Quest

Quest® Coexistence Manager™ for Notes 3.9.2

FBC Scenarios 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 Software, Quest, and the Quest logo 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.

CMN FBC Scenarios Guide
Updated - February 2024
Software Version - 3.9.2

Contents

About the CMN Documentation

The documentation for Quest Coexistence Manager for Notes (CMN) includes:

- ***Release Notes*** (printable PDF): Describes the current CMN 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 explains how to download and install the software.
- ***CMN User Guide*** (printable PDF): Comprehensive documentation of CMN's three primary components: Directory Connector, Mail Connector and Free/Busy Connector. Describes component capabilities, deployment considerations, configuration instructions and tips, and application notes and screen-by-screen field notes for CMN's Management Console software tools.
- ***FBC Scenarios Guide*** (printable PDF): Provides process instructions and application notes for installing and configuring CMN's Free/Busy Connector (FBC) in a variety of Exchange-side scenarios.
- ***CMN Program Parameters Reference*** (printable PDF): Listing of all CMN program parameters that are not associated with UI fields in CMN's Management Console, with descriptions and default values and usage/application notes. (Parameters associated with UI fields do appear in the *Configuration.xml* files, but should not be edited manually.)
- ***Management Console Online Help*** (three compiled Windows Help files, one for each CMN component): Field notes and application notes for the screens and features of CMN's Management Console.

All CMN 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 CMN Documentation

This table shows where you can find particular types of information about particular CMN components:

	for Dir Connector & Mail Connector	for Free/Busy Connector
Introduction and orientation:	— — CMN Quick-Start Guide and User Guide — —	
System requirements:	— — CMN Release Notes — —	
Installation instructions:	— — CMN Quick-Start Guide — —	
Configuration instructions:	CMN User Guide	CMN FBC Scenarios Guide
Operating instructions:	— — CMN User Guide — —	
Troubleshooting info:	CMN User Guide	CMN FBC Scenarios Guide

The CMN application Help files contain the same information as the *User Guide*, but make the information available on-screen at a single keystroke (from the CMN Management Console).

1

Introduction

Chapter 4 of the CMN *User Guide* provides an introduction to CMN's Free/Busy Connector ("FBC" or "F/B Connector") and its subcomponents, and a high-level overview of the data flow in both directions: Notes queries for Outlook F/B data (and the Exchange reply), and vice-versa. The F/B chapter in the User Guide also documents CMN's FBC Management Console software, which is used to configure the FBC.

FBC configuration requires much more than just a run through the CMN software, since both the Notes/Domino side and the Outlook/Exchange side must be configured to work with the FBC, and CMN's FBC Web Server must also be configured, and finally all of the connections among Notes/Domino, Exchange and CMN's Web Server must be configured and tested. We therefore provide those configuration instructions in this separate *Guide*.

- F/B Connector configuration scenarios
- Configuring and troubleshooting the F/B Connector with PowerShell

F/B Connector configuration scenarios

CMN's Free/Busy Connector ("FBC" or "F/B Connector") supports F/B coexistence for an on-premises Exchange, or for a hybrid or non-hybrid Office 365 ("O365") scenario. For a hybrid O365 (O365 synced to an on-premises Exchange), CMN's FBC is configured between Notes/Domino and the local on-premises Exchange, and synchronization of the local Exchange to O365 is configured apart from CMN—as described in Microsoft documentation.

CMN also 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 Domino server.

This *FBC Scenarios Guide* therefore provides process instructions and application notes for installing and configuring CMN's Free/Busy Connector in all of these Exchange-side scenarios:

- Hybrid Office 365 with shared (single) namespace
- Hybrid Office 365 with separate namespaces
- Non-hybrid Office 365 with shared (single) namespace
- Non-hybrid Office 365 with separate namespaces
- On-premises Exchange with shared (single) namespace
- On-premises Exchange with separate namespaces

Since the FBC for a hybrid Office 365 is configured only between Notes/Domino and the local on-premises Exchange, the process to configure CMN's FBC for a hybrid O365 is identical to the process for a local on-premises Exchange. The synchronization of the local Exchange to O365 is apart from CMN's FBC, and is fully documented by Microsoft.

This introductory chapter is followed by four chapters that each describe the complete process for installing and configuring the FBC for a particular Exchange-side environment:

Chapter 2: On-premises Exchange or hybrid O365 using shared (single) namespace

Chapter 3: On-premises Exchange or hybrid O365 using separate namespaces

Chapter 4: Non-hybrid O365 using shared (single) namespace

Chapter 5: Non-hybrid O365 using separate namespaces

To configure CMN's FBC for a hybrid O365, refer to the appropriate on-premises scenario instructions in this *Guide* (in chapter 2 or 3). Remember to configure and test the hybrid connection between your local Exchange environment and Office 365, as documented by Microsoft, before configuring CMN's FBC.

The scenario chapters also explain how to configure the Domino, Exchange and AD servers to work with CMN's FBC in the various scenarios.

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

Registering CMN with the Microsoft Azure portal

To use modern authentication (OAuth) with the Exchange Online (hybrid and native) for EWS as a method to access Exchange Online, you must register the CMN with the Microsoft Azure portal.

After configuring the Target Environments admin page in CMN for hybrid or native Office 365, specify the Azure Application ID that you have registered.

Depending on the region from where you are accessing the Microsoft Azure portal site, the user interface can differ.

Below are the Data sources that connect to Exchange Online using EWS:

- Exchange Online Mailbox Contents
- Exchange Online Mailbox Content Summary
- Exchange Online Calendar

Steps to register the CMN application:

1. Sign in to the Microsoft Azure portal. (You must have global admin rights to register an application.)
2. Search for App registrations in the search box on the top.

   - OR -

   On the left side of navigation pane, click Azure **Active Directory** service, click **App registrations** > **New Registration**.
3. On the **Register an application** page, enter the application registration information as below:
   - Name: Enter a name for the application. For example, CMN-EXO.
   - Supported account types: Select **Accounts in this organizational directory** (Single tenant)
4. Click Register.

   Now, the application is registered in the Microsoft Azure portal and the Application (Client) ID is displayed. Copy this ID and use it later to set the Azure Application ID in the Target Environments page.
5. Under Manage in the left section, click **Authentication**.
6. Under Advanced settings, select **Yes** to Allow public client flows and click **Save**.
7. Under Manage in the left section, click **API permissions**.
8. Click **Add a permission**.
9. Select the **APIs my organization** uses tab.
10. Search for Office 365 Exchange Online and click **Office 365 Exchange Online** in the search result.
11. Select **Application permissions**.
12. Select **full_access_as_app**.

In some Microsoft National Clouds, you might select accordingly.

13 Click **Add permissions**.

14 Click **Grant admin consent for** <Your Organization> and click **Yes** to confirm.

15 Under Manage on the left section, click **Manifest**.

16 A JSON file will be opened where you have to search for **requiredResourceAccess**, and add following text in that file, and finally click **Save**.

```
{"id": "dc890d15-9560-4a4c-9b7f-a736ec74ec40", "type": "Role"} in resource access.
```

To create a Client Secret:

1 Select Certificates & Secrets in the left-hand navigation under Manage.

2 Select New client secret, enter a short description for example, "CMN-ClientSecret" and select **Add**.

3 Choose the Expires from dropdown.

4 Click on **Add**

5 Copy the '**Value**' of the newly added client secret and save it as you will need it later.

6 Go to overview - note down the Tenant ID, Application (Client) ID and the above generated Client Secret value for authentication in CMN Console for Exchange free/busy.

Other supported variations to typical FBC scenarios

CMN's Free/Busy Connector supports several variations to the primary scenarios listed above. Accommodations for these variations are included in the installation and configuration procedures in the remaining chapters of this book, and we summarize them briefly here:

- ***Multi-Domain Support:*** The Free/Busy Connector can facilitate the exchange of F/B information among multiple subdomains supported by both the Exchange and Domino servers.
- ***Multiple Domino Servers:*** CMN supports sharing F/B information between multiple Domino servers and a single Exchange server.
- ***Domino Clusters:*** CMN supports a cluster of Domino servers (ClusterNode1 and ClusterNode2) that provide Lotus Notes mail service in an active/standby redundancy configuration. In this case, only a single CMN Web Server is required to support both Domino servers.

