wizard to Obtain and Install a Certificate). Alternatively you can manually request and install a certificate, as described in the second subtopic below (see To Manually Request and Install a Certificate Using IIS 7.0–8.5).

Using the *Autodiscover Certificate Wizard* to Obtain and Install a Certificate

Even when using the wizard, you will still have to manually request the certificate, and then tell the wizard where the certificate file resides, so the wizard can install it for use with Coexistence Manager for GroupWise.

To use the *Autodiscover Certificate Wizard* to install the necessary web services certificate using IIS 7.0–8.5:

1. In Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*): Click the **Autodiscover Certificate Wizard** button to launch the wizard.
2. Enter the information requested by the wizard until the wizard displays a window of data for you to copy to a certificate request form. Copy (Ctrl+a) the data.

   At this point the wizard will remain open, waiting for you to obtain the certificate. You can obtain a certificate from a local certification authority (CA) if you are using an on-premises Exchange server, or from a public CA (like Verisign or Microsoft Active Directory Certificate Services) if you are using Exchange in a hosted environment (e.g., Office 365).

   > **NOTE: If you need a multi-domain certificate:** See To Create a SAN Certificate below.

   > **NOTE:** You can request a certificate using Web enrollment pages. For more information, see http://support.microsoft.com/kb/931351.

3. Request and obtain the certificate (while the Coexistence Manager for GroupWise wizard waits).

   To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate. At some point you will paste into the request form the text you copied from the wizard (in step 2 above).

   To request a certificate from a local CA:

   a. From a web browser, enter ***https://<Local_Certification_Authority_computer>/certsrv***
   b. Click **Request a certificate**, then click **Advanced certificate request**.
   c. Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.
   d. Paste the text you copied from the wizard (in step 2 above) into the certificate request form.
   e. In the **Certificate Template** box, select **Web Server**.
   f. Click **Submit**.
   g. Select **Base 64 Encoded**, then select **Download certificate**.

4. Back in the *Autodiscover Certificate Wizard*: Click **Next**.
5. Specify the path and filename of the certificate file downloaded in step 3 above, and click **Finish** to register the file and dismiss the wizard.

To Manually Request and Install a Certificate Using IIS 7.0–8.5

To manually request a certificate using IIS 7.0–8.5:

1. From Internet Information Services, click **Server Certificates**.
2. From the Actions Pane, select **Create Certificate Request**.
3. Enter **autodiscover.<smtpdomain>** or **<smtpdomain>** for the primary domain and all required subdomains. Then click **Next**.
4. Accept the defaults, and click **Next**.
5. Specify the file name, and click **Finish**.
6. Request a certificate using a local CA or public CA.

To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate.

To request a certificate from a local CA:

a From a web browser, enter **https://<Local_Certification_Authority_computer>/certsrv**

b Click **Request a certificate**, then click **Advanced certificate request**.

c Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.

d Open the text file where you save the certificate request.

e Copy and paste the text from the certificate request into the **Saved Request** box when you selected Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

f In the **Certificate Template** box, select **Web Server**.

g Click **Submit**.

h Select **Base 64 Encoded**, then select **Download certificate**.

To manually install the certificate using IIS 7.0–8.5:

1 From Internet Information Services, click **Server Certificates**.

2 From the Actions Pane, select **Complete Certificate Request**.

3 Select the saved certificate file, and enter a friendly name for the certificate, then click **OK**.

NOTE: To create an https binding for the web site using IIS 7.0–8.5:

1 From the Connection Pane in IIS, select **QuestFreeBusy**.

2 From the Actions Pane, select **Bindings**.

3 Select **Add**. Select **https** as the type for a secure site, and enter the IP address and port number.

4 Select the SSL certificate to pass the certificate into the computer account, and click **View** to view any certificate information.

To Create a SAN Certificate

This procedure lets you configure a single certificate to answer for multiple addresses. This is obviously necessary for a multi-/subdomain configuration, but also, for a single-namespace environment, to create a certificate that will cover both Autodiscover and the root domain.

First, you *must* enable the SAN (Subject Alternate Name) flag on your CA. On the machine running CA services, run these commands at the command prompt to enable the flag:

```
certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
net stop certsvc
net start certsvc
```

When the SAN flag is enabled, you can create the certificate:

1 Open IIS on the machine running F/B and select the server. Scroll to the bottom, open **Server Certificates**, and click on **Create Certificate Request**.

2 For the common name, enter something appropriate for your larger domain. For example, for a domain *alejandro.xyzcorp.com*, the common name on the certificate is **.xyzcorp.com*. (This is somewhat generic, as we will later add specific namespaces to the certificate.)

3 Accept the defaults and enter a name for the request.

4 Open the certificate request you just created, and select and copy ***all*** of the text.

5 Open the certificate web enrollment page for the CA of your domain— e.g., *https://hostname/certsrv*. Then select **Request a Certificate**, and then select **Advanced Certificate Request**.

6 Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.

7 In the **Base-64-encoded certificate request** box, paste all of the text that you copied from the text file in step 4 above.

8 For the **Certificate Template**, select **Web Server**.

9 In the **Additional Attributes** box, enter any alternate-domain information in this format:

san:dns=dns.name[&dns=dns.name]

... with *&dns=dns.name* appended for each alternate domain you want the certificate to handle.

For a single-namespace environment: Enter the autodiscover and root domain, like this:

san:dns=autodiscover.xyzcorp.com&dns=xyzcorp.com

For a multi-/subdomain environment: You can enter as many domains as you like:

san:dns=autodiscover.sub1.xyzcorp.com
&dns=autodiscover.sub2.xyzcorp.com
&dns=autodiscover.sub3.xyzcorp.com
&dns=autodiscover.sub[...].xyzcorp.com
&dns=autodiscover.sub[n].xyzcorp.com

When you are finished, click **Submit**.

10 Select the **DER encoded** radio button, and then select **Download certificate chain**.

11 Enter a name for this.

12 Go back to IIS and click **Complete Certificate Request**.

13 For the **Filename** containing the certification authority's response, click the **Browse** button and select the certificate you just saved. (Be sure to change the file type to *.* instead of *.cer, or you won't see the file you saved—since it is a .P7B extension.) Type a friendly name that is easy to remember and identify so you can find your certificate on the list later. You should then see your new certificate on the list.

14 Select your new certificate and click **View**.

15 Click the **Details** tab, and scroll down to **Subject Alternative Name**. Highlight this field, and you should see all of your domains in the *Details* box.

Now bind your certificate to the HTTPS protocol on the QuestFreeBusy website:

1 On the Coexistence Manager for GroupWise F/B computer, in IIS Manager: Select **QuestFreeBusy**.

2 In the *Actions* pane on the right, select **Bindings**.

3 Select **https** and click **Edit**.

4 In the *Edit Site Binding* window, in the SSL certificate drop-down list: Select the certificate you just created.

5 Click **OK**.

4.3: Configure trusted sites for computers hosting F/B components

Log in as the Coexistence Manager for GroupWise account to be used with the F/B Connector (if you haven't already). Then, in **Internet Options** (via Windows Control Panel or IE **Tools**):

1 Click the *Security* tab, then select **Trusted sites** and click the **Custom level...** button.

2 In **Settings**, scroll down to **User Authentication | Logon**, and click the radio button for *Automatic logon with current user name and password*.

3 Click **OK** to save the selection and return to the *Security* tab.

4 Add the Exchange Server EWS and Autodiscover URLs to the **Trusted Sites**.

5 Click **OK** to save your new **Security** settings and dismiss the **Internet Options** dialog box.

4.4 (optional): Configure logging for F/B components

By default, Coexistence Manager for GroupWise is installed with the *log42net* utility to generate log files of Coexistence Manager for GroupWise components' system activity. This information is critical to diagnosing any problems that may arise. Logging is enabled by default for all Coexistence Manager for GroupWise components.

The default configurations will be suitable for almost all organizations and circumstances, but you can customize logging features if you like. The *log42net* utility may be configured to work a particular way with each Coexistence Manager for GroupWise component. Configuration instructions are nearly identical from one component to another, so we present those details separately, in Appendix C of the Coexistence Manager for GroupWise *User Guide* (not in this *FBC Configuration Guide*).

4.5: Configure Coexistence Manager for GroupWise's FBC for shared/single namespace (equivalent domains)

Coexistence Manager for GroupWise supports equivalent domain names (single, shared namespace) for GroupWise mail users and on-premises Exchange mail users. Equivalent domains are mapped to the primary domain in the Exchange server or GroupWise server. You can use a PowerShell cmdlet to perform this mapping:

- At the Coexistence Manager for GroupWise Web Server, open PowerShell and type:
  Set-CmgGroupWiseFreeBusyConfig -SmtpDomainMappings <*equivalentDomain*>=<*primaryDomain*>

And be sure to repeat the cmdlet for each equivalent domain.

4.6: Run Coexistence Manager for GroupWise's Management Console to configure FBC components

Use Coexistence Manager for GroupWise's Management Console to configure the Free/Busy Connector's components—to identify the participating servers and their locations, register the necessary account access credentials, and set other operating parameters and preferences. See chapter 4 of the Coexistence Manager for GroupWise *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

IMPORTANT: For a hybrid Office 365:

1. Be sure to add the O365 suffix (*yourdomain.onmicrosoft.com*) to the UPN (User Principal Name) suffixes in the Active Directory Domains and Trusts MMC. This lets Coexistence Manager for GroupWise sign-on to both O365 and the on-prem Exchange with the same credentials (assuming the passwords are the same). If the credentials are different, the FBC lookups to O365 will fail.
2. Make sure the O365 suffix is assigned as the coexistence admin's user logon name for the on-prem Active Directory.

NOTE: You may use PowerShell commands to configure Coexistence Manager for GroupWise Free/Busy Connector components, instead of Coexistence Manager for GroupWise's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Appendix B in this *Guide*: Appendix: Configuring and troubleshooting the FBC with PowerShell.

Step 5: Configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server

To configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server:

5.1: Synchronize Exchange and GroupWise directories

Before running any of Coexistence Manager for GroupWise's F/B Connector subcomponents, you must synchronize GroupWise users as Exchange contacts, and Exchange users to GroupWise. For best performance, Quest recommends using the Coexistence Manager for GroupWise Directory Connector. The Directory Connector is another Coexistence Manager for GroupWise component that you may have already installed and configured, or you can install it now. For complete information about the Coexistence Manager for GroupWise Directory Connector, see *User Guide* chapter 2.

If you are configuring the FBC for a local, on-premises Exchange environment (with or without a hybrid O365), use Coexistence Manager for GroupWise's Directory Connector to define a bidirectional update (a pair of single-direction updates, in opposite directions, run sequentially). Most admins schedule the pair to run automatically at regular intervals to keep both directories current throughout the coexistence period. Be sure that at least one bidirectional update has completed before continuing.

Coexistence Manager for GroupWise's Directory Connector does not support directory synchronizations directly between GroupWise and Office 365. In a hybrid O365 scenario, you can facilitate that directory synchronization by this "two-step" approach:

1. Configure the Coexistence Manager for GroupWise Directory Connector for bidirectional updates between GroupWise and the local, proprietary Active Directory, and then
2. Configure Microsoft's AD Sync tool to synchronize the local AD with the hosted (Office 365) AD.

The combination of the two, run in tandem, would configure an effective directory coexistence between GroupWise and Office 365.

Whatever method you choose to synchronize directories, make sure that the GroupWise SOAP web service is enabled (step 2.2 above), since that is also an environmental requirement for Coexistence Manager for GroupWise's Free/Busy Connector.

NOTE: GroupWise sometimes mistakenly generates F/B queries for addresses in the form *user-domain-com@domain.com* (instead of *user@domain.com*). Queries to such addresses will fail if AD does not recognize the address, so be sure to add that address form as an alias in AD for each Exchange user.

5.2: Configure Exchange server connections

Configure and verify the link from the Exchange server to the domains/subdomains supported by the GroupWise server. This procedure tests whether the certificate on the Coexistence Manager for GroupWise Web Server is trusted by the Exchange server.

To configure the Exchange Server link to the Coexistence Manager for GroupWise Web Server and verify that certificates are trusted by Exchange:

1. At the Exchange Server, open Exchange Management Shell and enter the following cmdlet:

   Add-AvailabilityAddressSpace -ForestName <*smtpdomain*> -AccessMethod OrgWideFB

   ... where <*smtpdomain*> is the name of the GroupWise domain.

2. Open a web browser and enter the URL **http://autodiscover.<domain>/autodiscover/autodiscover.xml** to ensure that the Exchange server resolves it to the Coexistence Manager for GroupWise FBC EWS without any certification errors.
3. Ensure the certificate created earlier is trusted by Exchange. If it is not, see 4.2: Obtain and install web services certificates.

4 For a multiple-domain or subdomains environment, repeat the above steps for each domain.

NOTE: If you created a self-signed certificate and a certification error appears in the Web browser:

1 Click the **SSL** button in the Web browser, then click **View Certificates**.
2 Right-click the certificate to open the **Import Certificate Wizard**.
3 Install the certificate in Trusted Root Certification Authorities, and click **Next**.
4 Click **Import**, then **Finish**.

If you requested a certificate from a public CA, the certificate is already trusted by Exchange.

For F/B coexistence with an Exchange 2013 in a single-namespace environment: On all servers running a mailbox role, modify the hostfile to add the IP address and host name of the Coexistence Manager for GroupWise Autodiscover.

To enable shared SMTP namespace F/B lookups in the Exchange-to-Notes direction, add the Coexistence Manager for GroupWise F/B Web Services IP address to the host file on the Exchange CAS server.

If Exchange has sites that are handled by Exchange 2003:

- These domains must be added to the 2007/2010/2013 servers' availability address space as *PublicFolders* (not *OrgWideFB*).

5.3: Configure DNS

Configure network load balancing (optional)

You can use Network Load Balancing to permit multiple web servers to handle Autodiscover requests. This is optional, *not* required to deploy Coexistence Manager for GroupWise. For more information, see this Microsoft article.

Configure DNS (Domain Name System)

Configure DNS to point *autodiscover.<smtpdomain.com>* to the computer where Coexistence Manager for GroupWise's Autodiscover service is installed. For each domain, Exchange connects to predefined Autodiscover URLs using DNS host entries.

For Exchange to get free/busy information from the domain supported by a GroupWise server, through the Coexistence Manager for GroupWise Free/Busy Connector, you must make the Coexistence Manager for GroupWise Autodiscover Web Service resolvable to this URL:

https://[autodiscover.]<smtpdomain>/autodiscover/autodiscover.xml

10

FBC Scenario #8

- **GroupWise 8 or later via F/B Internet URL**
- **On-premises Exchange 2007 or later (or hybrid O365)**
- **Outlook 2007 or later**
- **In a multi-namespace environment**

This procedure begins with the assumption that you have already reviewed the introductory chapter of this *FBC Configuration Guide* to Determine your FBC scenario. This chapter explains how to configure the FBC and the coexisting environments for F/B scenario #8, specified above.

Follow these steps, in order as presented here, to install and configure Coexistence Manager for GroupWise's F/B Connector for scenario #8:

- Step 1: Plan your FBC installation and configuration
- Step 2: Configure the GroupWise side
- Step 3: Configure the Exchange side
- Step 4: Configure CMG's FBC Web Server
- Step 5: Configure and test connections among GroupWise, Exchange and CMG's FBC Web Server

Remember that the FBC for a hybrid O365 is configured only between GroupWise and the local on-premises Exchange, while synchronization of the local Exchange to O365 is a connection apart from Coexistence Manager for GroupWise and documented separately by Microsoft. Configuring Coexistence Manager for GroupWise's FBC for a hybrid O365 is therefore the same as configuring for a local on-premises Exchange.

IMPORTANT: For a hybrid Office 365, remember to configure and test the hybrid connection between your local Exchange and O365 (as documented by Microsoft) ***before*** configuring Coexistence Manager for GroupWise's FBC.

Step 1: Plan your FBC installation and configuration

Review the System Requirements (in the Coexistence Manager for GroupWise *Release Notes*), and verify either that your environment conforms to the requirements, or that you will have the necessary hardware and software to meet the requirements.

1.1: Make a configuration map

Scan through the installation and configuration procedures in this chapter, and think through what this process will entail in your own environment, to accommodate your own needs and preferences. Identify any special circumstances or issues, and determine how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers, and how they will connect to the GroupWise and Exchange environments.

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers. If you prefer that all subcomponents reside

on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed below. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit, as described in a later step in this chapter.

The typical deployment of FBC components to two computers for this scenario (GW 8 or later via F/B URL, with Exchange 2007 or later and Outlook 2007 or later) is:

- On Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies):
  - Coexistence Manager for GroupWise Free/Busy Bridge
  - Coexistence Manager for GroupWise Exchange Free/Busy Service
- On Coexistence Manager for GroupWise Server 2 (for Exchange queries to GroupWise, and GroupWise replies):
  - Coexistence Manager for GroupWise GroupWise Free/Busy Service
  - Coexistence Manager for GroupWise Autodiscover
  - Coexistence Manager for GroupWise EWS

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted just above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

1.2: Complete the Coexistence Manager for GroupWise FBC Planning Worksheet

Use the worksheet in Appendix A of this *FBC Configuration Guide* to gather and organize the information you will need to enter into Coexistence Manager for GroupWise's Management Console application when configuring the Free/Busy Connector. You can print the worksheet to paper, and use a pen or pencil to write the information into the wide right margins.

The actual data-entry work will occur later in this procedure, in step 4.

Step 2: Configure the GroupWise side

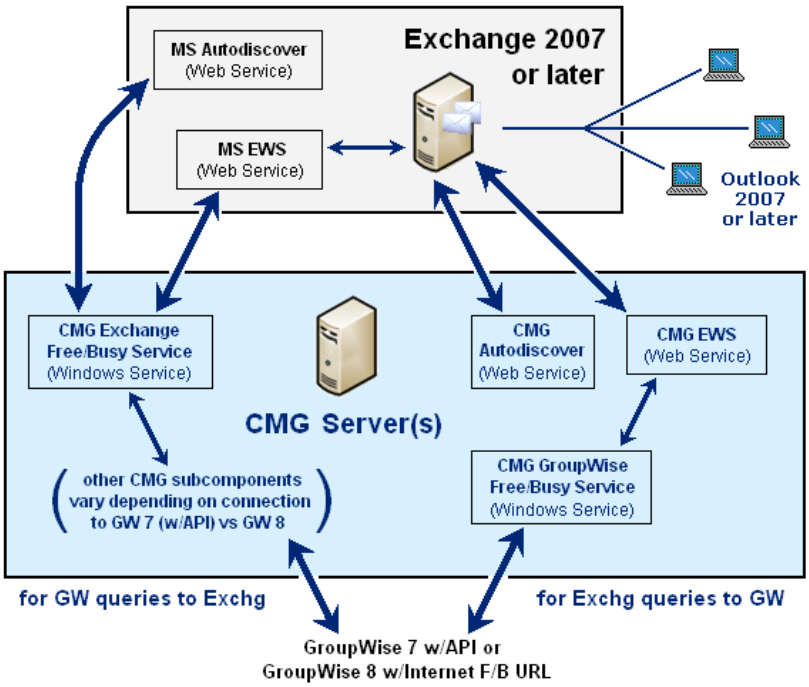
GroupWise versions 8 and later can connect to Coexistence Manager for GroupWise's Free/Busy Connector via a F/B Internet URL.

FBC coexistence with any supported GroupWise version requires the GroupWise SOAP web service, enabled on the GroupWise Post Office where the Coexistence Manager for GroupWise service account resides. To enable and configure SOAP, see this Novell article, and this one too.

A later step of this FBC configuration procedure describes how to configure and test connections among Coexistence Manager for GroupWise FBC components and the GroupWise and Exchange environments.

Step 3: Configure the Exchange side

Other than an accommodation for multiple subdomains (see next subtopic below), no additional Exchange configuration is necessary for the FBC to work with an Exchange environment whose Outlook clients are all version 2007 or later, and where Exchange will connect with the FBC by Microsoft's Autodiscover and EWS (with*out* Exchange public folders). This Exchange-side scenario is illustrated here:



If you are configuring FBC for a hybrid Office 365: Remember that the FBC for a hybrid O365 is configured only between GroupWise and the local on-premises Exchange, while synchronization of the local Exchange to O365 is configured apart from Coexistence Manager for GroupWise (and documented separately by Microsoft). Configuration of Coexistence Manager for GroupWise's FBC for a hybrid O365 is therefore the same as configuring for a local on-premises Exchange—as described here.

To configure the Exchange side for multiple subdomains

Coexistence Manager for GroupWise's Free/Busy Connector can facilitate the flow of free/busy information among multiple subdomains supported by both the Exchange and GroupWise servers. To support this scenario, run the *Add-AvailabilityAddressSpace* cmdlet on the Exchange server or Office 365 for each GroupWise SMTP domain supported.

Step 4: Configure Coexistence Manager for GroupWise's FBC Web Server

To configure Coexistence Manager for GroupWise's FBC Web Server:

- 4.1: Physically install the CMG FBC components
- 4.2: Obtain and install web services certificates
- 4.3: Configure trusted sites for computers hosting F/B components
- 4.4 (optional): Configure logging for F/B components
- 4.5: Run CMG's Management Console to configure FBC components

4.1: Physically install the Coexistence Manager for GroupWise FBC components

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The installation instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers.

If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed in step 1 above. All Coexistence Manager for GroupWise Free/BusyConnector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit.

See the configuration map you made in step 1 above to determine which components should be installed to which servers for this scenario.

IMPORTANT: ***Before you install,*** on any computer that will host any Coexistence Manager for GroupWise FBC web subcomponent, remove the IIS *DefaultWebSite*: In the navigation tree at left, right-click **DefaultWebSite**, and then select **Remove** from the pop-up menu. Coexistence Manager for GroupWise requires a dedicated server for its own web subcomponents.

Use the AutoRun utility now to install all the necessary Coexistence Manager for GroupWise F/B Connector subcomponents on the computer(s) where you want them installed.

IMPORTANT: ***Remember,*** the Coexistence Manager for GroupWise AutoRun installer must be run on the computer where you want to install a particular subcomponent. If you are deploying the F/B Connector to two different computers, you must run the AutoRun installer twice—once on each computer.

NOTE: The AutoRun installer automatically checks your environment to verify Coexistence Manager for GroupWise prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command string.

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

Remember: For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted in step 1 above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

4.2: Obtain and install web services certificates

Coexistence Manager for GroupWise Web Server components must support HTTPS to accept SSL connections. The server on which these components are installed must have a certificate that Exchange trusts. The single certificate must cover the primary domain and all subdomains supported by the GroupWise Server. The certificate covers the Autodiscover and EWS web services.

Coexistence Manager for GroupWise includes an *Autodiscover Certificate Wizard* to automate much of the process of installing this necessary certificate for the Free/Busy Connector. The wizard can be launched from Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*), as described in the procedure documented in the next subtopic below (see Using the Autodiscover Certificate Wizard to Obtain and Install a Certificate). Alternatively you can manually request and install a certificate, as described in the second subtopic below (see To Manually Request and Install a Certificate Using IIS 7.0–8.5).

Using the *Autodiscover Certificate Wizard* to Obtain and Install a Certificate

Even when using the wizard, you will still have to manually request the certificate, and then tell the wizard where the certificate file resides, so the wizard can install it for use with Coexistence Manager for GroupWise.

To use the *Autodiscover Certificate Wizard* to install the necessary web services certificate using IIS 7.0–8.5:

1. In Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*): Click the **Autodiscover Certificate Wizard** button to launch the wizard.
2. Enter the information requested by the wizard until the wizard displays a window of data for you to copy to a certificate request form. Copy (Ctrl+a) the data.

   At this point the wizard will remain open, waiting for you to obtain the certificate. You can obtain a certificate from a local certification authority (CA) if you are using an on-premises Exchange server, or from a public CA (like Verisign or Microsoft Active Directory Certificate Services) if you are using Exchange in a hosted environment (e.g., Office 365).

   > **NOTE: If you need a multi-domain certificate:** See To Create a SAN Certificate below.

   > **NOTE:** You can request a certificate using Web enrollment pages. For more information, see http://support.microsoft.com/kb/931351.

3. Request and obtain the certificate (while the Coexistence Manager for GroupWise wizard waits).

   To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate. At some point you will paste into the request form the text you copied from the wizard (in step 2 above).

   To request a certificate from a local CA:

   a. From a web browser, enter ***https://<Local_Certification_Authority_computer>/certsrv***
   b. Click **Request a certificate**, then click **Advanced certificate request**.
   c. Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.
   d. Paste the text you copied from the wizard (in step 2 above) into the certificate request form.
   e. In the **Certificate Template** box, select **Web Server**.
   f. Click **Submit**.
   g. Select **Base 64 Encoded**, then select **Download certificate**.

4. Back in the *Autodiscover Certificate Wizard*: Click **Next**.
5. Specify the path and filename of the certificate file downloaded in step 3 above, and click **Finish** to register the file and dismiss the wizard.

To Manually Request and Install a Certificate Using IIS 7.0–8.5

To manually request a certificate using IIS 7.0–8.5:

1. From Internet Information Services, click **Server Certificates**.
2. From the Actions Pane, select **Create Certificate Request**.
3. Enter **autodiscover.<smtpdomain>** or **<smtpdomain>** for the primary domain and all required subdomains. Then click **Next**.
4. Accept the defaults, and click **Next**.
5. Specify the file name, and click **Finish**.
6. Request a certificate using a local CA or public CA.

To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate.

To request a certificate from a local CA:

a From a web browser, enter **https://<Local_Certification_Authority_computer>/certsrv**

b Click **Request a certificate**, then click **Advanced certificate request**.

c Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.

d Open the text file where you save the certificate request.

e Copy and paste the text from the certificate request into the **Saved Request** box when you selected Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

f In the **Certificate Template** box, select **Web Server**.

g Click **Submit**.

h Select **Base 64 Encoded**, then select **Download certificate**.

To manually install the certificate using IIS 7.0–8.5:

1 From Internet Information Services, click **Server Certificates**.

2 From the Actions Pane, select **Complete Certificate Request**.

3 Select the saved certificate file, and enter a friendly name for the certificate, then click **OK**.

NOTE: To create an https binding for the web site using IIS 7.0–8.5:

1 From the Connection Pane in IIS, select **QuestFreeBusy**.

2 From the Actions Pane, select **Bindings**.

3 Select **Add**. Select **https** as the type for a secure site, and enter the IP address and port number.

4 Select the SSL certificate to pass the certificate into the computer account, and click **View** to view any certificate information.

To Create a SAN Certificate

This procedure lets you configure a single certificate to answer for multiple addresses. This is obviously necessary for a multi-/subdomain configuration, but also, for a single-namespace environment, to create a certificate that will cover both Autodiscover and the root domain.

First, you *must* enable the SAN (Subject Alternate Name) flag on your CA. On the machine running CA services, run these commands at the command prompt to enable the flag:

```
certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
net stop certsvc
net start certsvc
```

When the SAN flag is enabled, you can create the certificate:

1 Open IIS on the machine running F/B and select the server. Scroll to the bottom, open **Server Certificates**, and click on **Create Certificate Request**.

2 For the common name, enter something appropriate for your larger domain. For example, for a domain *alejandro.xyzcorp.com*, the common name on the certificate is **.xyzcorp.com*. (This is somewhat generic, as we will later add specific namespaces to the certificate.)

3 Accept the defaults and enter a name for the request.

4 Open the certificate request you just created, and select and copy ***all*** of the text.

5 Open the certificate web enrollment page for the CA of your domain— e.g., *https://hostname/certsrv*. Then select **Request a Certificate**, and then select **Advanced Certificate Request**.

6 Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.

7 In the **Base-64-encoded certificate request** box, paste all of the text that you copied from the text file in step 4 above.

8 For the **Certificate Template**, select **Web Server**.

9 In the **Additional Attributes** box, enter any alternate-domain information in this format:

san:dns=dns.name[&dns=dns.name]

... with *&dns=dns.name* appended for each alternate domain you want the certificate to handle.

For a single-namespace environment: Enter the autodiscover and root domain, like this:

san:dns=autodiscover.xyzcorp.com&dns=xyzcorp.com

For a multi-/subdomain environment: You can enter as many domains as you like:

san:dns=autodiscover.sub1.xyzcorp.com
&dns=autodiscover.sub2.xyzcorp.com
&dns=autodiscover.sub3.xyzcorp.com
&dns=autodiscover.sub[...].xyzcorp.com
&dns=autodiscover.sub[n].xyzcorp.com

When you are finished, click **Submit**.

10 Select the **DER encoded** radio button, and then select **Download certificate chain**.

11 Enter a name for this.

12 Go back to IIS and click **Complete Certificate Request**.

13 For the **Filename** containing the certification authority's response, click the **Browse** button and select the certificate you just saved. (Be sure to change the file type to *.* instead of *.cer, or you won't see the file you saved—since it is a .P7B extension.) Type a friendly name that is easy to remember and identify so you can find your certificate on the list later. You should then see your new certificate on the list.

14 Select your new certificate and click **View**.

15 Click the **Details** tab, and scroll down to **Subject Alternative Name**. Highlight this field, and you should see all of your domains in the *Details* box.

Now bind your certificate to the HTTPS protocol on the QuestFreeBusy website:

1 On the Coexistence Manager for GroupWise F/B computer, in IIS Manager: Select **QuestFreeBusy**.

2 In the *Actions* pane on the right, select **Bindings**.

3 Select **https** and click **Edit**.

4 In the *Edit Site Binding* window, in the SSL certificate drop-down list: Select the certificate you just created.

5 Click **OK**.

4.3: Configure trusted sites for computers hosting F/B components

Log in as the Coexistence Manager for GroupWise account to be used with the F/B Connector (if you haven't already). Then, in **Internet Options** (via Windows Control Panel or IE **Tools**):

1 Click the *Security* tab, then select **Trusted sites** and click the **Custom level...** button.

2 In **Settings**, scroll down to **User Authentication | Logon**, and click the radio button for *Automatic logon with current user name and password*.

3 Click **OK** to save the selection and return to the *Security* tab.

4 Add the Exchange Server EWS and Autodiscover URLs to the **Trusted Sites**.

5 Click **OK** to save your new **Security** settings and dismiss the **Internet Options** dialog box.

4.4 (optional): Configure logging for F/B components

By default, Coexistence Manager for GroupWise is installed with the *log42net* utility to generate log files of Coexistence Manager for GroupWise components' system activity. This information is critical to diagnosing any problems that may arise. Logging is enabled by default for all Coexistence Manager for GroupWise components.

The default configurations will be suitable for almost all organizations and circumstances, but you can customize logging features if you like. The *log42net* utility may be configured to work a particular way with each Coexistence Manager for GroupWise component. Configuration instructions are nearly identical from one component to another, so we present those details separately, in Appendix C of the Coexistence Manager for GroupWise *User Guide* (not in this *FBC Configuration Guide*).

4.5: Run Coexistence Manager for GroupWise's Management Console to configure FBC components

Use Coexistence Manager for GroupWise's Management Console to configure the Free/Busy Connector's components—to identify the participating servers and their locations, register the necessary account access credentials, and set other operating parameters and preferences. See chapter 4 of the Coexistence Manager for GroupWise *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

IMPORTANT: For a hybrid Office 365:

1. Be sure to add the O365 suffix (*yourdomain.onmicrosoft.com*) to the UPN (User Principal Name) suffixes in the Active Directory Domains and Trusts MMC. This lets Coexistence Manager for GroupWise sign-on to both O365 and the on-prem Exchange with the same credentials (assuming the passwords are the same). If the credentials are different, the FBC lookups to O365 will fail.
2. Make sure the O365 suffix is assigned as the coexistence admin's user logon name for the on-prem Active Directory.

NOTE: You may use PowerShell commands to configure Coexistence Manager for GroupWise Free/Busy Connector components, instead of Coexistence Manager for GroupWise's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Appendix B in this *Guide*: Appendix: Configuring and troubleshooting the FBC with PowerShell.

Step 5: Configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server

To configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server:

5.1: Synchronize Exchange and GroupWise directories

Before running any of Coexistence Manager for GroupWise's F/B Connector subcomponents, you must synchronize GroupWise users as Exchange contacts, and Exchange users to GroupWise. For best performance, Quest recommends using the Coexistence Manager for GroupWise Directory Connector. The Directory Connector is another Coexistence Manager for GroupWise component that you may have already installed and configured, or you can install it now. For complete information about the Coexistence Manager for GroupWise Directory Connector, see *User Guide* chapter 2.

If you are configuring the FBC for a local, on-premises Exchange environment (with or without a hybrid O365), use Coexistence Manager for GroupWise's Directory Connector to define a bidirectional update (a pair of single-direction updates, in opposite directions, run sequentially). Most admins schedule the pair to run automatically at regular intervals to keep both directories current throughout the coexistence period. Be sure that at least one bidirectional update has completed before continuing.

Coexistence Manager for GroupWise's Directory Connector does not support directory synchronizations directly between GroupWise and Office 365. In a hybrid O365 scenario, you can facilitate that directory synchronization by this "two-step" approach:

1. Configure the Coexistence Manager for GroupWise Directory Connector for bidirectional updates between GroupWise and the local, proprietary Active Directory, and then
2. Configure Microsoft's AD Sync tool to synchronize the local AD with the hosted (Office 365) AD.

The combination of the two, run in tandem, would configure an effective directory coexistence between GroupWise and Office 365.

Whatever method you choose to synchronize directories, make sure that the GroupWise SOAP web service is enabled (step 2.2 above), since that is also an environmental requirement for Coexistence Manager for GroupWise's Free/Busy Connector.

NOTE: GroupWise sometimes mistakenly generates F/B queries for addresses in the form *user-domain-com@domain.com* (instead of *user@domain.com*). Queries to such addresses will fail if AD does not recognize the address, so be sure to add that address form as an alias in AD for each Exchange user.

5.2: Configure Exchange server connections

Configure and verify the link from the Exchange server to the domains/subdomains supported by the GroupWise server. This procedure tests whether the certificate on the Coexistence Manager for GroupWise Web Server is trusted by the Exchange server.