General FBC deployment considerations

For technical reasons, the QCalCon subcomponent of the F/B Connector *must* be installed on a Domino server. But if the Domino environment contains more than one Domino server, QCalCon is installed on only one server. (Other Domino servers must be configured to find and use the single QCalCon instance on the "bridgehead" server.) In a typical scenario, the other four FBC subcomponents can be installed on a single computer, although deployment to two separate computers (as illustrated in the chapter 4 of the *CMN User Guide*) will improve performance in environments with higher volumes of F/B queries and replies.

Consider also that the Free/Busy Connector usually exerts the heaviest demand on computing resources, compared to the other two CMN components.

Configuring and troubleshooting the F/B Connector with PowerShell

You may use these PowerShell commands (instead of CMN's Management Console) to configure and/or troubleshoot F/B Connector issues.

PowerShell to configure the F/B Connector

Note that for every *set-cmn** command listed here, there is a corresponding *get-cmn** command that takes no parameters.

command	parameter
Set-CmnAutodiscoverConfig	[-CMxEwsUrl] <String>

- **CMxEwsUrl:** The URL of the EWS service.

command	parameters
Set-CmnEwsConfig	[[-HostName] <String>] [[-PortNumber] <Int32>]

HostName: Name of server hosting the Notes F/B Connector Service.

PortNumber: Port number the Notes F/B Connector Service is located on.

command	parameters
Set-CmnDominoFreeBusyConfig	[-DominoServerName <String>] [-DominoPassword <SecureString>] [-DominoUserFetchIntervalInMinutes <UInt32>] [-DominoUserSmtpDomains <String>] [-ListeningPort <UInt32>] [<CommonParameters>]

DominoServerName: Name of the Domino server, in Notes format (not FQDN).

DominoPassword: Password of the Domino user ($securePassword).

DominoUserFetchIntervalInMinutes: Time set to refresh list of Domino users.

DominoUserSmtpDomains: Fully qualified SMTP domain for Domino mail domain.

ListeningPort: Listening port for the Quest CMN Domino Free/Busy Connector Service. The F/B Connector uses port 8960 and 8961 for TCP communication. These ports can be adjusted if required using the provided cmdlets. Ensure these ports are not in use and not blocked by any firewall applications.

DominoIdFilePath: Path to ID file for Domino user. Must be stored on same computer where CMN Domino Free/Busy Connector Service is installed.

command	parameters
Set-CmnExchangeFreeBusyConfig	[[-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 EWS URLs that are valid for Autodisover to redirect to.

command	parameters
Set-CmnQCalConConfig	[[-ExchangeFreeBusyServiceHostName] <String>] [[-ExchangeFreeBusyPortNumber] <Int32>] [[-DaysOfFreeBusy] <UInt32>]

ExchangeFreeBusyServiceHostName: Name of the server hosting the Exchange F/B Connector Service.

ExchangeFreeBusyPortNumber: Port number of the Exchange F/B Connector Service.

DaysOfFreeBusy: Number of days of F/B to be retrieved from Exchange.

PowerShell to troubleshoot the F/B Connector

To get F/B info for an Exchange user:

command	parameter
Get-CmnExchangeFreeBusy	[-SmtpAddress] <String>

SmtpAddress: Email address of user for whom you are requesting F/B info.

To get F/B info for a Notes/Domino user:

command	parameter
Get-CmnDominoFreeBusy	[-SmtpAddress] <String>

SmtpAddress: Email address of user for whom you are requesting F/B info.

To get the URL of the Exchange Availability Web Service (EWS):

command	parameters
Get-CmnExchangeWebServicesUrl	[-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.

2

On-premises Exchange or hybrid O365 using shared (single) namespace

Follow these steps, in order as presented here, to install and configure CMN's Free/Busy Connector for an on-premises Exchange ***or*** a hybrid Office 365 environment with a shared (single) namespace:

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

Remember that the FBC for a hybrid O365 is configured only between Notes/Domino and the local on-premises Exchange, while synchronization of the local Exchange to O365 is configured apart from CMN (and documented separately by Microsoft). Configuration of CMN'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 CMN's FBC.

Step 1: Plan your FBC installation and configuration

To plan your overall FBC installation and configuration:

- 1-1: Verify system requirements
- 1-2: Make a configuration map
- 1-3: Complete the CMN FBC Planning Worksheet

1-1: Verify system requirements

Review the system requirements (in the CMN *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.

1-2: 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 decide how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers. For technical reasons, the QCalCon component of the Free/Busy Connector *must* be installed on a Domino server. But

if the Domino environment contains more than one Domino server, QCalCon is installed on only one server. (Other Domino servers can find and use a single QCalCon instance on a "bridgehead" server.) The other four Free/Busy Connector components can be installed on a single computer, although deployment to two separate computers will improve performance in environments with higher volumes of F/B queries and replies.

When Free/Busy Connector components are deployed to two computers, they are typically installed like this:

- Computer 1, for Domino queries of Exchange users (and Exchange replies with F/B info): hosts the CMN Exchange Free/Busy Service.
- Computer 2, for Exchange queries of Domino users (and Domino replies with F/B info): hosts the CMN Domino Free/Busy Service, and the CMN Autodiscover and EWS web services.

1-3: Complete the CMN FBC Planning Worksheet

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

Step 2: Configure the Notes/Domino side

A particular configuration of the Notes/Domino environment works best in most environments for compatibility with CMN's Free/Busy Connector. This section explains how to achieve the recommended configuration.

To configure the Notes/Domino side:

- 2-1: Physically install the CMN QCalCon task
- 2-2: Configure Domino Person documents
- 2-3: Add the domain documents
- 2-4: Set up the foreign SMTP document
- 2-5: Set up the server connection document
- 2-6: Add TCP/IP connection documents

If configuring CMN to support Domino clusters

CMN supports Domino server clusters (ClusterNode1 and ClusterNode2) that provide Lotus Notes mail service in an active/standby redundancy configuration. In this case, a single CMN Web Server is required to support both Domino Servers.

Some Domino configuration steps are required for this scenario, but they occur only after the CMN FBC Web Server is configured (in Step 4 below). Complete the steps here to configure the rest of the Notes/Domino side, and then you will configure support for Domino clusters later in Step 4.

2-1: Physically install the CMN QCalCon task

CMN's QCalCon is a Domino server task that facilitates communications between the Domino and Exchange servers, for transmitting Domino F/B queries to Exchange, and receiving F/B information from Exchange.

Run the CMN Autorun installer to install QCalCon to the Domino server. AutoRun offers the choice of a 32-bit or 64-bit edition of QCalCon. Choose the edition that matches the local Domino software edition (32- vs. 64-bit). (The host computer's operating system is irrelevant to this choice.)

The AutoRun installer automatically checks the environment to verify CMN prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command before executing.

To configure CMN's F/B Connector for multiple Domino servers

In a Domino environment containing more than one Domino server, QCalCon is typically installed on only one "bridgehead" server. A Domino admin then configures the non-QCalCon servers to route their local users' F/B queries to the QCalCon bridgehead server.

> **NOTE:** Some admins with multiple Domino 6.5.x servers (only) report that non-bridgehead Domino 6.5.x servers are unable to route F/B queries to a QCalCon bridgehead server. IBM (in this article) says only: "Domino [6.5.x or earlier] does not support this type of configuration for free time lookup." Despite the IBM disclaimer, CMN's Free/Busy Connector does work in many such environments if its QCalCon server task is installed on *all* Domino 6.5.x servers.