To configure the Exchange Server link to the Coexistence Manager for GroupWise Web Server and verify that certificates are trusted by Exchange:

1. At the Exchange Server, open Exchange Management Shell and enter the following cmdlet:

   Add-AvailabilityAddressSpace -ForestName <*smtpdomain*> -AccessMethod OrgWideFB

   ... where <*smtpdomain*> is the name of the GroupWise domain.
2. Open a web browser and enter the URL **http://autodiscover.<domain>/autodiscover/autodiscover.xml** to ensure that the Exchange server resolves it to the Coexistence Manager for GroupWise FBC EWS without any certification errors.
3. Ensure the certificate created earlier is trusted by Exchange. If it is not, see 4.2: Obtain and install web services certificates.
4. For a multiple-domain or subdomains environment, repeat the above steps for each domain.

NOTE: If you created a self-signed certificate and a certification error appears in the Web browser:

1. Click the **SSL** button in the Web browser, then click **View Certificates**.
2. Right-click the certificate to open the **Import Certificate Wizard**.
3. Install the certificate in Trusted Root Certification Authorities, and click **Next**.
4. Click **Import**, then **Finish**.

If you requested a certificate from a public CA, the certificate is already trusted by Exchange.

For F/B coexistence with an Exchange 2013 in a single-namespace environment: On all servers running a mailbox role, modify the hostfile to add the IP address and host name of the Coexistence Manager for GroupWise Autodiscover.

To enable shared SMTP namespace F/B lookups in the Exchange-to-Notes direction, add the Coexistence Manager for GroupWise F/B Web Services IP address to the host file on the Exchange CAS server.

If Exchange has sites that are handled by Exchange 2003:

- These domains must be added to the 2007/2010/2013 servers' availability address space as *PublicFolders* (not *OrgWideFB*).

5.3: Configure DNS

Configure network load balancing (optional)

You can use Network Load Balancing to permit multiple web servers to handle Autodiscover requests. This is optional, *not* required to deploy Coexistence Manager for GroupWise. For more information, see this Microsoft article.

Configure DNS (Domain Name System)

Configure DNS to point *autodiscover.<smtpdomain.com>* to the computer where Coexistence Manager for GroupWise's Autodiscover service is installed. For each domain, Exchange connects to predefined Autodiscover URLs using DNS host entries.

For Exchange to get free/busy information from the domain supported by a GroupWise server, through the Coexistence Manager for GroupWise Free/Busy Connector, you must make the Coexistence Manager for GroupWise Autodiscover Web Service resolvable to this URL:

https://[autodiscover.]<smtpdomain>/autodiscover/autodiscover.xml

11

FBC Scenario #9

- **GroupWise 8 or later via F/B Internet URL**
- **On-premises Exchange 2007 or 2003**
- **Outlook 2003 (using Exchange public folders)**
- **In a single (shared) namespace**

This procedure begins with the assumption that you have already reviewed the introductory chapter of this *FBC Configuration Guide* to Determine your FBC scenario. This chapter explains how to configure the FBC and the coexisting environments for F/B scenario #9, specified above.

Follow these steps, in order as presented here, to install and configure Coexistence Manager for GroupWise's F/B Connector for scenario #9:

- Step 1: Plan your FBC installation and configuration
- Step 2: Configure the GroupWise side
- Step 3: Configure the Exchange side
- Step 4: Configure CMG's FBC Web Server
- Step 5: Configure and test connections among GroupWise, Exchange and CMG's FBC Web Server

Step 1: Plan your FBC installation and configuration

Review the System Requirements (in the Coexistence Manager for GroupWise *Release Notes*), and verify either that your environment conforms to the requirements, or that you will have the necessary hardware and software to meet the requirements.

1.1: Make a configuration map

Scan through the installation and configuration procedures in this chapter, and think through what this process will entail in your own environment, to accommodate your own needs and preferences. Identify any special circumstances or issues, and determine how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers, and how they will connect to the GroupWise and Exchange environments.

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers. If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed below. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit, as described in a later step in this chapter.

The typical deployment of FBC components to two computers for this scenario (GW 8 or later via F/B URL, and connections to Outlook 2003 via Exchange public folders) depends on how the public folders will connect to the Coexistence Manager for GroupWise components for GroupWise queries to Exchange. With Exchange 2003, that

half of the process must be routed through Coexistence Manager for GroupWise's Public Folder Reader Service, and the typical deployment is:

- On Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies):
    - Coexistence Manager for GroupWise Free/Busy Bridge
    - Coexistence Manager for GroupWise Public Folder Reader Service
- On Coexistence Manager for GroupWise Server 2 (for Exchange queries to GroupWise, and GroupWise replies):
    - Coexistence Manager for GroupWise GroupWise Free/Busy Service
    - Coexistence Manager for GroupWise Public Folder Writer Service

With Exchange 2007, GroupWise queries to Exchange may be routed through Coexistence Manager for GroupWise's Public Folder Reader Service, by the same deployment as shown above, or may instead be routed through Microsoft's Autodiscover and EWS. In the latter case, the typical deployment for Coexistence Manager for GroupWise Server 2 is the same as shown above, but Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies) contains:

- Coexistence Manager for GroupWise Free/Busy Bridge
- Coexistence Manager for GroupWise Exchange Free/Busy Service

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted just above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

1.2: Complete the Coexistence Manager for GroupWise FBC Planning Worksheet

Use the worksheet in Appendix A of this *FBC Configuration Guide* to gather and organize the information you will need to enter into Coexistence Manager for GroupWise's Management Console application when configuring the Free/Busy Connector. You can print the worksheet to paper, and use a pen or pencil to write the information into the wide right margins.

The actual data-entry work will occur later in this procedure, in step 4.

Step 2: Configure the GroupWise side

GroupWise versions 8 and later can connect to Coexistence Manager for GroupWise's Free/Busy Connector via a F/B Internet URL.

FBC coexistence with any supported GroupWise version requires the GroupWise SOAP web service, enabled on the GroupWise Post Office where the Coexistence Manager for GroupWise service account resides. To enable and configure SOAP, see this Novell article, and this one too.

A later step of this FBC configuration procedure describes how to configure and test connections among Coexistence Manager for GroupWise FBC components and the GroupWise and Exchange environments.

Step 3: Configure the Exchange side

Configure domains, permissions and other server parameters and attributes so they will be able to work with Coexistence Manager for GroupWise's Free/Busy Connector.

To configure the Exchange side for multiple subdomains

Coexistence Manager for GroupWise's Free/Busy Connector can facilitate the flow of free/busy information among multiple subdomains supported by both the Exchange and GroupWise servers. To support this scenario, run the *Add-AvailabilityAddressSpace* cmdlet on the Exchange server for each GroupWise SMTP domain supported.

Configure Exchange 2003 or 2007 to use Exchange public folders

In these scenarios, Exchange queries for GroupWise F/B data (see the right halves of the Coexistence Manager for GroupWise servers in the diagrams below) are not sent to GroupWise, but rather are routed internally to Exchange's own public folders, which Coexistence Manager for GroupWise regularly refreshes by its Coexistence Manager for GroupWise Public Folder Writer Service. For GroupWise queries to Exchange, however, Coexistence Manager for GroupWise supports two options (described in the next two subtopics below):

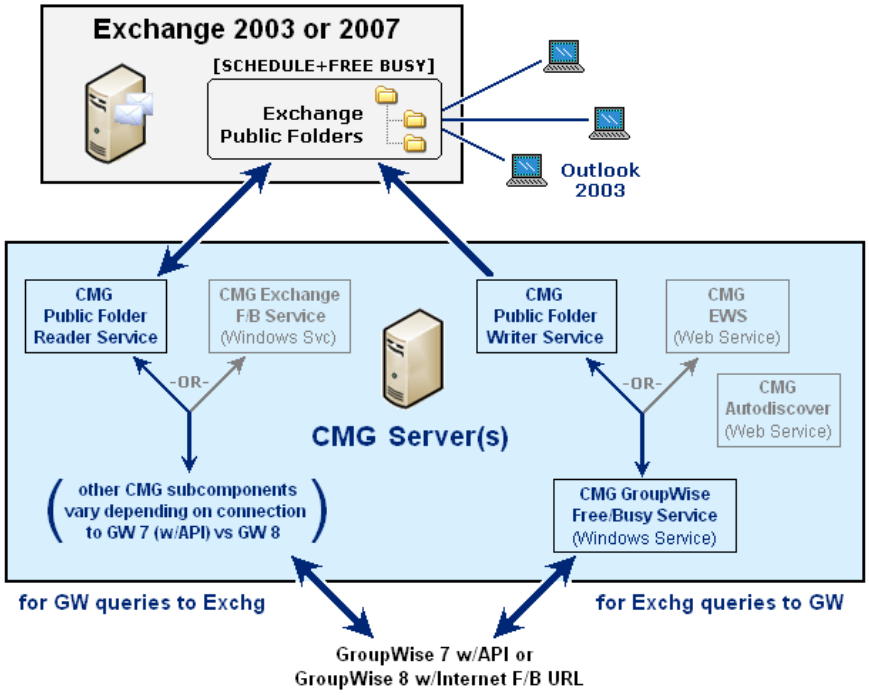
- with Outlook 2003 via Coexistence Manager for GroupWise's Public Folder Reader Service
- with Outlook 2003 and Exchange 2007 (only) via Microsoft's Autodiscover and EWS

FBC with Outlook 2003 via Coexistence Manager for GroupWise's Public Folder Reader Service

For either Exchange 2003 or 2007, GroupWise queries for Exchange F/B data (the left halves of the Coexistence Manager for GroupWise servers in the diagrams below) can pass through Coexistence Manager for GroupWise's Public Folder Reader Service. The Public Folder Reader Service relays GroupWise F/B queries to Exchange public folders, and then relays the F/B info back to GroupWise.

Outlook users' queries for GroupWise F/B info (the right halves of the Coexistence Manager for GroupWise servers in these diagrams) are routed directly to Exchange public folders (internally within the Exchange environment). The public folders reply by transmitting their F/B info directly to the Outlook users. No Coexistence Manager for GroupWise components are used for that query-reply portion of the F/B process. But the Exchange public folders must regularly be refreshed with GroupWise users' current F/B info, and that function is performed by Coexistence Manager for GroupWise's Public Folder Writer Service.

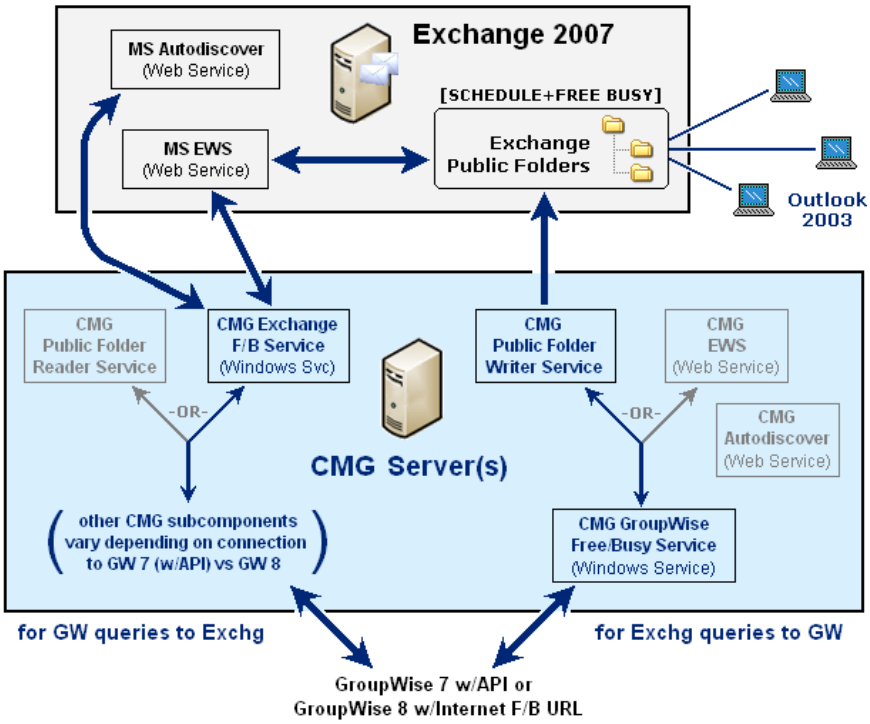
Coexistence Manager for GroupWise's Public Folder Writer Service collects GroupWise users' current F/B info from GroupWise to refresh the Exchange public folders, and also communicates with Active Directory to get and maintain a current list of GroupWise contacts in the Exchange system.



FBC with Outlook 2003 and Exchange 2007 via Microsoft's Autodiscover and EWS

Coexistence Manager for GroupWise can connect to Exchange 2007 public folders either via its Public Folder Reader Service (as described above), or via Microsoft's Autodiscover and EWS, as described here and illustrated in the diagram below. Connecting via the Microsoft services is not an option with Exchange 2003.

This configuration uses Coexistence Manager for GroupWise's Exchange Free/Busy Connector Service to relay GroupWise F/B queries to Microsoft's Autodiscover and EWS on the Exchange server, and relay the F/B info back from MS Autodiscover and EWS to GroupWise. (Microsoft's Autodiscover and EWS in turn relay GroupWise F/B queries to Exchange public folders, and receive the public folders' F/B info.)



Coexistence Manager for GroupWise uses its Public Folder Writer Service to get GroupWise users' current F/B info from GroupWise and, at regular intervals, to refresh the corresponding F/B info held in the Exchange public folders. The Public Folder Writer Service also communicates with Active Directory to get and maintain a current list of GroupWise contacts in the Exchange system. Outlook users' queries for GroupWise F/B info are routed directly to Exchange public folders (internally within the Exchange environment), while the public folders transmit the F/B info directly to the Outlook users.

Step 4: Configure Coexistence Manager for GroupWise's FBC Web Server

To configure Coexistence Manager for GroupWise's FBC Web Server:

- 4.1: Physically install the CMG FBC components
- 4.2: Configure trusted sites for computers hosting F/B components
- 4.3 (optional): Configure logging for F/B components
- 4.4: Configure CMG's FBC for shared/single namespace (equivalent domains)
- 4.5: Run CMG's Management Console to configure FBC components

4.1: Physically install the Coexistence Manager for GroupWise FBC components

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The installation instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers.

If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed in step 1 above. All Coexistence Manager for GroupWise Free/BusyConnector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit.

See the configuration map you made in step 1 above to determine which components should be installed to which servers for this scenario.

> **IMPORTANT:** ***Before you install,*** on any computer that will host any Coexistence Manager for GroupWise FBC web subcomponent, remove the IIS *DefaultWebSite*: In the navigation tree at left, right-click **DefaultWebSite**, and then select **Remove** from the pop-up menu. Coexistence Manager for GroupWise requires a dedicated server for its own web subcomponents.

Use the AutoRun utility now to install all the necessary Coexistence Manager for GroupWise F/B Connector subcomponents on the computer(s) where you want them installed.

> **IMPORTANT:** ***Remember,*** the Coexistence Manager for GroupWise AutoRun installer must be run on the computer where you want to install a particular subcomponent. If you are deploying the F/B Connector to two different computers, you must run the AutoRun installer twice—once on each computer.

> **NOTE:** Coexistence Manager for GroupWise's Public Folder Writer Service and Public Folder Reader Service are available only via the *Custom Setup* option of Coexistence Manager for GroupWise's F/B Connector *Setup* utility.

> **NOTE:** The AutoRun installer automatically checks your environment to verify Coexistence Manager for GroupWise prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command string.

> **NOTE:** ***If you are configuring F/B for Exchange 2003:*** Exchange 2003 does not support Coexistence Manager for GroupWise's F/B Bridge subcomponent or PowerShell. The AutoRun installer installs these subcomponents anyway, because it doesn't know how you intend to configure your F/B services, but the Coexistence Manager for GroupWise F/B Bridge and PowerShell will not be used in your configuration.

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

Remember: For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted in step 1 above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

4.2: Configure trusted sites for computers hosting F/B components

> **NOTE:** This step applies only if you are configuring the FBC to use Microsoft's Autodiscover and EWS for an Exchange 2007 server with Outlook 2003 clients.

Log in as the Coexistence Manager for GroupWise account to be used with the F/B Connector (if you haven't already). Then, in **Internet Options** (via Windows Control Panel or IE **Tools**):

1. Click the *Security* tab, then select **Trusted sites** and click the **Custom level...** button.
2. In **Settings**, scroll down to **User Authentication | Logon**, and click the radio button for *Automatic logon with current user name and password*.
3. Click **OK** to save the selection and return to the *Security* tab.
4. Add the Exchange Server EWS and Autodiscover URLs to the **Trusted Sites**.
5. Click **OK** to save your new **Security** settings and dismiss the **Internet Options** dialog box.

4.3 (optional): Configure logging for F/B components

By default, Coexistence Manager for GroupWise is installed with the *log42net* utility to generate log files of Coexistence Manager for GroupWise components' system activity. This information is critical to diagnosing any problems that may arise. Logging is enabled by default for all Coexistence Manager for GroupWise components.

The default configurations will be suitable for almost all organizations and circumstances, but you can customize logging features if you like. The *log42net* utility may be configured to work a particular way with each Coexistence Manager for GroupWise component. Configuration instructions are nearly identical from one component to another, so we present those details separately, in Appendix C of the Coexistence Manager for GroupWise *User Guide* (not in this *FBC Configuration Guide*).

4.4: Configure Coexistence Manager for GroupWise's FBC for shared/single namespace (equivalent domains)

Coexistence Manager for GroupWise supports equivalent domain names (single, shared namespace) for GroupWise mail users and on-premises Exchange mail users. Equivalent domains are mapped to the primary domain in the Exchange server or GroupWise server. You can use a PowerShell cmdlet to perform this mapping:

- At the Coexistence Manager for GroupWise Web Server, open PowerShell and type:
  Set-CmgGroupWiseFreeBusyConfig -SmtpDomainMappings <*equivalentDomain*>=<*primaryDomain*>

And be sure to repeat the cmdlet for each equivalent domain.

4.5: Run Coexistence Manager for GroupWise's Management Console to configure FBC components

Use Coexistence Manager for GroupWise's Management Console to configure the Free/Busy Connector's components—to identify the participating servers and their locations, register the necessary account access credentials, and set other operating parameters and preferences. See chapter 4 of the Coexistence Manager for GroupWise *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

> **NOTE:** You may use PowerShell commands to configure Coexistence Manager for GroupWise Free/Busy Connector components, instead of Coexistence Manager for GroupWise's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Appendix A in this *Guide*: Appendix: Configuring and troubleshooting the FBC with PowerShell.

Step 5: Configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server

5.1: Configure Coexistence Manager for GroupWise's Directory Connector for the FBC

The public-folders configuration for the FBC requires the corresponding DC connector to be configured, for both the *Provision* and *Update* functions, with an attribute assignment that matches the AD *extensionAttribute* you designate for this purpose. (The attribute and its value are designated in the F/B Connector Management Console, in the *Exchange Public Folder Writer-AD Contacts* screen, as described in the *User Guide*.)

5.2: Synchronize Exchange and GroupWise directories

Before running any of Coexistence Manager for GroupWise's F/B Connector subcomponents, you must synchronize GroupWise users as Exchange contacts, and Exchange users to GroupWise. For best performance, Quest recommends using the Coexistence Manager for GroupWise Directory Connector. The Directory Connector is another Coexistence Manager for GroupWise component that you may have already installed and configured, or you can install it now. For complete information about the Coexistence Manager for GroupWise Directory Connector, see *User Guide* chapter 2.

Use Coexistence Manager for GroupWise's Directory Connector to define a bidirectional update (a pair of single-direction updates, in opposite directions, run sequentially). Most admins schedule the pair to run automatically at regular intervals to keep both directories current throughout the coexistence period. Be sure that at least one bidirectional update has completed before continuing.

Whatever method you choose to synchronize directories, make sure that the GroupWise SOAP web service is enabled (step 2.2 above), since that is also an environmental requirement for Coexistence Manager for GroupWise's Free/Busy Connector.

NOTE: GroupWise sometimes mistakenly generates F/B queries for addresses in the form *user-domain-com@domain.com* (instead of *user@domain.com*). Queries to such addresses will fail if AD does not recognize the address, so be sure to add that address form as an alias in AD for each Exchange user.

12

FBC Scenario #10

- **GroupWise 8 or later via F/B Internet URL**
- **On-premises Exchange 2007 or 2003**
- **Outlook 2003 (using Exchange public folders)**
- **In a multi-namespace environment**

This procedure begins with the assumption that you have already reviewed the introductory chapter of this *FBC Configuration Guide* to Determine your FBC scenario. This chapter explains how to configure the FBC and the coexisting environments for F/B scenario #10, specified above.

Follow these steps, in order as presented here, to install and configure Coexistence Manager for GroupWise's F/B Connector for scenario #10:

Step 1: Plan your FBC installation and configuration

Review the System Requirements (in the Coexistence Manager for GroupWise *Release Notes*), and verify either that your environment conforms to the requirements, or that you will have the necessary hardware and software to meet the requirements.

1.1: Make a configuration map

Scan through the installation and configuration procedures in this chapter, and think through what this process will entail in your own environment, to accommodate your own needs and preferences. Identify any special circumstances or issues, and determine how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers, and how they will connect to the GroupWise and Exchange environments.

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers. If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed below. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit, as described in a later step in this chapter.

The typical deployment of FBC components to two computers for this scenario (GW 8 or later via F/B URL, and connections to Outlook 2003 via Exchange public folders) depends on how the public folders will connect to the Coexistence Manager for GroupWise components for GroupWise queries to Exchange. With Exchange 2003, that

half of the process must be routed through Coexistence Manager for GroupWise's Public Folder Reader Service, and the typical deployment is:

- On Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies):
    - Coexistence Manager for GroupWise Free/Busy Bridge
    - Coexistence Manager for GroupWise Public Folder Reader Service
- On Coexistence Manager for GroupWise Server 2 (for Exchange queries to GroupWise, and GroupWise replies):
    - Coexistence Manager for GroupWise GroupWise Free/Busy Service
    - Coexistence Manager for GroupWise Public Folder Writer Service

With Exchange 2007, GroupWise queries to Exchange may be routed through Coexistence Manager for GroupWise's Public Folder Reader Service, by the same deployment as shown above, or may instead be routed through Microsoft's Autodiscover and EWS. In the latter case, the typical deployment for Coexistence Manager for GroupWise Server 2 is the same as shown above, but Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies) contains:

- Coexistence Manager for GroupWise Free/Busy Bridge
- Coexistence Manager for GroupWise Exchange Free/Busy Service

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted just above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

1.2: Complete the Coexistence Manager for GroupWise FBC Planning Worksheet

Use the worksheet in Appendix A of this *FBC Configuration Guide* to gather and organize the information you will need to enter into Coexistence Manager for GroupWise's Management Console application when configuring the Free/Busy Connector. You can print the worksheet to paper, and use a pen or pencil to write the information into the wide right margins.

The actual data-entry work will occur later in this procedure, in step 4.

Step 2: Configure the GroupWise side

GroupWise versions 8 and later can connect to Coexistence Manager for GroupWise's Free/Busy Connector via a F/B Internet URL.

FBC coexistence with any supported GroupWise version requires the GroupWise SOAP web service, enabled on the GroupWise Post Office where the Coexistence Manager for GroupWise service account resides. To enable and configure SOAP, see this Novell article, and this one too.

A later step of this FBC configuration procedure describes how to configure and test connections among Coexistence Manager for GroupWise FBC components and the GroupWise and Exchange environments.

Step 3: Configure the Exchange side

Configure domains, permissions and other server parameters and attributes so they will be able to work with Coexistence Manager for GroupWise's Free/Busy Connector.

To configure the Exchange side for multiple subdomains

Coexistence Manager for GroupWise's Free/Busy Connector can facilitate the flow of free/busy information among multiple subdomains supported by both the Exchange and GroupWise servers. To support this scenario, run the *Add-AvailabilityAddressSpace* cmdlet on the Exchange server for each GroupWise SMTP domain supported.

Configure Exchange 2003 or 2007 to use Exchange public folders

In these scenarios, Exchange queries for GroupWise F/B data (see the right halves of the Coexistence Manager for GroupWise servers in the diagrams below) are not sent to GroupWise, but rather are routed internally to Exchange's own public folders, which Coexistence Manager for GroupWise regularly refreshes by its Coexistence Manager for GroupWise Public Folder Writer Service. For GroupWise queries to Exchange, however, Coexistence Manager for GroupWise supports two options (described in the next two subtopics below):

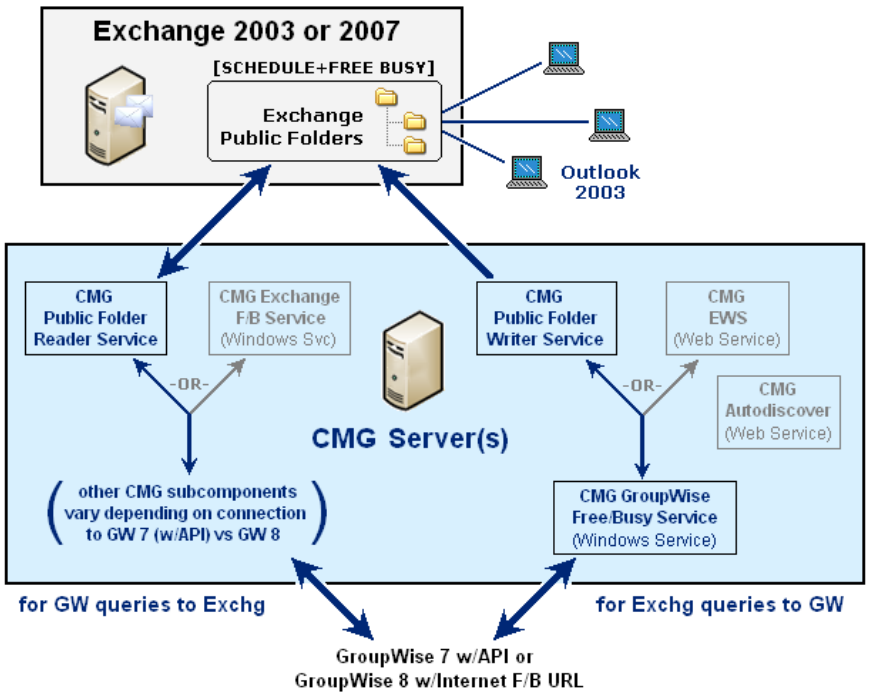
- with Outlook 2003 via Coexistence Manager for GroupWise's Public Folder Reader Service
- with Outlook 2003 and Exchange 2007 (only) via Microsoft's Autodiscover and EWS

FBC with Outlook 2003 via Coexistence Manager for GroupWise's Public Folder Reader Service

For either Exchange 2003 or 2007, GroupWise queries for Exchange F/B data (the left halves of the Coexistence Manager for GroupWise servers in the diagrams below) can pass through Coexistence Manager for GroupWise's Public Folder Reader Service. The Public Folder Reader Service relays GroupWise F/B queries to Exchange public folders, and then relays the F/B info back to GroupWise.

Outlook users' queries for GroupWise F/B info (the right halves of the Coexistence Manager for GroupWise servers in these diagrams) are routed directly to Exchange public folders (internally within the Exchange environment). The public folders reply by transmitting their F/B info directly to the Outlook users. No Coexistence Manager for GroupWise components are used for that query-reply portion of the F/B process. But the Exchange public folders must regularly be refreshed with GroupWise users' current F/B info, and that function is performed by Coexistence Manager for GroupWise's Public Folder Writer Service.

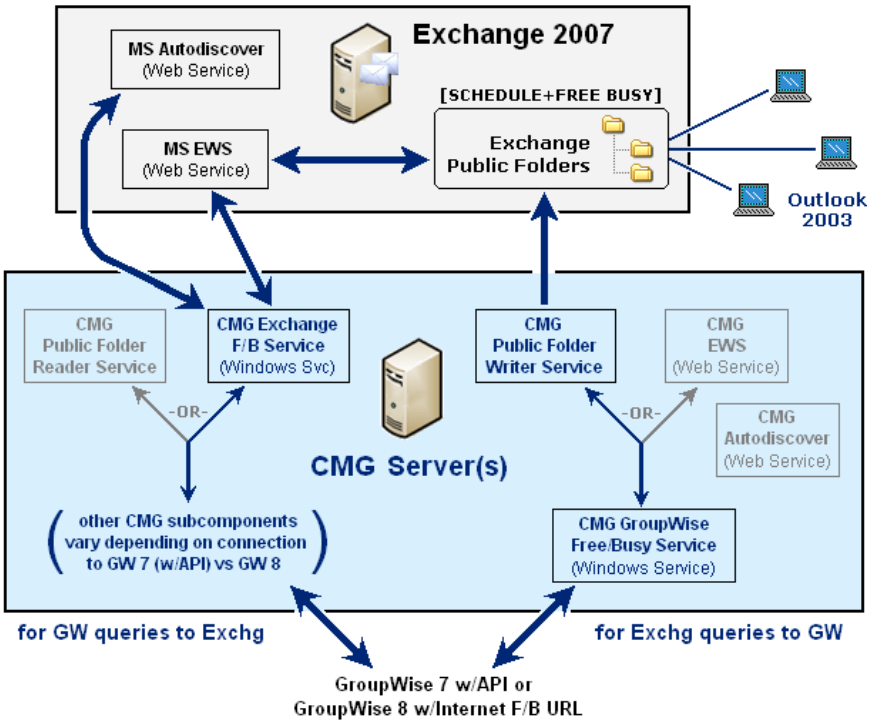
Coexistence Manager for GroupWise's Public Folder Writer Service collects GroupWise users' current F/B info from GroupWise to refresh the Exchange public folders, and also communicates with Active Directory to get and maintain a current list of GroupWise contacts in the Exchange system.



FBC with Outlook 2003 and Exchange 2007 via Microsoft's Autodiscover and EWS

Coexistence Manager for GroupWise can connect to Exchange 2007 public folders either via its Public Folder Reader Service (as described above), or via Microsoft's Autodiscover and EWS, as described here and illustrated in the diagram below. Connecting via the Microsoft services is not an option with Exchange 2003.

This configuration uses Coexistence Manager for GroupWise's Exchange Free/Busy Connector Service to relay GroupWise F/B queries to Microsoft's Autodiscover and EWS on the Exchange server, and relay the F/B info back from MS Autodiscover and EWS to GroupWise. (Microsoft's Autodiscover and EWS in turn relay GroupWise F/B queries to Exchange public folders, and receive the public folders' F/B info.)



Coexistence Manager for GroupWise uses its Public Folder Writer Service to get GroupWise users' current F/B info from GroupWise and, at regular intervals, to refresh the corresponding F/B info held in the Exchange public folders. The Public Folder Writer Service also communicates with Active Directory to get and maintain a current list of GroupWise contacts in the Exchange system. Outlook users' queries for GroupWise F/B info are routed directly to Exchange public folders (internally within the Exchange environment), while the public folders transmit the F/B info directly to the Outlook users.

Step 4: Configure Coexistence Manager for GroupWise's FBC Web Server

To configure Coexistence Manager for GroupWise's FBC Web Server:

- 4.1: Physically install the CMG FBC components
- 4.2: Configure trusted sites for computers hosting F/B components
- 4.3 (optional): Configure logging for F/B components
- 4.4: Run CMG's Management Console to configure FBC components

4.1: Physically install the Coexistence Manager for GroupWise FBC components

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The installation instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers.

If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed in step 1 above. All Coexistence Manager for GroupWise Free/BusyConnector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit.

See the configuration map you made in step 1 above to determine which components should be installed to which servers for this scenario.

> **IMPORTANT:** ***Before you install,*** on any computer that will host any Coexistence Manager for GroupWise FBC web subcomponent, remove the IIS *DefaultWebSite*: In the navigation tree at left, right-click **DefaultWebSite**, and then select **Remove** from the pop-up menu. Coexistence Manager for GroupWise requires a dedicated server for its own web subcomponents.

Use the AutoRun utility now to install all the necessary Coexistence Manager for GroupWise F/B Connector subcomponents on the computer(s) where you want them installed.

> **IMPORTANT:** ***Remember,*** the Coexistence Manager for GroupWise AutoRun installer must be run on the computer where you want to install a particular subcomponent. If you are deploying the F/B Connector to two different computers, you must run the AutoRun installer twice—once on each computer.

> **NOTE:** Coexistence Manager for GroupWise's Public Folder Writer Service and Public Folder Reader Service are available only via the *Custom Setup* option of Coexistence Manager for GroupWise's F/B Connector *Setup* utility.

> **NOTE:** The AutoRun installer automatically checks your environment to verify Coexistence Manager for GroupWise prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command string.

> **NOTE:** ***If you are configuring F/B for Exchange 2003:*** Exchange 2003 does not support Coexistence Manager for GroupWise's F/B Bridge subcomponent or PowerShell. The AutoRun installer installs these subcomponents anyway, because it doesn't know how you intend to configure your F/B services, but the Coexistence Manager for GroupWise F/B Bridge and PowerShell will not be used in your configuration.

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

Remember: For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted in step 1 above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

4.2: Configure trusted sites for computers hosting F/B components

> **NOTE:** This step applies only if you are configuring the FBC to use Microsoft's Autodiscover and EWS for an Exchange 2007 server with Outlook 2003 clients.

Log in as the Coexistence Manager for GroupWise account to be used with the F/B Connector (if you haven't already). Then, in **Internet Options** (via Windows Control Panel or IE **Tools**):

1. Click the *Security* tab, then select **Trusted sites** and click the **Custom level...** button.
2. In **Settings**, scroll down to **User Authentication | Logon**, and click the radio button for *Automatic logon with current user name and password*.
3. Click **OK** to save the selection and return to the *Security* tab.
4. Add the Exchange Server EWS and Autodiscover URLs to the **Trusted Sites**.
5. Click **OK** to save your new **Security** settings and dismiss the **Internet Options** dialog box.

4.3 (optional): Configure logging for F/B components

By default, Coexistence Manager for GroupWise is installed with the *log42net* utility to generate log files of Coexistence Manager for GroupWise components' system activity. This information is critical to diagnosing any problems that may arise. Logging is enabled by default for all Coexistence Manager for GroupWise components.

The default configurations will be suitable for almost all organizations and circumstances, but you can customize logging features if you like. The *log42net* utility may be configured to work a particular way with each Coexistence Manager for GroupWise component. Configuration instructions are nearly identical from one component to another, so we present those details separately, in Appendix C of the Coexistence Manager for GroupWise *User Guide* (not in this *FBC Configuration Guide*).