2-2: Configure Domino Person documents

> **NOTE:** This configuration is necessary in most environments, but in most cases it would be impractical to repeat these steps for every Exchange user. Instead, consider using CMN's Directory Connector to automate this task. The CMN Directory Connector correctly synchronizes the contacts to support Free/Busy Connector operations in our recommended configuration.

> **IMPORTANT:** CMN's F/B Connector requires that each user's SMTP forwarding address appear in the Domino *User name* field, although it can appear in any position within that field (first, middle or last).

For each user, begin with the semi-standard settings, including the calendar domain on the *Miscellaneous* tab. Then:

1. Set the **Mail system** to *Notes*, so the **Mail server** field can be populated with a server that is valid in the environment. (There is no need to specify a **Mail file**; only the **Mail server** must be modified.)
2. **Save & Close** the contact.
3. Reopen the contact, and change the **Mail system** back to **Other Internet Mail**. (This will hide the **Mail server** field, but the field is still populated even though it does not appear—necessary only when creating contacts manually.)
4. **Save & Close** the contact.

2-3: Add the domain documents

You will need a foreign domain with a name that matches the name in the **Calendar system** field.

Add a Notes foreign domain document. The *Mail Information* and *Calendar Information* tabs should have the gateway and calendar server name pointing to the location of the QCalCon server, using the Notes qualified server name. (QCalCon should already be installed and configured according to the *CMN User Guide* instructions.) The **Gateway mail file name** (on the *Mail Info* tab) and **Calendar system** (*Calendar Info* tab) must both be set to *Mail.box*. In environments that use multiple *mail.box* files, the name should match one of those files (typically *mail1.box*, *mail2.box*, etc.).

2-4: Set up the foreign SMTP document

The configuration settings for CMN are all on the *Routing* tab. All the settings on the other tabs are left at their respective defaults.

1. The **Internet Domain** field must be set to the name of the domain you will use for the Exchange users. Note that the **Internet Domain** value must begin with an asterisk as the first character of the name, *with no dot*—just an asterisk and then the FQDN.
2. The **Domain name** must be entered as *CMNOUT*, to match with a connection document that will be set up next.

2-5: Set up the server connection document

This Connection Document is used both for the Free/Busy Connector and for mail-routing.

1. On the *Basics* tab: Set the **Connection type** to *SMTP*, and the **Source server** is the server where the F/B request will originate.
2. To accommodate multiple mail servers, set up just one *Server Connection* document with the **Source server** set so that any of those servers can use this same document:
   - ***Source Domain*** (field appears in some but not all Domino versions): The Domino domain.
   - ***Connect via:*** Set to *Direct connection*.
   - ***Destination server:*** Can be any arbitrary name you want to assign.
   - ***Destination domain:*** Should be set to *CMNOUT*, to match the **Domain name** in the *Foreign SMTP Document* (set up in the preceding section). You can use some other value, but the **Destination domain** value here must match the **Foreign SMTP Domain** name. Note this is a "virtual domain," not a real domain. It doesn't really exist or go anywhere, but we use these fields to get Domino to match documents and route mail the way we want.
3. Set the **SMTP MTA relay host** to the IP address of the CMN Mail Connector.
4. On the *Replication/Routing* tab (for the same connection document): The **Replication task** should be *Disabled*, and the **Routing task** should be set to *Mail Routing* or *SMTP Mail Routing*, depending on the setup of your environment.
5. On the *Schedule* tab (for the same connection document): Set this connection document to be enabled 24 hours per day.

2-6: Add TCP/IP connection documents

In some environments, free/busy lookups may also require that you add TCP/IP Connection documents in both directions between the Domino servers housing mail databases (mailbox servers) and the Domino server running the QCalCon Domino Server Task.

NOTE: This step may not be necessary if internal TCP/IP communications are already established in the environment. The bottom-line requirement is that the QCalCon server must be able to communicate with other servers.

To add TCP/IP connection documents: In Domino Admin, expand *Configuration*, expand *Messaging* and then click **Connections**. Add a connection, and then:

1. On the *Basics* tab:
   - ***Connection type:*** Local Area Network.
   - ***Source Server:*** name of the Domino server (in the Notes / Domino format, e.g. source_Notes_mail_database_server/DOMINODOMAIN).
   - ***Use the port(s):*** TCP/IP.
   - ***Usage priority:*** Normal.
   - ***Destination server:*** the Domino server hosting the QCalCon Domino Server Task (in the Notes / Domino format, e.g. *target_Notes_QCalCon_server/DOMINODOMAIN*).
   - ***Destination domain:*** DOMINODOMAIN of the server running the QCalCon Domino Server Task.
   - ***Optional network address:*** IP address of the destination server.

IMPORTANT: Remember that a TCP/IP Connection document is required in both directions. The *Basics* tab settings must be reversed on the other TCP/IP Connection document to define a connection in the other direction. The net result of this configuration with a Domino mail database server and the QCalCon Domino Server Task running on a separate Domino server is that you will have two TCP/IP Connection documents, with one document pair for each Domino mail database server.

2 On the *Replication/Routing* tab:
   - ***Replication task:*** Disabled.
   - ***Routing task:*** Mail Routing.
   - ***Route at once if:*** 1 messages pending.
3 On the *Schedule* tab: Modify the settings on this tab to meet sending requirements (24 hours).
4 Click **Save and Close**.

Step 3: Configure the Exchange side

Configure domains, permissions and other server parameters and attributes so they will be able to work with CMN's Free/Busy Connector.

If you are configuring FBC for a hybrid Office 365: Remember that the FBC for a hybrid O365 is configured only between Notes/Domino and the local on-premises Exchange, while synchronization of the local Exchange to O365 is configured apart from CMN (and documented separately by Microsoft). Configuration of CMN'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

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

Step 4: Configure CMN's FBC Web Server

To configure CMN's FBC Web Server:

4-1: Physically install the CMN FBC components

All CMN FBC components are installed by the AutoRun utility that accompanies the CMN product kit.

The AutoRun installer automatically checks the environment to verify CMN prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command before executing.

For a typical configuration:

- ***On the CMN FBC Web Server:*** Run AutoRun to install the Autodiscover, EWS and the Domino FBC Service on the CMN FBC Web Server.
- ***On either the same CMN FBC Web Server or a separate CMN Exchange FBC Server:*** Run AutoRun to install the CMN Exchange FBC Service.

To configure CMN's F/B Connector for multiple Domino servers

For Exchange queries for Domino F/B information, the simplest approach is to dedicate a separate CMN FBC server for each Domino server, with all the CMN servers feeding into the single Exchange server. It is technically possible, but somewhat more complicated, to configure a single instance of the Domino FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple Domino servers—an approach that requires more elaborate Domino configurations.

4-2: Obtain and install web services certificates

CMN Web Server components must accept SSL connections from the mail systems. 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 Notes Server. The certificate is valid for the Autodiscover and EWS web services.

You can obtain a certificate from either of two sources:

- 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.

> **NOTE:** You can request a certificate using Web enrollment pages. For more information, see http://support.microsoft.com/kb/931351.
>
> **If you need a multi-domain certificate:** See To create a SAN certificate.

When you receive the certificate, you must install it on the appropriate server.

To configure the certificate for multi-domain support

The Free/Busy Connector can facilitate the exchange of free/busy information among multiple subdomains supported by both the Exchange and Domino servers. For a multi-domain scenario, ensure the certificate used on the CMN Web Server has subject alternate names for all associated autodiscover host names.

To request and install a certificate using IIS 7.0

To request a certificate using IIS 7.0:

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. For more information, see To request a certificate from a local CA or To request a certificate from a public CA.

To install the certificate using IIS 7.0:

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**.