4.4: Run Coexistence Manager for GroupWise's Management Console to configure FBC components

Use Coexistence Manager for GroupWise's Management Console to configure the Free/Busy Connector's components—to identify the participating servers and their locations, register the necessary account access credentials, and set other operating parameters and preferences. See chapter 4 of the Coexistence Manager for GroupWise *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

> **NOTE:** You may use PowerShell commands to configure Coexistence Manager for GroupWise Free/Busy Connector components, instead of Coexistence Manager for GroupWise's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Appendix A in this *Guide*: Appendix: Configuring and troubleshooting the FBC with PowerShell.

Step 5: Configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server

5.1: Configure Coexistence Manager for GroupWise's Directory Connector for the FBC

The public-folders configuration for the FBC requires the corresponding DC connector to be configured, for both the *Provision* and *Update* functions, with an attribute assignment that matches the AD *extensionAttribute* you designate for this purpose. (The attribute and its value are designated in the F/B Connector Management Console, in the *Exchange Public Folder Writer-AD Contacts* screen, as described in the *User Guide*.)

5.2: Synchronize Exchange and GroupWise directories

Before running any of Coexistence Manager for GroupWise's F/B Connector subcomponents, you must synchronize GroupWise users as Exchange contacts, and Exchange users to GroupWise. For best performance, Quest recommends using the Coexistence Manager for GroupWise Directory Connector. The Directory Connector is another Coexistence Manager for GroupWise component that you may have already installed and configured, or you can install it now. For complete information about the Coexistence Manager for GroupWise Directory Connector, see *User Guide* chapter 2.

Use Coexistence Manager for GroupWise's Directory Connector to define a bidirectional update (a pair of single-direction updates, in opposite directions, run sequentially). Most admins schedule the pair to run automatically at regular intervals to keep both directories current throughout the coexistence period. Be sure that at least one bidirectional update has completed before continuing.

Whatever method you choose to synchronize directories, make sure that the GroupWise SOAP web service is enabled (step 2.2 above), since that is also an environmental requirement for Coexistence Manager for GroupWise's Free/Busy Connector.

NOTE: GroupWise sometimes mistakenly generates F/B queries for addresses in the form *user-domain-com@domain.com* (instead of *user@domain.com*). Queries to such addresses will fail if AD does not recognize the address, so be sure to add that address form as an alias in AD for each Exchange user.

13

FBC Scenario #11

• GroupWise 8 or later via F/B Internet URL
• Office 365 (non-hybrid)
• In a single (shared) namespace

This procedure begins with the assumption that you have already reviewed the introductory chapter of this *FBC Configuration Guide* to Determine your FBC scenario. This chapter explains how to configure the FBC and the coexisting environments for F/B scenario #11, specified above.

Follow these steps, in order as presented here, to install and configure Coexistence Manager for GroupWise's F/B Connector for scenario #11:

- Step 1: Plan your FBC installation and configuration
- Step 2: Configure the GroupWise side
- Step 3: Configure the Office 365 side
- Step 4: Configure CMG's FBC Web Server
- Step 5: Configure and test connections among GroupWise, Exchange and CMG's FBC Web Server

Step 1: Plan your FBC installation and configuration

Review the System Requirements (in the Coexistence Manager for GroupWise *Release Notes*), and verify either that your environment conforms to the requirements, or that you will have the necessary hardware and software to meet the requirements.

1.1: Make a configuration map

Scan through the installation and configuration procedures in this chapter, and think through what this process will entail in your own environment, to accommodate your own needs and preferences. Identify any special circumstances or issues, and determine how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers, and how they will connect to the GroupWise and Exchange environments.

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers. If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed below. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit, as described in a later step in this chapter.

The typical deployment of FBC components to two computers for this scenario (GW 8 or later via F/B URL, with non-hybrid Office 365) is:

- On Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies):

    - Coexistence Manager for GroupWise Free/Busy Bridge
    - Coexistence Manager for GroupWise Exchange Free/Busy Service
- On Coexistence Manager for GroupWise Server 2 (for Exchange queries to GroupWise, and GroupWise replies):
    - Coexistence Manager for GroupWise GroupWise Free/Busy Service
    - Coexistence Manager for GroupWise Autodiscover
    - Coexistence Manager for GroupWise EWS

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted just above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

1.2: Complete the Coexistence Manager for GroupWise FBC Planning Worksheet

Use the worksheet in Appendix A of this *FBC Configuration Guide* to gather and organize the information you will need to enter into Coexistence Manager for GroupWise's Management Console application when configuring the Free/Busy Connector. You can print the worksheet to paper, and use a pen or pencil to write the information into the wide right margins.

The actual data-entry work will occur later in this procedure, in step 4.

Step 2: Configure the GroupWise side

GroupWise versions 8 and later can connect to Coexistence Manager for GroupWise's Free/Busy Connector via a F/B Internet URL.

FBC coexistence with any supported GroupWise version requires the GroupWise SOAP web service, enabled on the GroupWise Post Office where the Coexistence Manager for GroupWise service account resides. To enable and configure SOAP, see this Novell article, and this one too.

A later step of this FBC configuration procedure describes how to configure and test connections among Coexistence Manager for GroupWise FBC components and the GroupWise and Exchange environments.

Step 3: Configure the Office 365 side

To configure a non-hybrid Office 365 for Coexistence Manager for GroupWise's F/B Connector in a single/shared namespace environment:

1. In O365, configure an outbound send connector to point to Coexistence Manager for GroupWise's Mail Connector, to facilitate mail flow apart from free/busy.
2. Configure an Autodiscover website for Coexistence Manager for GroupWise that is **not** *Autodiscover.x.y*—since that name is reserved for Outlook use. (In these examples, the "*x.y*" domain is the SMTP address to the right of the @ symbol.) The Coexistence Manager for GroupWise website could be, for example, *coexist.x.y*. The Coexistence Manager for GroupWise website must also have a matching certificate. (To obtain and install a matching certificate, see 4.2: Obtain and install web services certificates.)

3 Run the O365 A*dd-AvailabilityAddressSpace* cmdlet for the Coexistence Manager for GroupWise Autodiscover address ("*coexist.x.y*") configured in step 2 above.

4 In DNS, make sure the *coexist* domain has an A record pointing to Coexistence Manager for GroupWise.

5 Test the configuration: Open a web browser and enter the URL ("*https://coexist.x.y/autodiscover/autodiscover.xml*") to verify that it resolves it correctly and without any certification errors.

To configure Office 365 for multiple subdomains

Coexistence Manager for GroupWise's Free/Busy Connector can facilitate the flow of free/busy information among multiple subdomains supported by both Office 365 and the GroupWise servers. To support this scenario, run the *Add-AvailabilityAddressSpace* cmdlet on Office 365 for each GroupWise SMTP domain supported.

Step 4: Configure Coexistence Manager for GroupWise's FBC Web Server

To configure Coexistence Manager for GroupWise's FBC Web Server:

4.1: Physically install the Coexistence Manager for GroupWise FBC components

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The installation instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers.

See the configuration map you made in step 1 above to determine which components should be installed to which servers for this scenario.

If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed in step 1 above. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit.

IMPORTANT: ***Before you install,*** on any computer that will host any Coexistence Manager for GroupWise FBC web subcomponent, remove the IIS *DefaultWebSite*: In the navigation tree at left, right-click **DefaultWebSite**, and then select **Remove** from the pop-up menu. Coexistence Manager for GroupWise requires a dedicated server for its own web subcomponents.

Use the AutoRun utility now to install all the necessary Coexistence Manager for GroupWise F/B Connector subcomponents on the computer(s) where you want them installed.

IMPORTANT: ***Remember,*** the Coexistence Manager for GroupWise AutoRun installer must be run on the computer where you want to install a particular subcomponent. If you are deploying the F/B Connector to two different computers, you must run the AutoRun installer twice—once on each computer.

NOTE: The AutoRun installer automatically checks your environment to verify Coexistence Manager for GroupWise prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command string.

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

Remember: For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted in step 1 above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

4.2: Obtain and install web services certificates

Coexistence Manager for GroupWise Web Server components must support HTTPS to accept SSL connections. The server on which these components are installed must have a certificate that Exchange trusts. The single certificate must cover the primary domain and all subdomains supported by the GroupWise Server. The certificate covers the Autodiscover and EWS web services.

Coexistence Manager for GroupWise includes an *Autodiscover Certificate Wizard* to automate much of the process of installing this necessary certificate for the Free/Busy Connector. The wizard can be launched from Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*), as described in the procedure documented in the next subtopic below (see Using the Autodiscover Certificate Wizard to Obtain and Install a Certificate). Alternatively you can manually request and install a certificate, as described in the second subtopic below (see To Manually Request and Install a Certificate Using IIS 7.0–8.5).

Using the *Autodiscover Certificate Wizard* to Obtain and Install a Certificate

Even when using the wizard, you will still have to manually request the certificate, and then tell the wizard where the certificate file resides, so the wizard can install it for use with Coexistence Manager for GroupWise.

To use the *Autodiscover Certificate Wizard* to install the necessary web services certificate using IIS 7.0–8.5:

1. In Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*): Click the **Autodiscover Certificate Wizard** button to launch the wizard.
2. Enter the information requested by the wizard until the wizard displays a window of data for you to copy to a certificate request form. Copy (Ctrl+a) the data.

   At this point the wizard will remain open, waiting for you to obtain the certificate. You can obtain a certificate from a local certification authority (CA) if you are using an on-premises Exchange server, or from a public CA (like Verisign or Microsoft Active Directory Certificate Services) if you are using Exchange in a hosted environment (e.g., Office 365).

   NOTE: If you need a multi-domain certificate: See To Create a SAN Certificate below.

   NOTE: You can request a certificate using Web enrollment pages. For more information, see http://support.microsoft.com/kb/931351.

3. Request and obtain the certificate (while the Coexistence Manager for GroupWise wizard waits).

   To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate. At some point you will paste into the request form the text you copied from the wizard (in step 2 above).

   To request a certificate from a local CA:

   a. From a web browser, enter ***https://<Local_Certification_Authority_computer>/certsrv***

b Click **Request a certificate**, then click **Advanced certificate request**.

c Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.

d Paste the text you copied from the wizard (in step 2 above) into the certificate request form.

e In the **Certificate Template** box, select **Web Server**.

f Click **Submit**.

g Select **Base 64 Encoded**, then select **Download certificate**.

4 Back in the *Autodiscover Certificate Wizard*: Click **Next**.

5 Specify the path and filename of the certificate file downloaded in step 3 above, and click **Finish** to register the file and dismiss the wizard.

To Manually Request and Install a Certificate Using IIS 7.0–8.5

To manually request a certificate using IIS 7.0–8.5:

1 From Internet Information Services, click **Server Certificates**.

2 From the Actions Pane, select **Create Certificate Request**.

3 Enter **autodiscover.<smtpdomain>** or **<smtpdomain>** for the primary domain and all required subdomains. Then click **Next**.

4 Accept the defaults, and click **Next**.

5 Specify the file name, and click **Finish**.

6 Request a certificate using a local CA or public CA.

To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate.

To request a certificate from a local CA:

a From a web browser, enter **https://<Local_Certification_Authority_computer>/certsrv**

b Click **Request a certificate**, then click **Advanced certificate request**.

c Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.

d Open the text file where you save the certificate request.

e Copy and paste the text from the certificate request into the **Saved Request** box when you selected Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

f In the **Certificate Template** box, select **Web Server**.

g Click **Submit**.

h Select **Base 64 Encoded**, then select **Download certificate**.

To manually install the certificate using IIS 7.0–8.5:

1 From Internet Information Services, click **Server Certificates**.

2 From the Actions Pane, select **Complete Certificate Request**.

3 Select the saved certificate file, and enter a friendly name for the certificate, then click **OK**.

NOTE: To create an https binding for the web site using IIS 7.0–8.5:

1 From the Connection Pane in IIS, select **QuestFreeBusy**.

2 From the Actions Pane, select **Bindings**.

3 Select **Add**. Select **https** as the type for a secure site, and enter the IP address and port number.

4 Select the SSL certificate to pass the certificate into the computer account, and click **View** to view any certificate information.

To Create a SAN Certificate

This procedure lets you configure a single certificate to answer for multiple addresses. This is obviously necessary for a multi-/subdomain configuration, but also, for a single-namespace environment, to create a certificate that will cover both Autodiscover and the root domain.

First, you *must* enable the SAN (Subject Alternate Name) flag on your CA. On the machine running CA services, run these commands at the command prompt to enable the flag:

```
certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
net stop certsvc
net start certsvc
```

When the SAN flag is enabled, you can create the certificate:

1 Open IIS on the machine running F/B and select the server. Scroll to the bottom, open **Server Certificates**, and click on **Create Certificate Request**.

2 For the common name, enter something appropriate for your larger domain. For example, for a domain *alejandro.xyzcorp.com*, the common name on the certificate is **.xyzcorp.com*. (This is somewhat generic, as we will later add specific namespaces to the certificate.)

3 Accept the defaults and enter a name for the request.

4 Open the certificate request you just created, and select and copy ***all*** of the text.

5 Open the certificate web enrollment page for the CA of your domain— e.g., *https://hostname/certsrv*. Then select **Request a Certificate**, and then select **Advanced Certificate Request**.

6 Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.

7 In the **Base-64-encoded certificate request** box, paste all of the text that you copied from the text file in step 4 above.

8 For the **Certificate Template**, select **Web Server**.

9 In the **Additional Attributes** box, enter any alternate-domain information in this format:

```
san:dns=dns.name[&dns=dns.name]
```

... with *&dns=dns.name* appended for each alternate domain you want the certificate to handle.

For a single-namespace environment: Enter the autodiscover and root domain, like this:

```
san:dns=autodiscover.xyzcorp.com&dns=xyzcorp.com
```

For a multi-/subdomain environment: You can enter as many domains as you like:

```
san:dns=autodiscover.sub1.xyzcorp.com
&dns=autodiscover.sub2.xyzcorp.com
&dns=autodiscover.sub3.xyzcorp.com
&dns=autodiscover.sub[...].xyzcorp.com
&dns=autodiscover.sub[n].xyzcorp.com
```

When you are finished, click **Submit**.

10 Select the **DER encoded** radio button, and then select **Download certificate chain**.

11 Enter a name for this.

12 Go back to IIS and click **Complete Certificate Request**.

13 For the **Filename** containing the certification authority's response, click the **Browse** button and select the certificate you just saved. (Be sure to change the file type to *.* instead of *.cer, or you won't see the file you saved—since it is a .P7B extension.) Type a friendly name that is easy to remember and identify so you can find your certificate on the list later. You should then see your new certificate on the list.

14 Select your new certificate and click **View**.

15 Click the **Details** tab, and scroll down to **Subject Alternative Name**. Highlight this field, and you should see all of your domains in the *Details* box.

Now bind your certificate to the HTTPS protocol on the QuestFreeBusy website:

1 On the Coexistence Manager for GroupWise F/B computer, in IIS Manager: Select **QuestFreeBusy**.

2 In the *Actions* pane on the right, select **Bindings**.

3 Select **https** and click **Edit**.

4 In the *Edit Site Binding* window, in the SSL certificate drop-down list: Select the certificate you just created.

5 Click **OK**.

4.3: Configure trusted sites for computers hosting F/B components

Log in as the Coexistence Manager for GroupWise account to be used with the F/B Connector (if you haven't already). Then, in **Internet Options** (via Windows Control Panel or IE **Tools**):

1 Click the *Security* tab, then select **Trusted sites** and click the **Custom level...** button.

2 In **Settings**, scroll down to **User Authentication | Logon**, and click the radio button for *Automatic logon with current user name and password*.

3 Click **OK** to save the selection and return to the *Security* tab.

4 Add the Exchange Server EWS and Autodiscover URLs to the **Trusted Sites**.

5 Click **OK** to save your new **Security** settings and dismiss the **Internet Options** dialog box.

4.4 (optional): Configure logging for F/B components

By default, Coexistence Manager for GroupWise is installed with the *log42net* utility to generate log files of Coexistence Manager for GroupWise components' system activity. This information is critical to diagnosing any problems that may arise. Logging is enabled by default for all Coexistence Manager for GroupWise components.

The default configurations will be suitable for almost all organizations and circumstances, but you can customize logging features if you like. The *log42net* utility may be configured to work a particular way with each Coexistence Manager for GroupWise component. Configuration instructions are nearly identical from one component to another, so we present those details separately, in Appendix C of the Coexistence Manager for GroupWise *User Guide* (not in this *FBC Configuration Guide*).

4.5: Configure Coexistence Manager for GroupWise's FBC for shared/single namespace (equivalent domains)

Coexistence Manager for GroupWise supports equivalent domain names (single, shared namespace) for GroupWise mail users and on-premises Exchange mail users. Equivalent domains are mapped to the primary domain in the Exchange server or GroupWise server. You can use a PowerShell cmdlet to perform this mapping:

- At the Coexistence Manager for GroupWise Web Server, open PowerShell and type:
  Set-CmgGroupWiseFreeBusyConfig -SmtpDomainMappings <*equivalentDomain*>=<*primaryDomain*>

And be sure to repeat the cmdlet for each equivalent domain.

4.6: Run Coexistence Manager for GroupWise's Management Console to configure FBC components

Use Coexistence Manager for GroupWise's Management Console to configure the Free/Busy Connector's components—to identify the participating servers and their locations, register the necessary account access credentials, and set other operating parameters and preferences. See chapter 4 of the Coexistence Manager for GroupWise *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

NOTE: You may use PowerShell commands to configure Coexistence Manager for GroupWise Free/Busy Connector components, instead of Coexistence Manager for GroupWise's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Appendix B in this *Guide*: Appendix: Configuring and troubleshooting the FBC with PowerShell.

Step 5: Configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server

To configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server:

5.1: Synchronize Office 365 and GroupWise directories

Before running any of Coexistence Manager for GroupWise's F/B Connector subcomponents, you must synchronize GroupWise users as Office 365 contacts, and Exchange users to GroupWise. Coexistence Manager for GroupWise's Directory Connector does not support directory synchronizations directly between GroupWise and Office 365. In this non-hybrid O365 scenario, however, you can configure Microsoft's *Azure AD Sync* synchronization tool to synchronize a local AD with Office 365. See Microsoft's *Azure AD Sync* tool documentation for instructions and guidance in configuring the *Azure AD Sync* tool for this purpose.

Make sure that the GroupWise SOAP web service is enabled (step 2 above), since that is also an environmental requirement for Coexistence Manager for GroupWise's Free/Busy Connector.

NOTE: GroupWise sometimes mistakenly generates F/B queries for addresses in the form *user-domain-com@domain.com* (instead of *user@domain.com*). Queries to such addresses will fail if AD does not recognize the address, so be sure to add that address form as an alias in AD for each Exchange user.

5.2: Configure Office 365 connections

Configure and verify the link from Office 365 to the domains/subdomains supported by the GroupWise server. This procedure tests whether the certificate on the Coexistence Manager for GroupWise Web Server is trusted by O365.

For FBC coexistence with Office 365, run *Enable-OrganizationCustomization*, and then create the availability address space by opening a PowerShell session and using the following commands:

```
$Credential = Get-Credential

$Session = New-PSSession -Credential $Credential -AllowRedirection -ConnectionUri
https://ps.outlook.com/PowerShell -Authentication Basic -ConfigurationName Microsoft.Exchange

Import-PSSession $Session
```

New-AvailabilityConfig –OrgWideAccount <username@domain.onmicrosoft.com>
[replace <username@domain.onmicrosoft.com> with your O365 admin account]

$domain = "<domain.onmicrosoft.com>"
[replace <domain.onmicrosoft.com> with your SMTP domain name in Office 365]

$adminUserId = "<username@domain.onmicrosoft.com>"
[replace <username@domain.onmicrosoft.com> with your O365 admin account]

$adminCredsId = "<username@domain.onmicrosoft.com>"
[replace <username@domain.onmicrosoft.com> with your O365 admin account]

$adminCredsPassword = "<YourPassword>"
[replace <YourPassword> with your Office 365 admin password]

$securePassword = ConvertTo-SecureString $adminCredsPassword -AsPlainText -Force

$adminCreds = New-Object
System.Management.Automation.PSCredential($adminCredsId,$securePassword)

Add-AvailabilityAddressSpace -AccessMethod OrgWideFB -ForestName <domain.com> -Credentials
$adminCreds –TargetAutodiscoverEpr 'https://autodiscover.<domain.com>/autodiscover/autodiscover.xml'
[replace <domain.com> with your SMTP domain name]

5.3: Configure DNS

Configure network load balancing (optional)

You can use Network Load Balancing to permit multiple web servers to handle Autodiscover requests. This is optional, *not* required to deploy Coexistence Manager for GroupWise. For more information, see this Microsoft article.

Configure DNS (Domain Name System)

Configure DNS to point *autodiscover.<smtpdomain.com>* to the computer where Coexistence Manager for GroupWise's Autodiscover service is installed. For each domain, Exchange connects to predefined Autodiscover URLs using DNS host entries.

For Exchange to get free/busy information from the domain supported by a GroupWise server, through the Coexistence Manager for GroupWise Free/Busy Connector, you must make the Coexistence Manager for GroupWise Autodiscover Web Service resolvable to this URL:

https://[autodiscover.]<smtpdomain>/autodiscover/autodiscover.xml

14

FBC Scenario #12

• GroupWise 8 or later via F/B Internet URL
• Office 365 (non-hybrid)
• In a multi-namespace environment

This procedure begins with the assumption that you have already reviewed the introductory chapter of this *FBC Configuration Guide* to Determine your FBC scenario. This chapter explains how to configure the FBC and the coexisting environments for F/B scenario #12, specified above.

Follow these steps, in order as presented here, to install and configure Coexistence Manager for GroupWise's F/B Connector for scenario #12:

- Step 1: Plan your FBC installation and configuration
- Step 2: Configure the GroupWise side
- Step 3: Configure the Office 365 side
- Step 4: Configure CMG's FBC Web Server
- Step 5: Configure and test connections among GroupWise, Exchange and CMG's FBC Web Server

Step 1: Plan your FBC installation and configuration

Review the System Requirements (in the Coexistence Manager for GroupWise *Release Notes*), and verify either that your environment conforms to the requirements, or that you will have the necessary hardware and software to meet the requirements.

1.1: Make a configuration map

Scan through the installation and configuration procedures in this chapter, and think through what this process will entail in your own environment, to accommodate your own needs and preferences. Identify any special circumstances or issues, and determine how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers, and how they will connect to the GroupWise and Exchange environments.

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers. If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed below. All Coexistence Manager for GroupWise Free/Busy Connector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit, as described in a later step in this chapter.

The typical deployment of FBC components to two computers for this scenario (GW 8 or later via F/B URL, with non-hybrid Office 365) is:

- On Coexistence Manager for GroupWise Server 1 (for GroupWise queries to Exchange, and Exchange replies):

    - Coexistence Manager for GroupWise Free/Busy Bridge
    - Coexistence Manager for GroupWise Exchange Free/Busy Service
- On Coexistence Manager for GroupWise Server 2 (for Exchange queries to GroupWise, and GroupWise replies):
    - Coexistence Manager for GroupWise GroupWise Free/Busy Service
    - Coexistence Manager for GroupWise Autodiscover
    - Coexistence Manager for GroupWise EWS

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted just above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

1.2: Complete the Coexistence Manager for GroupWise FBC Planning Worksheet

Use the worksheet in Appendix A of this *FBC Configuration Guide* to gather and organize the information you will need to enter into Coexistence Manager for GroupWise's Management Console application when configuring the Free/Busy Connector. You can print the worksheet to paper, and use a pen or pencil to write the information into the wide right margins.

The actual data-entry work will occur later in this procedure, in step 4.

Step 2: Configure the GroupWise side

GroupWise versions 8 and later can connect to Coexistence Manager for GroupWise's Free/Busy Connector via a F/B Internet URL.

FBC coexistence with any supported GroupWise version requires the GroupWise SOAP web service, enabled on the GroupWise Post Office where the Coexistence Manager for GroupWise service account resides. To enable and configure SOAP, see this Novell article, and this one too.

A later step of this FBC configuration procedure describes how to configure and test connections among Coexistence Manager for GroupWise FBC components and the GroupWise and Exchange environments.

Step 3: Configure the Office 365 side

To configure a non-hybrid Office 365 for Coexistence Manager for GroupWise's F/B Connector in a separate/multiple namespace environment:

1. In DNS, make sure the *coexist* domain has an A record pointing to Coexistence Manager for GroupWise.
2. Configure an Autodiscover website for Coexistence Manager for GroupWise (for example, *Autodiscover.x.y*, where the "*x.y*" domain is the SMTP address to the right of the @ symbol). The Coexistence Manager for GroupWise website must also have a matching certificate. (To obtain and install a matching certificate, see 4.2: Obtain and install web services certificates.)
3. Run the O365 A*dd-AvailabilityAddressSpace* cmdlet for the Coexistence Manager for GroupWise Autodiscover address.

4 Test the configuration: Open a web browser and enter the URL ("*https://Autodiscover.x.y/autodiscover/autodiscover.xml*") to verify that it resolves it correctly and without any certification errors.

To configure Office 365 for multiple subdomains

Coexistence Manager for GroupWise's Free/Busy Connector can facilitate the flow of free/busy information among multiple subdomains supported by both Office 365 and the GroupWise servers. To support this scenario, run the *Add-AvailabilityAddressSpace* cmdlet on Office 365 for each GroupWise SMTP domain supported.

Step 4: Configure Coexistence Manager for GroupWise's FBC Web Server

To configure Coexistence Manager for GroupWise's FBC Web Server:

4.1: Physically install the Coexistence Manager for GroupWise FBC components

For any given scenario and configuration, it is possible to install all Coexistence Manager for GroupWise F/B Connector components on a single server, as shown in the illustrations in the introductory chapter (*Determine your FBC scenario*) of this *Guide*. However, many production environments experience sufficient query volume to warrant separate servers to ensure optimal performance. The installation instructions here therefore describe how to install Coexistence Manager for GroupWise's F/B Connector on two servers.

See the configuration map you made in step 1 above to determine which components should be installed to which servers for this scenario.

If you prefer that all subcomponents reside on a single server, simply combine the components of *Coexistence Manager for GroupWise Server 1* and *Coexistence Manager for GroupWise Server 2* as they are listed in step 1 above. All Coexistence Manager for GroupWise Free/BusyConnector subcomponents are installed by the AutoRun utility included in the Coexistence Manager for GroupWise product kit.

IMPORTANT: ***Before you install,*** on any computer that will host any Coexistence Manager for GroupWise FBC web subcomponent, remove the IIS *DefaultWebSite*: In the navigation tree at left, right-click **DefaultWebSite**, and then select **Remove** from the pop-up menu. Coexistence Manager for GroupWise requires a dedicated server for its own web subcomponents.

Use the AutoRun utility now to install all the necessary Coexistence Manager for GroupWise F/B Connector subcomponents on the computer(s) where you want them installed.

IMPORTANT: ***Remember,*** the Coexistence Manager for GroupWise AutoRun installer must be run on the computer where you want to install a particular subcomponent. If you are deploying the F/B Connector to two different computers, you must run the AutoRun installer twice—once on each computer.

NOTE: The AutoRun installer automatically checks your environment to verify Coexistence Manager for GroupWise prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command string.

To configure Coexistence Manager for GroupWise's F/B Connector for multiple GroupWise servers

Remember: For Exchange queries for GroupWise F/B information, the simplest approach is to dedicate a separate Coexistence Manager for GroupWise FBC Server 2 (as noted in step 1 above, for Exchange queries to GroupWise, and GroupWise replies) for each GroupWise server, with all the Coexistence Manager for GroupWise servers feeding into the single Exchange server.

It is technically possible, but somewhat more complicated, to configure a single instance of the GroupWise FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple GroupWise servers—an approach that requires more elaborate GroupWise configurations.

4.2: Obtain and install web services certificates

Coexistence Manager for GroupWise Web Server components must support HTTPS to accept SSL connections. The server on which these components are installed must have a certificate that Exchange trusts. The single certificate must cover the primary domain and all subdomains supported by the GroupWise Server. The certificate covers the Autodiscover and EWS web services.

Coexistence Manager for GroupWise includes an *Autodiscover Certificate Wizard* to automate much of the process of installing this necessary certificate for the Free/Busy Connector. The wizard can be launched from Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*), as described in the procedure documented in the next subtopic below (see Using the Autodiscover Certificate Wizard to Obtain and Install a Certificate). Alternatively you can manually request and install a certificate, as described in the second subtopic below (see To Manually Request and Install a Certificate Using IIS 7.0–8.5).

Using the *Autodiscover Certificate Wizard* to Obtain and Install a Certificate

Even when using the wizard, you will still have to manually request the certificate, and then tell the wizard where the certificate file resides, so the wizard can install it for use with Coexistence Manager for GroupWise.

To use the *Autodiscover Certificate Wizard* to install the necessary web services certificate using IIS 7.0–8.5:

1 In Coexistence Manager for GroupWise's Management Console, on the *Quest Web Services* screen (under *GroupWise Free/Busy Connector*): Click the **Autodiscover Certificate Wizard** button to launch the wizard.

2 Enter the information requested by the wizard until the wizard displays a window of data for you to copy to a certificate request form. Copy (Ctrl+a) the data.

At this point the wizard will remain open, waiting for you to obtain the certificate. You can obtain a certificate from a local certification authority (CA) if you are using an on-premises Exchange server, or from a public CA (like Verisign or Microsoft Active Directory Certificate Services) if you are using Exchange in a hosted environment (e.g., Office 365).

> **NOTE: If you need a multi-domain certificate:** See To Create a SAN Certificate below.

> **NOTE:** You can request a certificate using Web enrollment pages. For more information, see http://support.microsoft.com/kb/931351.

3 Request and obtain the certificate (while the Coexistence Manager for GroupWise wizard waits).

To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate. At some point you will paste into the request form the text you copied from the wizard (in step 2 above).

To request a certificate from a local CA:

a From a web browser, enter ***https://<Local_Certification_Authority_computer>/certsrv***

b Click **Request a certificate**, then click **Advanced certificate request**.

c Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.

d Paste the text you copied from the wizard (in step 2 above) into the certificate request form.

e In the **Certificate Template** box, select **Web Server**.

f Click **Submit**.

g Select **Base 64 Encoded**, then select **Download certificate**.

4 Back in the *Autodiscover Certificate Wizard*: Click **Next**.

5 Specify the path and filename of the certificate file downloaded in step 3 above, and click **Finish** to register the file and dismiss the wizard.

To Manually Request and Install a Certificate Using IIS 7.0–8.5

To manually request a certificate using IIS 7.0–8.5:

1 From Internet Information Services, click **Server Certificates**.

2 From the Actions Pane, select **Create Certificate Request**.

3 Enter **autodiscover.<smtpdomain>** or **<smtpdomain>** for the primary domain and all required subdomains. Then click **Next**.

4 Accept the defaults, and click **Next**.

5 Specify the file name, and click **Finish**.

6 Request a certificate using a local CA or public CA.

To get a certificate from a public CA: Go to the web site of the public CA, and follow their instructions to request a certificate.

To request a certificate from a local CA:

a From a web browser, enter **https://<Local_Certification_Authority_computer>/certsrv**

b Click **Request a certificate**, then click **Advanced certificate request**.

c Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file**.

d Open the text file where you save the certificate request.

e Copy and paste the text from the certificate request into the **Saved Request** box when you selected Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

f In the **Certificate Template** box, select **Web Server**.

g Click **Submit**.

h Select **Base 64 Encoded**, then select **Download certificate**.

To manually install the certificate using IIS 7.0–8.5:

1 From Internet Information Services, click **Server Certificates**.

2 From the Actions Pane, select **Complete Certificate Request**.

3 Select the saved certificate file, and enter a friendly name for the certificate, then click **OK**.

NOTE: To create an https binding for the web site using IIS 7.0–8.5:

1 From the Connection Pane in IIS, select **QuestFreeBusy**.

2 From the Actions Pane, select **Bindings**.

3 Select **Add**. Select **https** as the type for a secure site, and enter the IP address and port number.

4 Select the SSL certificate to pass the certificate into the computer account, and click **View** to view any certificate information.

To Create a SAN Certificate

This procedure lets you configure a single certificate to answer for multiple addresses. This is obviously necessary for a multi-/subdomain configuration, but also, for a single-namespace environment, to create a certificate that will cover both Autodiscover and the root domain.

First, you *must* enable the SAN (Subject Alternate Name) flag on your CA. On the machine running CA services, run these commands at the command prompt to enable the flag:

```
certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
net stop certsvc
net start certsvc
```

When the SAN flag is enabled, you can create the certificate:

1. Open IIS on the machine running F/B and select the server. Scroll to the bottom, open **Server Certificates**, and click on **Create Certificate Request**.
2. For the common name, enter something appropriate for your larger domain. For example, for a domain *alejandro.xyzcorp.com*, the common name on the certificate is **.xyzcorp.com*. (This is somewhat generic, as we will later add specific namespaces to the certificate.)
3. Accept the defaults and enter a name for the request.
4. Open the certificate request you just created, and select and copy ***all*** of the text.
5. Open the certificate web enrollment page for the CA of your domain— e.g., *https://hostname/certsrv*. Then select **Request a Certificate**, and then select **Advanced Certificate Request**.
6. Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.
7. In the **Base-64-encoded certificate request** box, paste all of the text that you copied from the text file in step 4 above.
8. For the **Certificate Template**, select **Web Server**.
9. In the **Additional Attributes** box, enter any alternate-domain information in this format:

   ```
   san:dns=dns.name[&dns=dns.name]
   ```

   ... with *&dns=dns.name* appended for each alternate domain you want the certificate to handle.

   For a single-namespace environment: Enter the autodiscover and root domain, like this:

   ```
   san:dns=autodiscover.xyzcorp.com&dns=xyzcorp.com
   ```

   For a multi-/subdomain environment: You can enter as many domains as you like:

   ```
   san:dns=autodiscover.sub1.xyzcorp.com
   &dns=autodiscover.sub2.xyzcorp.com
   &dns=autodiscover.sub3.xyzcorp.com
   &dns=autodiscover.sub[...].xyzcorp.com
   &dns=autodiscover.sub[n].xyzcorp.com
   ```

   When you are finished, click **Submit**.
10. Select the **DER encoded** radio button, and then select **Download certificate chain**.
11. Enter a name for this.
12. Go back to IIS and click **Complete Certificate Request**.
13. For the **Filename** containing the certification authority's response, click the **Browse** button and select the certificate you just saved. (Be sure to change the file type to *.* instead of *.cer, or you won't see the file you saved—since it is a .P7B extension.) Type a friendly name that is easy to remember and identify so you can find your certificate on the list later. You should then see your new certificate on the list.
14. Select your new certificate and click **View**.
15. Click the **Details** tab, and scroll down to **Subject Alternative Name**. Highlight this field, and you should see all of your domains in the *Details* box.