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

1. From the *Connection* pane in IIS, select **Default Web Sites**.
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 request and install a certificate using IIS 6.0

To request a certificate using IIS 6.0:

1. From Internet Information Services (IIS) Manager dialog box, right-click **Default Web Site**, and select **Properties**.
2. From the Directory Security tab, select **Server Certificate** to open the Web Server Certificate Wizard.
3. Click **Next**.
4. Select **Create a new certificate request**, and click **Next**.
5. Select **Prepare the request now, but send it later**, and click **Next**.
6. Accept the defaults. Ensure **Select cryptographic service provider (CSP) for this certificate** is checked, and click **Next**.
7. Select **Microsoft RSA SChannel Cryptographic Provider**, and click **Next**.
8. Select or enter your organization's name and organizational unit, and click **Next**.
9. Enter *autodiscover.<smtpdomain>* —or— *<smtpdomain>* as the common name, for the primary domain and all required subdomains. Then click **Next**.
10. Enter the geographical information, and click **Next**.
11. Specify a file name to save the certificate request, and click **Next**.
12. Review the information, and click **Next**. Then click **Finish**.
13. Request a certificate using a local CA or public CA. For more information, see To request a certificate from a local CA or To request a certificate from a public CA.

To install the certificate using IIS 6.0:

1. From Internet Information Services (IIS) Manager dialog box, right-click **Default Web Site**, and select **Properties**.
2. From the Directory Security tab, select **Server Certificate** to open the Web Server Certificate Wizard, and click **Next**.
3. Select **Process the pending request and install the certificate**, and click **Next**.
4. Browse to the location of the text file, and click **Next**.
5. Leave the default port as 443, and click **Next**.
6. Review the certificate summary. Click **Next**, then click **Finish**.
7. From Internet Information Services (IIS) Manager dialog box, right-click **Default Web Site**, and select **Properties**.
8. From the Directory Security tab, select **Edit**.
9. Select the **Require secure channel** check box, and click **OK**.

To request a certificate from a local CA

1. From a web browser, enter *https://<Local_Certification_Authority_computer>/certsrv*
2. Click **Request a certificate**, then **Advanced certificate request**.

3 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**.

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

5 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.

6 In the **Certificate Template** box, select **Web Server**. Click **Submit**.

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

8 Save the file.

To request a certificate from a public CA

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

To create a SAN certificate

This procedure lets you configure a single certificate to answer for multiple addresses. For your single-namespace environment, this creates 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 your single-namespace environment, enter the autodiscover and root domain, like this:

```
san:dns=autodiscover.xyzcorp.com&dns=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 it later on the list. 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 default first website:

1 On the CMN F/B computer, in IIS Manager: Select **Default Web Site**.

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 CMN 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, CMN is installed with the *log4net* utility to generate log files of CMN components' activity. This information is critical to diagnosing any configuration issues that may arise. Logging is enabled by default for all CMN components.

The default configurations will be suitable for most organizations and circumstances, but you can customize logging features. The *log4net* utility may be configured to work a particular way with each CMN component. Configuration instructions are nearly identical for all components, so we present the instructions separately, in Appendix C of the *User Guide*.

4-5: Configure CMN's FBC for shared/single namespace (equivalent domains)

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

- At the CMN Web Server, open the PowerShell and type:
  Set-CmnDominoFreeBusyConfig -SmtpDomainMappings <equivalentDomain>=<primaryDomain>

4-6 (conditional): Configuring CMN's FBC for Domino clusters

CMN supports Domino server clusters (ClusterNode1 and ClusterNode2) that provide Lotus Notes mail service in an active/standby redundancy configuration. In this case, a single CMN Web Server is required to support both Domino Servers. Follow the procedures below to set up this configuration. Initially, ClusterNode1 is the active Domino server.

To install and configure CMN's FBC for the active Domino server in a cluster:

1. Ensure that the Domino Admin client installed in the CMN Web Server is able to connect to both Domino servers.
2. Install and configure CMN to support ClusterNode1, as per normal procedures.
3. Ensure that Free/Busy information is retrieved correctly in both directions using ClusterNode1.

To enable the second Domino server in a cluster to support retrieval of Domino F/B information by Exchange:

1. Failover to the standby server in the Domino Server cluster. (ClusterNode2 is now active.)
2. Ensure the Domino Admin client is connected to ClusterNode2.
3. At the CMN Web Server, stop the CMN Domino F/B Connector service.
4. At the CMN Web Server, open the PowerShell and type:
   Set-CmnDominoFreeBusyConfig -DominoServerName <ClusterNode2ServerName>
5. Restart the CMN Domino Free/Busy Connector service.
6. Ensure that Domino Free/Busy information is retrieved correctly by Exchange users (using ClusterNode2).
7. Failover to the standby server in the Domino Server cluster. ClusterNode1 is now active.
8. Ensure that Domino Free/Busy information continues to be retrieved correctly by Exchange users (using ClusterNode1).

To enable the second Domino server in a cluster to retrieve Exchange free/busy information:

1. Install QCalCon in ClusterNode2. See 2-1: Physically install the CMN QCalCon task. (QCalCon was installed in ClusterNode1 during step 2 of the initial procedure of this series.)
2. Configure QCalCon in ClusterNode2 to point to the CMN Exchange Server (where the CMN Exchange F/B Connector Service is installed).
3. Failover to the Standby server in the Domino Server cluster to make ClusterNode2 the active server (if it is not already the active server).
4. Ensure that free/busy information from Exchange is retrieved correctly by Domino users (using ClusterNode2).
5. Perform final tests to ensure that free/busy information from Exchange is successfully retrieved using either Domino server in the cluster.

4-7: Run CMN's Management Console to configure FBC components

Use CMN'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 CMN *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

IMPORTANT: For a hybrid Office 365, be sure to specify the EWS endpoint in the CMN F/B Connector Management Console.

- If the EWS URL points to the on-premises environment, clear the **Exchange Online** check box, and fill in the **Exchange Username** and **Exchange Password** boxes with the coexistence admin's credentials for the on-prem Active Directory.
- If the EWS URL points to the Exchange Online, select the **Exchange Online** check box, fill in the **Tenant ID**, **Client ID** and **Client Secret** boxes with the coexistence admin credentials for the Cloud.

NOTE: You may use PowerShell commands to configure CMN Free/Busy Connector components, instead of CMN's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Configuring and troubleshooting the F/B Connector with PowerShell in chapter 1 of this *Scenarios Guide*.

Step 5: Configure and test connections among Notes/Domino, Exchange and CMN's FBC Web Server

5-1: Synchronize Exchange and Domino directories

Before using CMN's Free/Busy Connector, both directories should be updated to include representative objects for users in both systems. For best results, Quest recommends the CMN Directory Connector for this purpose. The Directory Connector is another CMN component that may already be installed and configured. For more information about the CMN Directory Connector, see *User Guide* chapter 2.

Use CMN's Directory Connector to define a bidirectional update (a pair of single-direction updates, in opposite directions, run sequentially)—if you do not have such a pair already defined.

Schedule the DC connector to run automatically at a frequency to keep both directories current throughout the coexistence period.

You may choose instead to perform a directory synchronization manually, in which case you may follow the two procedures below.

To synchronize Domino mail users to Exchange contacts:

1. Using the Exchange Management Console, create a mail contact for a Domino user account.
2. Ensure that the Exchange contact has a primary external SMTP address set to the same value as the *InternetAddress* property for the Lotus Notes mail user account.
3. Repeat the above steps for each Lotus Notes mail user account.

To synchronize Exchange mail users to Domino contacts:

1. Ensure that a Foreign Domain document has been created. To create a Foreign Domain document:
   a. As a Domino Administrator, select the **Configuration** tab.
   b. Select **Messaging | Domains**, then click **Add Domain**.
   c. Select the **Basics** tab. In the *Foreign domain name* box, enter a fictitious domain name (for example, *CMNFreeBusy*). This forces Domino to direct queries to QCalCon rather than to internal queues. Quest recommends using subdomains with the F/B Connector if feasible.

      The name of the foreign SMTP domain must be prepended by an asterisk, for example: **Exchange.sitraka.com*. This forces Domino to direct queries to QCalCon rather than to internal queues. Quest recommends using subdomains with the F/B Connector if feasible.
   d. Select the **Mail Information** tab. Enter the Gateway server name where the QCalCon Domino Server Task is installed.

e Enter the Gateway mail file name: *mail.box*

f Click the **Calendar Information** tab, and enter the Calendar server name of the server running QCalCon Domino Server Task.

g In the Calendar system, enter: *mail.box*

2 Create a new Person Document using Lotus Notes.

3 Set the mail type to *Other Internet Mail*.

4 Set the *CalendarDomain* property to the same value as the *CalendarSystem* property of the Foreign Domain document. (This permits configuration of CMN's Free/Busy Domino server task, QCalCon.)

5 Set the *InternetAddress* property of the Person Document to the Exchange SMTP email address.

5-2: Configure Exchange server connections

Configure and verify the link from the Exchange Server to the domains/subdomains supported by the Domino Server. This procedure tests whether the certificate on the CMN Web Server is trusted by the Exchange Server.

To configure the Exchange Server link to the CMN 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 Domino 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 CMN 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 CMN Autodiscover.

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

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 CMN. For more information, see this Microsoft article.

Configure DNS (Domain Name System)

Configure DNS to point *autodiscover.<smtpdomain.com>* to the computer where CMN'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 Domino server, through the CMN Free/Busy Connector, you must make the CMN Autodiscover Web Service resolvable to this URL:

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

3

On-premises Exchange or hybrid O365 using separate namespaces

Follow these steps, in order as presented here, to install and configure CMN's Free/Busy Connector for on-premises Exchange ***or*** a hybrid Office 365 environment with separate (multiple) namespaces:

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

Remember that the FBC for a hybrid O365 is configured only between Notes/Domino and the local on-premises Exchange, while synchronization of the local Exchange to O365 is configured apart from CMN (and documented separately by Microsoft). Configuration of CMN'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 CMN's FBC.

Step 1: Plan your FBC installation and configuration

To plan your overall FBC installation and configuration:

- 1-1: Verify system requirements
- 1-2: Make a configuration map
- 1-3: Complete the CMN FBC Planning Worksheet

1-1: Verify system requirements

Review the system requirements (in the CMN *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.

1-2: 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 decide how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers. For technical reasons, the QCalCon component of the Free/Busy Connector *must* be installed on a Domino server. But if the Domino environment contains more than one Domino server, QCalCon is installed on only one server. (Other Domino servers can find and use a single QCalCon instance on a "bridgehead" server.) The other four Free/Busy

Connector components can be installed on a single computer, although deployment to two separate computers will improve performance in environments with higher volumes of F/B queries and replies.

When Free/Busy Connector components are deployed to two computers, they are typically installed like this:

- Computer 1, for Domino queries of Exchange users (and Exchange replies with F/B info): hosts the CMN Exchange Free/Busy Service.
- Computer 2, for Exchange queries of Domino users (and Domino replies with F/B info): hosts the CMN Domino Free/Busy Service, and the CMN Autodiscover and EWS web services.

1-3: Complete the CMN FBC Planning Worksheet

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

Step 2: Configure the Notes/Domino side