Now bind your certificate to the HTTPS protocol on the QuestFreeBusy website:

1. On the Coexistence Manager for GroupWise F/B computer, in IIS Manager: Select **QuestFreeBusy**.
2. In the *Actions* pane on the right, select **Bindings**.
3. Select **https** and click **Edit**.
4. In the *Edit Site Binding* window, in the SSL certificate drop-down list: Select the certificate you just created.
5. Click **OK**.

4.3: Configure trusted sites for computers hosting F/B components

Log in as the Coexistence Manager for GroupWise account to be used with the F/B Connector (if you haven't already). Then, in **Internet Options** (via Windows Control Panel or IE **Tools**):

1. Click the *Security* tab, then select **Trusted sites** and click the **Custom level...** button.
2. In **Settings**, scroll down to **User Authentication | Logon**, and click the radio button for *Automatic logon with current user name and password*.
3. Click **OK** to save the selection and return to the *Security* tab.
4. Add the Exchange Server EWS and Autodiscover URLs to the **Trusted Sites**.
5. Click **OK** to save your new **Security** settings and dismiss the **Internet Options** dialog box.

4.4 (optional): Configure logging for F/B components

By default, Coexistence Manager for GroupWise is installed with the *log42net* utility to generate log files of Coexistence Manager for GroupWise components' system activity. This information is critical to diagnosing any problems that may arise. Logging is enabled by default for all Coexistence Manager for GroupWise components.

The default configurations will be suitable for almost all organizations and circumstances, but you can customize logging features if you like. The *log42net* utility may be configured to work a particular way with each Coexistence Manager for GroupWise component. Configuration instructions are nearly identical from one component to another, so we present those details separately, in Appendix C of the Coexistence Manager for GroupWise *User Guide* (not in this *FBC Configuration Guide*).

4.5: Run Coexistence Manager for GroupWise's Management Console to configure FBC components

Use Coexistence Manager for GroupWise's Management Console to configure the Free/Busy Connector's components—to identify the participating servers and their locations, register the necessary account access credentials, and set other operating parameters and preferences. See chapter 4 of the Coexistence Manager for GroupWise *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

> **NOTE:** You may use PowerShell commands to configure Coexistence Manager for GroupWise Free/Busy Connector components, instead of Coexistence Manager for GroupWise's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Appendix B in this *Guide*: Appendix: Configuring and troubleshooting the FBC with PowerShell.

Step 5: Configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server

To configure and test connections among GroupWise, Exchange and Coexistence Manager for GroupWise's FBC Web Server:

5.1: Synchronize Exchange and GroupWise directories

Before running any of Coexistence Manager for GroupWise's F/B Connector subcomponents, you must synchronize GroupWise users as Office 365 contacts, and Exchange users to GroupWise. Coexistence Manager for GroupWise's Directory Connector does not support directory synchronizations directly between GroupWise and Office 365. In this non-hybrid O365 scenario, however, you can configure Microsoft's *Azure AD Sync* synchronization tool to synchronize a local AD with Office 365. See Microsoft's *Azure AD Sync* tool documentation for instructions and guidance in configuring the *Azure AD Sync* tool for this purpose.

Make sure that the GroupWise SOAP web service is enabled (step 2 above), since that is also an environmental requirement for Coexistence Manager for GroupWise's Free/Busy Connector.

NOTE: GroupWise sometimes mistakenly generates F/B queries for addresses in the form *user-domain-com@domain.com* (instead of *user@domain.com*). Queries to such addresses will fail if AD does not recognize the address, so be sure to add that address form as an alias in AD for each Exchange user.

5.2: Configure Office 365 connections

Configure and verify the link from Office 365 to the domains/subdomains supported by the GroupWise server. This procedure tests whether the certificate on the Coexistence Manager for GroupWise Web Server is trusted by O365.

For FBC coexistence with Office 365, run *Enable-OrganizationCustomization*, and then create the availability address space by opening a PowerShell session and using the following commands:

```
$Credential = Get-Credential

$Session = New-PSSession -Credential $Credential -AllowRedirection -ConnectionUri
https://ps.outlook.com/PowerShell -Authentication Basic -ConfigurationName Microsoft.Exchange

Import-PSSession $Session

New-AvailabilityConfig –OrgWideAccount <username@domain.onmicrosoft.com>
[replace <username@domain.onmicrosoft.com> with your O365 admin account]

$domain = "<domain.onmicrosoft.com>"
[replace <domain.onmicrosoft.com> with your SMTP domain name in Office 365]

$adminUserId = "<username@domain.onmicrosoft.com>"
[replace <username@domain.onmicrosoft.com> with your O365 admin account]

$adminCredsId = "<username@domain.onmicrosoft.com>"
[replace <username@domain.onmicrosoft.com> with your O365 admin account]

$adminCredsPassword = "<YourPassword>"
[replace <YourPassword> with your Office 365 admin password]

$securePassword = ConvertTo-SecureString $adminCredsPassword -AsPlainText -Force
```

$adminCreds = New-Object
System.Management.Automation.PSCredential($adminCredsId,$securePassword)

Add-AvailabilityAddressSpace -AccessMethod OrgWideFB -ForestName <domain.com> -Credentials $adminCreds –TargetAutodiscoverEpr 'https://autodiscover.<domain.com>/autodiscover/autodiscover.xml'
[replace <domain.com> with your SMTP domain name]

5.3: Configure DNS

Configure network load balancing (optional)

You can use Network Load Balancing to permit multiple web servers to handle Autodiscover requests. This is optional, *not* required to deploy Coexistence Manager for GroupWise. For more information, see this Microsoft article.

Configure DNS (Domain Name System)

Configure DNS to point *autodiscover.<smtpdomain.com>* to the computer where Coexistence Manager for GroupWise's Autodiscover service is installed. For each domain, Exchange connects to predefined Autodiscover URLs using DNS host entries.

For Exchange to get free/busy information from the domain supported by a GroupWise server, through the Coexistence Manager for GroupWise Free/Busy Connector, you must make the Coexistence Manager for GroupWise Autodiscover Web Service resolvable to this URL:

https://[autodiscover.]<smtpdomain>/autodiscover/autodiscover.xml

15

Appendix: FBC Planning Worksheet

Use this worksheet to gather and organize the information you will need to enter into Coexistence Manager for GroupWise's Management Console application to configure the Free/Busy Connector (FBC).

This worksheet is designed with wide right margins, to leave you room to write in the information you are gathering and any pertinent notes.

GroupWise Coexistence Manager for GroupWise Router | Coexistence Manager for GroupWise Router Service

This information applies only if you are connecting to GroupWise 7, or if you have GroupWise 8 and will connect to CMG via the API Gateway (which requires the Coexistence Manager for GroupWise Router).

The first fields in the Management Console screen specify the folders where the Coexistence Manager for GroupWise Router will send or look for various items for its routing functions. In Coexistence Manager for GroupWise's Management Console you can use **Browse** buttons to find and select directories.

- **Novell Account:** Novell account login user name.
- **Password:** Password associated with the **Novell Account** cited above.
- **Check For New Requests Every ____ Seconds:** Polling frequency for F/B queries. The interval (in seconds) the Router will wait between successive checks to see if there is a new query to process.
- **Request Retry Duration:** Number of minutes the Coexistence Manager for GroupWise Router Service will continue trying to move a file (message), if preceding attempt(s) have failed. The service repeats such attempts at intervals specified by the **Check For New Requests** value above, until successful or until the **Request Retry Duration** is reached.
- **Update Performance Counters Every ____ Seconds:** Update frequency for the F/B performance counters that feed Windows' System Monitor feature.
- **Enable Performance Counters:** A checkbox to indicate whether you want the F/B Connector performance counters to run.

Exchange F/B Connector | Bridge

This information applies only for an Exchange-to-GroupWise connector, and only if you are connecting to GroupWise 8 and have chosen the original, shared-address-book configuration. Coexistence Manager for GroupWise uses this information to configure its Bridge web service, for GroupWise queries for Exchange F/B information.

Requests Directory: Specify the folder where F/B requests will be held. In Coexistence Manager for GroupWise's Management Console you can use a **Browse** button to find and select a directory.

Results Directory: Specify the folder where F/B results will be held. In Coexistence Manager for GroupWise's Management Console you can use a **Browse** button to find and select a directory.

Check For New Requests Every ____ Seconds: Polling frequency. How long the Bridge will wait between successive checks to see if there is a new F/B query to process.

Time Zone for GroupWise API Gateway server: In Coexistence Manager for GroupWise's Management Console you can use a drop-down list box to select the correct time zone.

Quest Exchange Free/Busy Connector Host Name is prefilled by Coexistence Manager for GroupWise with *localhost*—the appropriate value for a typical Coexistence Manager for GroupWise configuration. In a typical configuration, the Coexistence Manager for GroupWise Bridge is installed on the same computer as the Coexistence Manager for GroupWise Exchange Free/Busy Connector service, so the generic relative value *localhost* will suffice in this context. If the Coexistence Manager for GroupWise Bridge is installed on a different computer, then enter the correct **Host Name** here.

Exchange F/B Connector | Exchange Free/Busy

This information is necessary to configure Coexistence Manager for GroupWise's Exchange F/B Connector service, for GroupWise queries for Exchange F/B information.

Exchange Server Location: How should F/B queries be routed to the coexisting Exchange environment? By **EWS Endpoint**, by **Autodiscover Endpoint**, or by **Autodiscover Only**?

All queries for Exchange users' F/B information must pass through an Exchange EWS, which facilitates communications between Exchange and the Coexistence Manager for GroupWise Exchange FBC service. In an Exchange environment with a single EWS at a known fixed location (URL), you can point the FBC service directly to the EWS by specifying the EWS URL and host name. If there is no single Exchange EWS with a known fixed location, the FBC service can query the Exchange Autodiscover service, which tracks and reports the current location of an available EWS.

If you will coexist with an Exchange environment where you don't know the location of either the EWS or the Autodiscover endpoint, the Coexistence Manager for GroupWise FBC service will have to search the network for the connection it needs.

Specify your choice by selecting one of these methods:

- **EWS Endpoint:** Select this option if you have an on-premises Exchange with a single Exchange EWS whose location (URL) is fixed relative to Coexistence Manager for GroupWise's Exchange FBC service. This approach typically yields the best performance of the three options, but is the least flexible since the connection will fail if the Exchange EWS is not at the specified URL. If you select this option, you must also specify:
  - **Exchange EWS Host Name:** Name of the Exchange server where EWS requests should be sent.
  - **EWS URL:** Location of Microsoft EWS web service on the Exchange server.
- **Autodiscover Endpoint:** Select this option if you have an on-premises Exchange environment with multiple Exchange EWS endpoints (for example, in a load-balanced environment) and you have an Exchange Autodiscover service that can determine which EWS endpoint to use. This can also be the best choice if you want to coexist with Microsoft's hosted Office 365 (see the Office 365 notes below). Performance will be slower than if you direct the FBC service to a fixed-location EWS (above), but will still be faster than if neither the EWS nor the Autodiscover value is specified (below). For this option, you must also specify:
  - **Exchange Autodiscover URL:** Location of the Autodiscover service on the Exchange server (or, for Office 365, of Microsoft's Autodiscover URL, as noted below).

  NOTE: ***If coexisting with Microsoft's Office 365:*** Select the **Autodiscover Endpoint** option and set the **Exchange Autodiscover URL** to Microsoft's Autodiscover URL:

  https://autodiscover-s.outlook.com/autodiscover/autodiscover.svc

  Note, however, that this is a Microsoft URL that is subject to change, in which case this connection would fail and the Free/Busy Connector would fail. Remember this if you set the Exchange Autodiscover URL to the Microsoft URL, and Coexistence Manager for GroupWise's F/B Connector works fine for a time but then suddenly and consistently fails. The most likely cause is a change in Microsoft's Autodiscover URL. Contact Microsoft to get the new URL, or select the **Autodiscover Only** option (below) instead.
- **Autodiscover Only:** Select this option if you will coexist with an Exchange environment where you don't know the location of either the EWS or Autodiscover. In this case, the FBC service will search the network

for the connection it needs, so this is the most flexible option, but it is also much slower than either alternative above.

Regardless of your selection for **Exchange Server Location**, Coexistence Manager for GroupWise's Management Console will ask for all of the information listed below.

Exchange Online: Mark this checkbox only if you are configuring coexistence with Microsoft's Office 365 hosted Exchange services. If you are configuring coexistence with a local, on-premises Exchange server, make sure this checkbox is *un*marked.

Exchange Username (only if the Coexistence Manager for GroupWise admin computer and the Exchange environment are in different domains): The **Username** for the administrator account the F/B Connector will use to access data and features in Exchange.

> **IMPORTANT:** Leave these **Exchange Username** and **Exchange Password** fields empty unless you are coexisting with a hosted Exchange (such as Office 365), or with a local on-premises Exchange that isn't in the same domain as the Coexistence Manager for GroupWise admin server. But if Coexistence Manager for GroupWise resides in a different domain from Exchange, then entries here are mandatory.

Exchange Password (only if the Coexistence Manager for GroupWise admin computer and the Exchange environment are in different domains): The **Password** associated with the **Exchange Username** cited above.

Show Tentative As Busy: Select **Yes** or **No** to determine whether *Tentative* F/B status in Outlook should appear as *Busy* in GroupWise.

GroupWise F/B Connector | GroupWise Free/Busy

This information is necessary to configure Coexistence Manager for GroupWise's GroupWise F/B Connector service, for Exchange queries for GroupWise F/B information.

GroupWise Soap Service Host Name: IP address or full DNS hostname for the GroupWise server.

GroupWise Soap Service Port Number: The SOAP port for the GroupWise server. Coexistence Manager for GroupWise prefills this field with the GroupWise default, 7191, but be sure to change it if your SOAP service is assigned to a different port.

GroupWise Request Retry Delay: Number of seconds to wait between retrying Free/Busy requests to the GroupWise system. This number should be significantly less than the **GroupWise Request Timeout** value (below).

GroupWise Request Timeout: Number of seconds the GroupWise Free/Busy Connector should run before timing out and returning the results it has obtained up until the timeout. Note that Outlook Free/Busy requests timeout at about 25 seconds so this number should be a few seconds less than that.

GroupWise User Name: User name for the GroupWise SOAP logon process.

GroupWise Trusted Application Name: Name of the trusted application (for example, *QuestFreeBusy*) by which the **GroupWise User Name** specified above will access the GroupWise Post Office.

- **GroupWise Trusted Application Key:** An authentication code that permits access to GroupWise data and features by the **GroupWise User Name** specified above. This **Key** is associated with a particular **Trusted Application Name**, specified in the field above. You can create the key with ConsoleOne (in GroupWise 8.01 SP1 or later), or simply run a command from the Windows command prompt:
  - For GroupWise 7 or 8, enter: \Quest\Quest Coexistence Manager for GroupWise\TrustedApplication\GroupWise8\CreateTrustedKey8.exe
  - Or for GroupWise 2012, enter: \Quest\Quest Coexistence Manager for GroupWise\TrustedApplication\GroupWise2012\CreateTrustedKey2012.exe

SMTP Domain Mappings: Used when the domain specified in GroupWise for a user's email address is different from the domain specified for the same GroupWise user on an Exchange system. For example, if the user's email address in GroupWise is *JohnSmith@ gwsitraka.com*, and his email address in Exchange is *JohnSmith@exsitraka.com*, then an SMTP domain mapping would be created for *exsitraka.com=gwsitraka.com*. Then when Outlook does a F/B search for *JohnSmith@exsitraka.com*, the Coexistence Manager for GroupWise

F/B Connector translates it as a request to GroupWise for *JohnSmith@gwsitraka.com*. SMTP Domain Mappings are used only for Exchange-to-GroupWise F/B queries.

GroupWise F/B Connector | Quest Web Services

This information applies only if you are configuring Coexistence Manager for GroupWise's FBC for Outlook 2003 clients, which requires Coexistence Manager for GroupWise's Autodiscover and EWS for Exchange queries to GroupWise for F/B information. This information does ***not*** apply if you are configuring for Outlook 2007 or later clients, with Microsoft's (not Coexistence Manager for GroupWise's) Autodiscover and EWS.