A particular configuration of the Notes/Domino environment works best in most environments for compatibility with CMN's Free/Busy Connector. This section explains how to achieve the recommended configuration.

To configure the Notes/Domino side:

- 2-1: Physically install the CMN QCalCon task
- 2-2: Configure Domino Person documents
- 2-3: Add the domain documents
- 2-4: Set up the foreign SMTP document
- 2-5: Set up the server connection document
- 2-6: Add TCP/IP connection documents

If configuring CMN to support Domino clusters

CMN supports Domino server clusters (ClusterNode1 and ClusterNode2) that provide Lotus Notes mail service in an active/standby redundancy configuration. In this case, a single CMN Web Server is required to support both Domino Servers.

Some Domino configuration steps are required for this scenario, but they occur only after the CMN FBC Web Server is configured (in Step 4 below). Complete the steps here to configure the rest of the Notes/Domino side, and then you will configure support for Domino clusters later in Step 4.

2-1: Physically install the CMN QCalCon task

CMN's QCalCon is a Domino server task that facilitates communications between the Domino and Exchange servers, for transmitting Domino F/B queries to Exchange, and receiving F/B information from Exchange.

Run the CMN Autorun installer to install QCalCon to the Domino server. AutoRun offers the choice of a 32-bit or 64-bit edition of QCalCon. Choose the edition that matches the local Domino software edition (32- vs. 64-bit). (The host computer's operating system is irrelevant to this choice.)

The AutoRun installer automatically checks the environment to verify CMN prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command before executing.

To configure CMN's F/B Connector for multiple Domino servers

In a Domino environment containing more than one Domino server, QCalCon is typically installed on only one "bridgehead" server. A Domino admin then configures the non-QCalCon servers to route their local users' F/B queries to the QCalCon bridgehead server.

> **NOTE:** Some admins with multiple Domino 6.5.x servers (only) report that non-bridgehead Domino 6.5.x servers are unable to route F/B queries to a QCalCon bridgehead server. IBM (in this article) says only: "Domino [6.5.x or earlier] does not support this type of configuration for free time lookup." Despite the IBM disclaimer, CMN's Free/Busy Connector does work in many such environments if its QCalCon server task is installed on *all* Domino 6.5.x servers.

2-2: Configure Domino Person documents

> **NOTE:** This configuration is necessary in most environments, but in most cases it would be impractical to repeat these steps for every Exchange user. Instead, consider using CMN's Directory Connector to automate this task. The CMN Directory Connector correctly synchronizes the contacts to support Free/Busy Connector operations in our recommended configuration.

> **IMPORTANT:** CMN's F/B Connector requires that each user's SMTP forwarding address appear in the Domino *User name* field, although it can appear in any position within that field (first, middle or last).

For each user, begin with the semi-standard settings, including the calendar domain on the *Miscellaneous* tab. Then:

1. Set the **Mail system** to *Notes*, so the **Mail server** field can be populated with a server that is valid in the environment. (There is no need to specify a **Mail file**; only the **Mail server** must be modified.)
2. **Save & Close** the contact.
3. Reopen the contact, and change the **Mail system** back to **Other Internet Mail**. (This will hide the **Mail server** field, but the field is still populated even though it does not appear—necessary only when creating contacts manually.)
4. **Save & Close** the contact.

2-3: Add the domain documents

You will need a foreign domain with a name that matches the name in the **Calendar system** field.

Add a Notes foreign domain document. The *Mail Information* and *Calendar Information* tabs should have the gateway and calendar server name pointing to the location of the QCalCon server, using the Notes qualified server name. (QCalCon should already be installed and configured according to the *CMN User Guide* instructions.) The **Gateway mail file name** (on the *Mail Info* tab) and **Calendar system** (*Calendar Info* tab) must both be set to *Mail.box*. In environments that use multiple *mail.box* files, the name should match one of those files (typically *mail1.box*, *mail2.box*, etc.).

2-4: Set up the foreign SMTP document

The configuration settings for CMN are all on the *Routing* tab. All the settings on the other tabs are left at their respective defaults.

1. The **Internet Domain** field must be set to the name of the domain you will use for the Exchange users. Note that the **Internet Domain** value must begin with an asterisk as the first character of the name, *with no dot*—just an asterisk and then the FQDN.
2. The **Domain name** must be entered as *CMNOUT*, to match with a connection document that will be set up next.

2-5: Set up the server connection document

This Connection Document is used both for the Free/Busy Connector and for mail-routing.

1. On the *Basics* tab: Set the **Connection type** to *SMTP*, and the **Source server** is the server where the F/B request will originate.
2. To accommodate multiple mail servers, set up just one *Server Connection* document with the **Source server** set so that any of those servers can use this same document:
   - ***Source Domain*** (field appears in some but not all Domino versions): The Domino domain.
   - ***Connect via:*** Set to *Direct connection*.
   - ***Destination server:*** Can be any arbitrary name you want to assign.
   - ***Destination domain:*** Should be set to *CMNOUT*, to match the **Domain name** in the *Foreign SMTP Document* (set up in the preceding section). You can use some other value, but the **Destination domain** value here must match the **Foreign SMTP Domain** name. Note this is a "virtual domain," not a real domain. It doesn't really exist or go anywhere, but we use these fields to get Domino to match documents and route mail the way we want.
3. Set the **SMTP MTA relay host** to the IP address of the CMN Mail Connector.
4. On the *Replication/Routing* tab (for the same connection document): The **Replication task** should be *Disabled*, and the **Routing task** should be set to *Mail Routing* or *SMTP Mail Routing*, depending on the setup of your environment.
5. On the *Schedule* tab (for the same connection document): Set this connection document to be enabled 24 hours per day.

2-6: Add TCP/IP connection documents

In some environments, free/busy lookups may also require that you add TCP/IP Connection documents in both directions between the Domino servers housing mail databases (mailbox servers) and the Domino server running the QCalCon Domino Server Task.

NOTE: This step may not be necessary if internal TCP/IP communications are already established in the environment. The bottom-line requirement is that the QCalCon server must be able to communicate with other servers.

To add TCP/IP connection documents: In Domino Admin, expand *Configuration*, expand *Messaging* and then click **Connections**. Add a connection, and then:

1. On the *Basics* tab:
   - ***Connection type:*** Local Area Network.
   - ***Source Server:*** name of the Domino server (in the Notes / Domino format, e.g. source_Notes_mail_database_server/DOMINODOMAIN).
   - ***Use the port(s):*** TCP/IP.
   - ***Usage priority:*** Normal.
   - ***Destination server:*** the Domino server hosting the QCalCon Domino Server Task (in the Notes / Domino format, e.g. *target_Notes_QCalCon_server/DOMINODOMAIN*).
   - ***Destination domain:*** DOMINODOMAIN of the server running the QCalCon Domino Server Task.
   - ***Optional network address:*** IP address of the destination server.

IMPORTANT: Remember that a TCP/IP Connection document is required in both directions. The *Basics* tab settings must be reversed on the other TCP/IP Connection document to define a connection in the other direction. The net result of this configuration with a Domino mail database server and the QCalCon Domino Server Task running on a separate Domino server is that you will have two TCP/IP Connection documents, with one document pair for each Domino mail database server.

2 On the *Replication/Routing* tab:
   - ***Replication task:*** Disabled.
   - ***Routing task:*** Mail Routing.
   - ***Route at once if:*** 1 messages pending.
3 On the *Schedule* tab: Modify the settings on this tab to meet sending requirements (24 hours).
4 Click **Save and Close**.

Step 3: Configure the Exchange side

Configure domains, permissions and other server parameters and attributes so they will be able to work with CMN's Free/Busy Connector.

If you are configuring FBC for a hybrid Office 365: Remember that the FBC for a hybrid O365 is configured only between Notes/Domino and the local on-premises Exchange, while synchronization of the local Exchange to O365 is configured apart from CMN (and documented separately by Microsoft). Configuration of CMN'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

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

Step 4: Configure CMN's FBC Web Server

To configure CMN's FBC Web Server:

4-1: Physically install the CMN FBC components

All CMN FBC components are installed by the AutoRun utility that accompanies the CMN product kit.

The AutoRun installer automatically checks the environment to verify CMN prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command before executing.

For a typical configuration:

- ***On the CMN FBC Web Server:*** Run AutoRun to install the Autodiscover, EWS and the Domino FBC Service on the CMN FBC Web Server.
- ***On either the same CMN FBC Web Server or a separate CMN Exchange FBC Server:*** Run AutoRun to install the CMN Exchange FBC Service.

To configure CMN's F/B Connector for multiple Domino servers

For Exchange queries for Domino F/B information, the simplest approach is to dedicate a separate CMN FBC server for each Domino server, with all the CMN servers feeding into the single Exchange server. It is technically possible, but somewhat more complicated, to configure a single instance of the Domino FBC Service, EWS and

Autodiscover to process free/busy traffic to and from multiple Domino servers—an approach that requires more elaborate Domino configurations.

4-2: Obtain and install web services certificates

CMN Web Server components must accept SSL connections from the mail systems. 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 Notes Server. The certificate is valid for the Autodiscover and EWS web services.

You can obtain a certificate from either of two sources:

- 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.

> **NOTE:** You can request a certificate using Web enrollment pages. For more information, see http://support.microsoft.com/kb/931351.
>
> **If you need a multi-domain certificate:** See To create a SAN certificate.

When you receive the certificate, you must install it on the appropriate server.

To configure the certificate for multi-domain support

The Free/Busy Connector can facilitate the exchange of free/busy information among multiple subdomains supported by both the Exchange and Domino servers. For a multi-domain scenario, ensure the certificate used on the CMN Web Server has subject alternate names for all associated autodiscover host names.

To request and install a certificate using IIS 7.0

To request a certificate using IIS 7.0:

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. For more information, see To request a certificate from a local CA or To request a certificate from a public CA.

To install the certificate using IIS 7.0:

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**.

> ***To create an https binding for the web site using IIS 7.0:***
>
> 1. From the *Connection* pane in IIS, select **Default Web Sites**.
> 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 request and install a certificate using IIS 6.0

To request a certificate using IIS 6.0:

1. From Internet Information Services (IIS) Manager dialog box, right-click **Default Web Site**, and select **Properties**.
2. From the Directory Security tab, select **Server Certificate** to open the Web Server Certificate Wizard.
3. Click **Next**.
4. Select **Create a new certificate request**, and click **Next**.
5. Select **Prepare the request now, but send it later**, and click **Next**.
6. Accept the defaults. Ensure **Select cryptographic service provider (CSP) for this certificate** is checked, and click **Next**.
7. Select **Microsoft RSA SChannel Cryptographic Provider**, and click **Next**.
8. Select or enter your organization's name and organizational unit, and click **Next**.
9. Enter *autodiscover.*<*smtpdomain*> —or— <*smtpdomain*> as the common name, for the primary domain and all required subdomains. Then click **Next**.
10. Enter the geographical information, and click **Next**.
11. Specify a file name to save the certificate request, and click **Next**.
12. Review the information, and click **Next**. Then click **Finish**.
13. Request a certificate using a local CA or public CA. For more information, see To request a certificate from a local CA or To request a certificate from a public CA.

To install the certificate using IIS 6.0:

1. From Internet Information Services (IIS) Manager dialog box, right-click **Default Web Site**, and select **Properties**.
2. From the Directory Security tab, select **Server Certificate** to open the Web Server Certificate Wizard, and click **Next**.
3. Select **Process the pending request and install the certificate**, and click **Next**.
4. Browse to the location of the text file, and click **Next**.
5. Leave the default port as 443, and click **Next**.
6. Review the certificate summary. Click **Next**, then click **Finish**.
7. From Internet Information Services (IIS) Manager dialog box, right-click **Default Web Site**, and select **Properties**.
8. From the Directory Security tab, select **Edit**.
9. Select the **Require secure channel** check box, and click **OK**.

To request a certificate from a local CA

1. From a web browser, enter *https://<Local_Certification_Authority_computer>/certsrv*
2. Click **Request a certificate**, then **Advanced certificate request**.
3. 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**.
4. Open the text file where you save the certificate request.
5. 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.
6. In the **Certificate Template** box, select **Web Server**. Click **Submit**.

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

8 Save the file.

To request a certificate from a public CA

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

To create a SAN certificate

This procedure lets you configure a single certificate to answer for multiple addresses. 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 your 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 it later on the list. 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 default first website:

1 On the CMN F/B computer, in IIS Manager: Select **Default Web Site**.

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 CMN 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, CMN is installed with the *log4net* utility to generate log files of CMN components' activity. This information is critical to diagnosing any configuration issues that may arise. Logging is enabled by default for all CMN components.

The default configurations will be suitable for most organizations and circumstances, but you can customize logging features. The *log4net* utility may be configured to work a particular way with each CMN component. Configuration instructions are nearly identical for all components, so we present the instructions separately, in Appendix C of the *User Guide*.

4-5 (conditional): Configuring CMN's FBC for Domino clusters

CMN supports Domino server clusters (ClusterNode1 and ClusterNode2) that provide Lotus Notes mail service in an active/standby redundancy configuration. In this case, a single CMN Web Server is required to support both Domino Servers. Follow the procedures below to set up this configuration. Initially, ClusterNode1 is the active Domino server.

To install and configure CMN's FBC for the active Domino server in a cluster:

1 Ensure that the Domino Admin client installed in the CMN Web Server is able to connect to both Domino servers.

2 Install and configure CMN to support ClusterNode1, as per normal procedures.

3 Ensure that Free/Busy information is retrieved correctly in both directions using ClusterNode1.

To enable the second Domino server in a cluster to support retrieval of Domino F/B information by Exchange:

1. Failover to the standby server in the Domino Server cluster. (ClusterNode2 is now active.)
2. Ensure the Domino Admin client is connected to ClusterNode2.
3. At the CMN Web Server, stop the CMN Domino F/B Connector service.
4. At the CMN Web Server, open the PowerShell and type:
   Set-CmnDominoFreeBusyConfig -DominoServerName <ClusterNode2ServerName>
5. Restart the CMN Domino Free/Busy Connector service.
6. Ensure that Domino Free/Busy information is retrieved correctly by Exchange users (using ClusterNode2).
7. Failover to the standby server in the Domino Server cluster. ClusterNode1 is now active.
8. Ensure that Domino Free/Busy information continues to be retrieved correctly by Exchange users (using ClusterNode1).

To enable the second Domino server in a cluster to retrieve Exchange free/busy information:

1. Install QCalCon in ClusterNode2. See 2-1: Physically install the CMN QCalCon task. (QCalCon was installed in ClusterNode1 during step 2 of the initial procedure of this series.)
2. Configure QCalCon in ClusterNode2 to point to the CMN Exchange Server (where the CMN Exchange F/B Connector Service is installed).
3. Failover to the Standby server in the Domino Server cluster to make ClusterNode2 the active server (if it is not already the active server).
4. Ensure that free/busy information from Exchange is retrieved correctly by Domino users (using ClusterNode2).
5. Perform final tests to ensure that free/busy information from Exchange is successfully retrieved using either Domino server in the cluster.

4-6: Run CMN's Management Console to configure FBC components

Use CMN'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 CMN *User Guide* for field notes and application notes for each screen in the F/B Connector Management Console.

IMPORTANT: For a hybrid Office 365, be sure to specify the EWS endpoint in the CMN F/B Connector Management Console.

- If the EWS URL points to the on-premises environment, clear the **Exchange Online** check box, and fill in the **Exchange Username** and **Exchange Password** boxes with the coexistence admin's credentials for the on-prem Active Directory.
- If the EWS URL points to the Exchange Online, select the **Exchange Online** check box, fill details in the **Tenant ID**, **Client ID** and **Client Secret** fields with the coexistence admin's credentials for the Cloud.

NOTE: You may use PowerShell commands to configure CMN Free/Busy Connector components, instead of CMN's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Configuring and troubleshooting the F/B Connector with PowerShell in chapter 1 of this *Scenarios Guide*.

Step 5: Configure and test connections among Notes/Domino, Exchange and CMN's FBC Web Server

5-1: Synchronize Exchange and Domino directories

Before using CMN's Free/Busy Connector, both directories should be updated to include representative objects for users in both systems. For best results, Quest recommends the CMN Directory Connector for this purpose. The Directory Connector is another CMN component that may already be installed and configured. For more information about the CMN Directory Connector, see *User Guide* chapter 2.

Use CMN's Directory Connector to define a bidirectional update (a pair of single-direction updates, in opposite directions, run sequentially)—if you do not have such a pair already defined.

Schedule the DC connector to run automatically at a frequency to keep both directories current throughout the coexistence period.

You may choose instead to perform a directory synchronization manually, in which case you may follow the two procedures below.

To synchronize Domino mail users to Exchange contacts:

1. Using the Exchange Management Console, create a mail contact for a Domino user account.
2. Ensure that the Exchange contact has a primary external SMTP address set to the same value as the *InternetAddress* property for the Lotus Notes mail user account.
3. Repeat the above steps for each Lotus Notes mail user account.

To synchronize Exchange mail users to Domino contacts:

1. Ensure that a Foreign Domain document has been created. To create a Foreign Domain document:
    a. As a Domino Administrator, select the **Configuration** tab.
    b. Select **Messaging | Domains**, then click **Add Domain**.
    c. Select the **Basics** tab. In the *Foreign domain name* box, enter a fictitious domain name (for example, *CMNFreeBusy*). This forces Domino to direct queries to QCalCon rather than to internal queues. Quest recommends using subdomains with the F/B Connector if feasible.

    The name of the foreign SMTP domain must be prepended by an asterisk, for example: **Exchange.sitraka.com*. This forces Domino to direct queries to QCalCon rather than to internal queues. Quest recommends using subdomains with the F/B Connector if feasible.
    d. Select the **Mail Information** tab. Enter the Gateway server name where the QCalCon Domino Server Task is installed.
    e. Enter the Gateway mail file name: *mail.box*
    f. Click the **Calendar Information** tab, and enter the Calendar server name of the server running QCalCon Domino Server Task.
    g. In the Calendar system, enter: *mail.box*
2. Create a new Person Document using Lotus Notes.
3. Set the mail type to *Other Internet Mail*.
4. Set the *CalendarDomain* property to the same value as the *CalendarSystem* property of the Foreign Domain document. (This permits configuration of CMN's Free/Busy Domino server task, QCalCon.)
5. Set the *InternetAddress* property of the Person Document to the Exchange SMTP email address.

5-2: Configure Exchange server connections

Configure and verify the link from the Exchange Server to the domains/subdomains supported by the Domino Server. This procedure tests whether the certificate on the CMN Web Server is trusted by the Exchange Server.

To configure the Exchange Server link to the CMN 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 Domino 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 CMN 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.