- **Web Service Prefix:** The first element of the **Autodiscover Url** (below) for CMG's Autodiscover web service. The default value is *autodiscover*, but you can designate an alternate web service prefix for the GroupWise Free/Busy Connector. This field accommodates F/B coexistence with Exchange 2013 or Office 365 (Wave 14 or 15), where the prefix is configurable.
- **Web Service Host Name:** From the Autodiscover Host *A Record*, this is the **Host Name** obtained from your DNS configuration entries in an earlier step of the configuration. (See the *Configure DNS* step of your scenario's configuration instructions for more information.) This field is prefilled by Coexistence Manager for GroupWise, assuming the Autodiscover service is installed on the same computer as the Coexistence Manager for GroupWise GroupWise Free/Busy Connector service, but the value may be edited for a non-standard configuration.
- The **Quest Autodiscover Url** and **Quest EWS Url** fields are both filled by Coexistence Manager for GroupWise, derived from the **Web Service Prefix** and **Web Service Host Name** values (above), and cannot be changed.
- **Autodiscover Certificate Wizard:** Button to launch the wizard, which automates much of the process of installing the necessary autodiscover certificate for the Free/Busy Connector. (For more information about this wizard, see the *web services certificates* step of your scenario's configuration instructions.)
- **Quest GroupWise Free/Busy Connector Host Name:** Prefilled by Coexistence Manager for GroupWise with *localhost*—the appropriate value for a typical Coexistence Manager for GroupWise configuration. In a typical configuration, the Coexistence Manager for GroupWise EWS subcomponent is installed on the same computer as the Coexistence Manager for GroupWise GroupWise Free/Busy Connector service, so the generic relative value *localhost* will suffice in this context. If the Coexistence Manager for GroupWise EWS is installed on a different computer, then enter the correct **Host Name** here.

  In either case, Coexistence Manager for GroupWise derives the **Endpoint** field value from the **Host Name** value. The **Endpoint** field value cannot be edited.

16

Appendix: Configuring and troubleshooting the FBC with PowerShell

You may use these PowerShell commands (instead of Coexistence Manager for GroupWise's Management Console) to configure Coexistence Manager for GroupWise Free/Busy Connector subcomponents and/or troubleshoot F/B Connector issues.

- Commands to configure the F/B Connector
- Commands to troubleshoot the F/B Connector

Commands to configure the F/B Connector

Note that for every set-cmg* command listed here, there is a corresponding get-cmg* command that takes no parameters.

Table 3.

Command	Parameter
Set-CmgAutodiscoverConfig	[-CMxEwsUrl] <String> [-IsRedirectEnabled]

- **CMxEwsUrl:** The URL of the EWS (i.e., Availability) service.
- **IsRedirectEnabled:** $True or $False. Is Autodiscover redirection enabled or not?

Table 4.

Command	Parameter
Set-CmgAvailabilityConfig	[[-HostName] <String>] [[-PortNumber] <Int32>]

- **HostName:** Name of server hosting the GroupWise F/B Connector Service.
- **PortNumber:** Port number the GroupWise F/B Connector Service is located on.

Table 5.

Command	Parameter
Set-CmgExchangeFreeBusyConfig	[[-HostName] <String>] [[-PortNumber] <Int32>] [-ShowTentativeAsBusy] [[-ExchangeEwsUrl] <String>] [[-Credentials] <PSCredential>] [-ValidateRedirect] [[-ValidRedirectUrlList] <String[]>]

- **HostName:** Name of the server hosting Exchange F/B Connector Service.
- **PortNumber:** Port number the Exchange F/B Connector Service is located on.
- **ShowTentativeAsBusy:** $True or $False. Show Tentative Busy as Busy?
- **ExchangeEwsUrl:** The URL of the Exchange Web Service.
- **Credentials:** Credentials to access the Exchange Service. Use *Get-Credential* to get the credentials.
- **ValidateRedirect:** $True or $False. Can Autodiscover redirect to a different domain?
- **ValidRedirectUrlList:** Comma-separated list of valid EWS URLs to which Autodisover can redirect.

Table 6.

Command	Parameter
Set-CmgFreeBusyBridgeConfig	[[-ExchangeFreeBusyServiceHostName] <String>] [[-ExchangeFreeBusyPortNumber] <Int32>] [[-DaysOfFreeBusy] <UInt32>]

- **ExchangeFreeBusyServiceHostName:** Name of the server hosting the Exchange F/B Connector Svc.
- **ExchangeFreeBusyPortNumber:** Port number of the Exchange F/B Connector Service.
- **DaysOfFreeBusy:** Number of days of F/B to be retrieved from Exchange.

Table 7.

Command	Parameter
Set-CmgGroupWiseFreeBusyConfig	[[-QuestFreeBusyServiceHostName] <String>] [[-QuestFreeBusyServicePortNumber] <Int32>] [[-GroupWiseSoapServiceHostName] <String>] [[-GroupWiseSoapServicePortNumber] <Int32>] [[-SmtpDomainMappings] <String[]>] [[-SessionLoginName] <String>] [[-TrustedApplicationKey] <SecureString>] [[-TrustedApplicationName] <String>] [[-GroupWiseRetryDelayInSeconds] <Int32>] [[-GroupWiseTimeoutInSeconds] <Int32>]

- **QuestFreeBusyServiceHostName:** Name of the server where the GroupWise F/B Connector Svc resides.
- **QuestFreeBusyServicePortNumber:** Port for the GroupWise F/B Connector Service.
- **GroupWiseSoapServiceHostName:** Name of the server hosting the GroupWise SOAP service.
- **GroupWiseSoapServicePortNumber:** Port for the GroupWise SOAP service.
- **SmtpDomainMappings:** Comma separated list of SMTP domain mappings.
- **SessionLoginName:** User name for the GroupWise SOAP logon.
- **TrustedApplicationKey:** The key must be entered as a SecureString, so use the following PowerShell command to create the key:

  ```
  $key = Read-Host "Enter Key" –AsSecureString
  ```

- **TrustedApplicationName:** Name of the Trusted Application.
- **GroupWiseRetryDelayInSeconds:** Number of seconds to wait between retrying F/B requests to GroupWise. This number should be significantly less than the *GroupWiseTimeoutInSeconds* value.
- **GroupWiseTimeoutInSeconds:** Number of seconds the GroupWise connector service should run before timing out and returning the results it has obtained up until the timeout. Note that Outlook Free/Busy requests timeout at 25 seconds, so this number should be a few seconds less than that.

Commands to troubleshoot the F/B Connector

To get F/B info for an Exchange user via the FreeBusyBridge Web Service:

Table 8.

Command	Parameter
Get-CmgFreeBusyBridge	[-WebServerName] <String> [-UserEmailAddress] <String>

- **WebServerName:** Name of server where FreeBusyBridge Web Service resides.
- **UserEmailAddress:** Email address for whom to get F/B info from Exchange.

To get F/B info for an Exchange user via the Exchange F/B Connector Service:

Table 9.

Command	Parameter
Get-CmgExchangeFreeBusy	[-UserEmailAddress] <String> [-StartDate] <DateTime> [-EndDate] <DateTime>

- **UserEmailAddress:** Email address of an Exchange user.
- **StartDate:** Starting date for the F/B search.
- **EndDate:** Ending date for the F/B search.

To get F/B info for a group of GroupWise users via the GroupWise F/B Connector Service:

Table 10.

Command	Parameter
Get-CmgGroupWiseFreeBusy	[-UserEmailAddresses] <String[]> [-StartDate] <DateTime> [-EndDate] <DateTime>

- **UserEmailAddresses:** List of email addresses of GroupWise users.
- **StartDate:** Starting date for the F/B search.
- **EndDate:** Ending date for the F/B search.

To get the URL of the Exchange Availability Web Service (EWS):

Table 11.

Command	Parameter
Get-CmgExchangeWebServicesUrl	[-EmailAddress] <String> [-Credentials <PSCredential>]

- **EmailAddress:** Email address of an Exchange user.
- **Credentials:** Credentials to access the Exchange Service. Use *Get-Credential* to get the credentials.

17

Appendix: Troubleshooting the FBC

This Appendix describes the most common problems encountered when installing and using Coexistence Manager for GroupWise's FBC, and provides suggestions and procedures that are most likely to resolve them. Many issues can be resolved quickly by reviewing this short list of preliminary checks before calling Quest Support:

- **Review the component log file(s).** You can find valuable information about component errors and warnings in the components' respective log files. If you call Quest Support and a support engineer can't immediately identify the problem, typically he/she will ask for copies of your log files.
- **Verify system requirements.** Coexistence Manager for GroupWise problems are often traced back to inconsistencies between the product's System requirements and the host network's hardware or software specifications. You may therefore save yourself some time and trouble by simply comparing your local system to the Coexistence Manager for GroupWise system requirements. System requirements are documented in the *Release Notes* that accompany each release.
- **Always ask yourself:**
  - **Is this a known limitation or known issue?** Check the *Known Limitations* appendix of the Coexistence Manager for GroupWise *User Guide*, and the *Known Issues* section of the current Coexistence Manager for GroupWise *Release Notes*, to see whether the problem might simply be a known limitation of the process.
  - **What has changed since the last server restart?** Configuration values are normally updated only when a service is restarted. This can hide a pending problem for weeks or longer until an administrator restarts the services and the changes are applied.

This troubleshooting information is organized in sections by the conditions and symptoms of various problems:

Outlook crashes upon F/B lookup

If an Outlook client repeatedly crashes during F/B lookups, and you are running an Exchange 2007 or Exchange 2010 Client Access Server, the cause may be a known issue in the combination of .NET Framerwork 3.5 SP1 and .NET Framework 2.0 SP2. For more information, see Microsoft's KnowledgeBase article, and Microsoft Support can point you to a HotFix to resolve this problem.

GroupWise-to-Exchange F/B query connection fails with Office 365

If you are coexisting with Office 365, and Coexistence Manager for GroupWise's F/B Connector works fine for a time but then suddenly and consistently fails, the most likely cause is a change in Microsoft's Autodiscover URL.

Our configuration instructions for the F/B Connector (see Management Console screen: Exchange F/B Connector | Exchange Free/Busy) suggest that, for Office 365, you select the **Autodiscover Endpoint** connection method, and set the **Exchange Autodiscover URL** field to this Microsoft URL:

https://autodiscover-s.outlook.com/autodiscover/autodiscover.svc

But this is a Microsoft URL that is subject to change, in which case the connection would fail and the Free/Busy Connector would fail. In that case, contact Microsoft to get the new URL, or select the **Autodiscover Only** method instead.

Outlook users get certificate errors when logging into Outlook

If Outlook users get certificate errors when logging into Outlook, after Coexistence Manager for GroupWise's F/B Connector has been configured, the most likely cause is a name mismatch in the certificate. Check to verify that the certificate in use on the Exchange server for port 443 is accepting all required named domains. If the error shows a name mismatch, the certificate may not have the required domain.

Exchange free/busy errors

To troubleshoot errors retrieving free/busy information from Exchange, you can use these PowerShell cmdlets:

To get F/B info for an Exchange user via the Exchange F/B Connector Service:

Table 12.

command	parameter
Get-CmgExchangeFreeBusy	[-UserEmailAddress] <String> [-StartDate] <DateTime> [-EndDate] <DateTime>

- **UserEmailAddress:** Email address of an Exchange user.
- **StartDate:** Starting date for the F/B search.
- **EndDate:** Ending date for the F/B search.

To get F/B info for an Exchange user via the FreeBusyBridge Web Service:

Table 13.

command	parameter
Get-CmgFreeBusyBridge	[-WebServerName] <String> [-UserEmailAddress] <String>

- **WebServerName:** Name of server where FreeBusyBridge Web Service resides.
- **UserEmailAddress:** Email address for whom to get F/B info from Exchange.

These cmdlets retrieve free/busy information for one or more users directly from Exchange using the same code used by the Exchange F/B Connector Service or Bridge Web Service. The cmdlets can be used to narrow down whether the problem is retrieving Free/Busy information from Exchange, or the configuration of the Bridge, or of the Autodiscover service or EWS.

GroupWise free/busy errors

To troubleshoot errors retrieving Free/Busy information from GroupWise, you can use the *Get-CmgGroupWiseFreeBusy* cmdlet. This cmdlet will retrieve F/B information for one or more users using the Coexistence Manager for GroupWise Mail Connector service.

To get F/B info for a group of GroupWise users via the GroupWise F/B Connector Service:

Table 14.

command	parameter
Get-CmgGroupWiseFreeBusy	[-UserEmailAddresses] <String[]> [-StartDate] <DateTime> [-EndDate] <DateTime>

- **UserEmailAddresses:** List of email addresses of GroupWise users.
- **StartDate:** Starting date for the F/B search.
- **EndDate:** Ending date for the F/B search.

This cmdlet can be used to narrow down whether the problem is retrieving Free/Busy information from GroupWise, or the configuration of the Autodiscover or Availability web services.

"Unable to generate a temporary class" error when attempting Exchange-to-GroupWise F/B query

An Exchange-to-GroupWise F/B query will generate this error:

> Microsoft.Exchange.InfoWorker.Common.Availability.ProxyWebRequestProcessing Exception: System.Web.Services.Protocols.SoapException: Server was unable to process request. ---> Unable to generate a temporary class (result=1).
>
> error CS2001: Source file 'C:\Windows\TEMP\cqywcsxm.0.cs' could not be found
>
> error CS2008: No inputs specified

... if the IIS_IUSRS user does not have **List folder / read data** permission. To resolve this, grant the user that **List folder / read data** permission.

Outlook/OWA users cannot see free/busy information for GroupWise users

On the Exchange server

- Verify that *Add-AvailabilityAddressSpace* has been executed on the Exchange server. To see if the cmdlet has run, type on the Exchange Management Console: *Get-AvailabilityAddressSpace*

  If you need to run the cmdlet to coexist with an on-premises Exchange:

  > Add-AvailabilityAddressSpace -ForestName <*YourDomain.com*> -AccessMethod OrgWideFB -Credentials $adminCreds -UseServiceAccount $true

  Or, if coexisting with Office 365:

  > Add-AvailabilityAddressSpace -ForestName <*YourDomain.com*> -AccessMethod OrgWideFB -Credentials $adminCreds -UseServiceAccount <*AccountName*> -TargetAutodiscoverEpr 'https://autodiscover.<*YourDomain.com*>/autodiscover/autodiscover.xml'

- Ensure you can ping <*smtpdomain*> or *autodiscover.*<*smtpdomain*> and that it resolves to the computer running the Coexistence Manager for GroupWise F/B Connector.

- Open a web browser such as Internet Explorer and type *https://<host>/autodiscover/autodiscover.xml* (where <*host*> is either <*smtpdomain*> or *autodiscover.*<*smtpdomain*>), and ensure an .xml file appears and that you do not have any certificate errors.
    - If the .xml file displayed has the text "**this is a placeholder file**", then IIS is not properly configured with an XML Handler.

To configure IIS 7.0–8.5 with Integrated Application pools

1. Open IIS Manager for IIS. Expand the root node and click **Application Pools**.
2. Ensure the Managed Pipeline mode for *CMxAutodiscoverAppPool* and *CMxEWSAppPool* are both set to **Integrated**.
3. Access *https://<host>/autodiscover/autodiscover.xml*, and ensure you do not see the error message "**this is a placeholder file**".
4. From the Exchange server, open a web browser such as Internet Explorer, and type *https://<host>/EWS/Service.asmx* (where <*host*> is either <*smtpdomain*> or *autodiscover.*<*smtpdomain*>), and ensure an .xml file appears and that you do not have any certificate errors.

On the DNS server

- Ensure that the appropriate DNS entries have been made to route <*smtpdomain*> or *autodiscover.*<*smtpdomain*> to the computer running the Coexistence Manager for GroupWise Free/Busy Connector.

On the computer running Coexistence Manager for GroupWise Free/Busy Web Services

- On the computer running Coexistence Manager for GroupWise Free/Busy Connector web services, run the *Get-CmgAutodiscoverConfig* cmdlet, and verify that the *CmgAvailabilityUrl* is set to *https://<host>/EWS/Service.asmx* (where <*host*> is either <*smtpdomain*> or *autodiscover.*<*smtpdomain*>).
- On the computer running Coexistence Manager for GroupWise Free/Busy Connector web services, ensure that *Get-CmgAvailabilityConfig* is configured to communicate to the correct host and port for the computer running the Coexistence Manager for GroupWise GroupWise Free/Busy Connector service.

On the computer running Coexistence Manager for GroupWise GroupWise Free/Busy Connector Service

- On the computer running the Coexistence Manager for GroupWise GroupWise Free/Busy Connector Service, ensure the GroupWise service is properly configured using *Set-CmgGroupWiseFreeBusyConfig*.
- Ensure the Coexistence Manager for GroupWise GroupWise Free/Busy Connector service is running and there are no errors in the event log.
- Ensure GroupWise is properly configured to connect to your GroupWise FBC server.

Outlook/OWA users cannot see free/busy information for large number of users

If you see the following error message: The maximum message size quota for incoming messages (65536) has been exceeded, you must increase the quota by using the *MaxReceivedMessageSize* property on the appropriate binding element.

If you are using OWA or Outlook and querying Free/Busy information for a GroupWise user, edit the Web.Config file in the EWS folder on the Coexistence Manager for GroupWise Web Server:

- Add the *maxReceivedMessageSize* property to the file and set it to a large value:

```
<netTcpBinding>
   <binding name="Coexistence Manager for GroupWiseFreeBusyClientSettings"
      openTimeout="00:01:00"
      receiveTimeout="00:01:00"
      sendTimeout="00:01:00"
```

```
      closeTimeout="00:01:00"
      maxReceivedMessageSize="655360">
      <security mode="None"/>
   </binding>
</netTcpBinding>
```

Other Free/Busy Connector issues

Look through your Coexistence Manager for GroupWise Free/Busy Connector log files for clues to help diagnose and resolve the problem. If the default logging settings don't meet your diagnostic needs, see Appendix C: Configuring CMG logging for instructions to change logging configuration settings.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/company/contact-us.aspx or call +1-949-754-8000.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.

Index

G

H

I

L

M

N

O

P

R

S

T

W