To enable shared SMTP namespace F/B lookups in the Exchange-to- Notes direction: Add the CMN F/B Web Services IP address to the host file on the Exchange CAS server.

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 CMN. For more information, see this Microsoft article.

Configure DNS (Domain Name System)

Configure DNS to point *autodiscover.<smtpdomain.com>* to the computer where CMN'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 Domino server, through the CMN Free/Busy Connector, you must make the CMN Autodiscover Web Service resolvable to this URL:

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

4

Non-hybrid O365 using shared (single) namespace

Follow these steps, in order as presented here, to install and configure CMN's Free/Busy Connector for a non-hybrid Office 365 environment with a shared (single) namespace:

- Step 1: Plan your FBC installation and configuration
- Step 2: Configure the Notes/Domino side
- Step 3: Configure the O365 side
- Step 4: Configure CMN's FBC Web Server
- Step 5: Configure and test connections among Notes/Domino, O365 and CMN's FBC Web Server

Step 1: Plan your FBC installation and configuration

To plan your overall FBC installation and configuration:

- 1-1: Verify system requirements
- 1-2: Make a configuration map
- 1-3: Complete the CMN FBC Planning Worksheet

1-1: Verify system requirements

Review the system requirements (in the CMN *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.

1-2: 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 decide how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers. For technical reasons, the QCalCon component of the Free/Busy Connector *must* be installed on a Domino server. But if the Domino environment contains more than one Domino server, QCalCon is installed on only one server. (Other Domino servers can find and use a single QCalCon instance on a "bridgehead" server.) The other four Free/Busy Connector components can be installed on a single computer, although deployment to two separate computers will improve performance in environments with higher volumes of F/B queries and replies.

When Free/Busy Connector components are deployed to two computers, they are typically installed like this:

- Computer 1, for Domino queries of Exchange users (and Exchange replies with F/B info): hosts the CMN Exchange Free/Busy Service.

- Computer 2, for Exchange queries of Domino users (and Domino replies with F/B info): hosts the CMN Domino Free/Busy Service, and the CMN Autodiscover and EWS web services.

1-3: Complete the CMN FBC Planning Worksheet

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

Step 2: Configure the Notes/Domino side

A particular configuration of the Notes/Domino environment works best in most environments for compatibility with CMN's Free/Busy Connector. This section explains how to achieve the recommended configuration.

To configure the Notes/Domino side:

- 2-1: Physically install the CMN QCalCon task
- 2-2: Configure Domino Person documents
- 2-3: Add the domain documents
- 2-4: Set up the foreign SMTP document
- 2-5: Set up the server connection document
- 2-6: Add TCP/IP connection documents

If configuring CMN to support Domino clusters

CMN supports Domino server clusters (ClusterNode1 and ClusterNode2) that provide Lotus Notes mail service in an active/standby redundancy configuration. In this case, a single CMN Web Server is required to support both Domino Servers.

Some Domino configuration steps are required for this scenario, but they occur only after the CMN FBC Web Server is configured (in Step 4 below). Complete the steps here to configure the rest of the Notes/Domino side, and then you will configure support for Domino clusters later in Step 4.

2-1: Physically install the CMN QCalCon task

CMN's QCalCon is a Domino server task that facilitates communications between the Domino and Exchange servers, for transmitting Domino F/B queries to Exchange, and receiving F/B information from Exchange.

Run the CMN Autorun installer to install QCalCon to the Domino server. AutoRun offers the choice of a 32-bit or 64-bit edition of QCalCon. Choose the edition that matches the local Domino software edition (32- vs. 64-bit). (The host computer's operating system is irrelevant to this choice.)

The AutoRun installer automatically checks the environment to verify CMN prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command before executing.

To configure CMN's F/B Connector for multiple Domino servers

In a Domino environment containing more than one Domino server, QCalCon is typically installed on only one "bridgehead" server. A Domino admin then configures the non-QCalCon servers to route their local users' F/B queries to the QCalCon bridgehead server.

NOTE: Some admins with multiple Domino 6.5.x servers (only) report that non-bridgehead Domino 6.5.x servers are unable to route F/B queries to a QCalCon bridgehead server. IBM (in this article) says only: "Domino [6.5.x or earlier] does not support this type of configuration for free time lookup." Despite the IBM disclaimer, CMN's Free/Busy Connector does work in many such environments if its QCalCon server task is installed on *all* Domino 6.5.x servers.

2-2: Configure Domino Person documents

NOTE: This configuration is necessary in most environments, but in most cases it would be impractical to repeat these steps for every Exchange user. Instead, consider using CMN's Directory Connector to automate this task. The CMN Directory Connector correctly synchronizes the contacts to support Free/Busy Connector operations in our recommended configuration.

IMPORTANT: CMN's F/B Connector requires that each user's SMTP forwarding address appear in the Domino *User name* field, although it can appear in any position within that field (first, middle or last).

For each user, begin with the semi-standard settings, including the calendar domain on the *Miscellaneous* tab. Then:

1. Set the **Mail system** to *Notes*, so the **Mail server** field can be populated with a server that is valid in the environment. (There is no need to specify a **Mail file**; only the **Mail server** must be modified.)
2. **Save & Close** the contact.
3. Reopen the contact, and change the **Mail system** back to **Other Internet Mail**. (This will hide the **Mail server** field, but the field is still populated even though it does not appear—necessary only when creating contacts manually.)
4. **Save & Close** the contact.

2-3: Add the domain documents

You will need a foreign domain with a name that matches the name in the **Calendar system** field.

Add a Notes foreign domain document. The *Mail Information* and *Calendar Information* tabs should have the gateway and calendar server name pointing to the location of the QCalCon server, using the Notes qualified server name. (QCalCon should already be installed and configured according to the *CMN User Guide* instructions.) The **Gateway mail file name** (on the *Mail Info* tab) and **Calendar system** (*Calendar Info* tab) must both be set to *Mail.box*. In environments that use multiple *mail.box* files, the name should match one of those files (typically *mail1.box*, *mail2.box*, etc.).

2-4: Set up the foreign SMTP document

The configuration settings for CMN are all on the *Routing* tab. All the settings on the other tabs are left at their respective defaults.

1. The **Internet Domain** field must be set to the name of the domain you will use for the Exchange users. Note that the **Internet Domain** value must begin with an asterisk as the first character of the name, *with no dot*—just an asterisk and then the FQDN.
2. The **Domain name** must be entered as *CMNOUT*, to match with a connection document that will be set up next.

2-5: Set up the server connection document

This Connection Document is used both for the Free/Busy Connector and for mail-routing.

1. On the *Basics* tab: Set the **Connection type** to *SMTP*, and the **Source server** is the server where the F/B request will originate.
2. To accommodate multiple mail servers, set up just one *Server Connection* document with the **Source server** set so that any of those servers can use this same document:
   - ***Source Domain*** (field appears in some but not all Domino versions): The Domino domain.
   - ***Connect via:*** Set to *Direct connection*.
   - ***Destination server:*** Can be any arbitrary name you want to assign.

- ***Destination domain:*** Should be set to *CMNOUT*, to match the **Domain name** in the *Foreign SMTP Document* (set up in the preceding section). You can use some other value, but the **Destination domain** value here must match the **Foreign SMTP Domain** name. Note this is a "virtual domain," not a real domain. It doesn't really exist or go anywhere, but we use these fields to get Domino to match documents and route mail the way we want.

3 Set the **SMTP MTA relay host** to the IP address of the CMN Mail Connector.

4 On the *Replication/Routing* tab (for the same connection document): The **Replication task** should be *Disabled*, and the **Routing task** should be set to *Mail Routing* or *SMTP Mail Routing*, depending on the setup of your environment.

5 On the *Schedule* tab (for the same connection document): Set this connection document to be enabled 24 hours per day.

2-6: Add TCP/IP connection documents

In some environments, free/busy lookups may also require that you add TCP/IP Connection documents in both directions between the Domino servers housing mail databases (mailbox servers) and the Domino server running the QCalCon Domino Server Task.

NOTE: This step may not be necessary if internal TCP/IP communications are already established in the environment. The bottom-line requirement is that the QCalCon server must be able to communicate with other servers.

To add TCP/IP connection documents: In Domino Admin, expand *Configuration*, expand *Messaging* and then click **Connections**. Add a connection, and then:

1 On the *Basics* tab:

- ***Connection type:*** Local Area Network.
- ***Source Server:*** name of the Domino server (in the Notes / Domino format, e.g. source_Notes_mail_database_server/DOMINODOMAIN).
- ***Use the port(s):*** TCP/IP.
- ***Usage priority:*** Normal.
- ***Destination server:*** the Domino server hosting the QCalCon Domino Server Task (in the Notes / Domino format, e.g. *target_Notes_QCalCon_server/DOMINODOMAIN*).
- ***Destination domain:*** DOMINODOMAIN of the server running the QCalCon Domino Server Task.
- ***Optional network address:*** IP address of the destination server.

IMPORTANT: Remember that a TCP/IP Connection document is required in both directions. The *Basics* tab settings must be reversed on the other TCP/IP Connection document to define a connection in the other direction. The net result of this configuration with a Domino mail database server and the QCalCon Domino Server Task running on a separate Domino server is that you will have two TCP/IP Connection documents, with one document pair for each Domino mail database server.

2 On the *Replication/Routing* tab:

- ***Replication task:*** Disabled.
- ***Routing task:*** Mail Routing.
- ***Route at once if:*** 1 messages pending.

3 On the *Schedule* tab: Modify the settings on this tab to meet sending requirements (24 hours).

4 Click **Save and Close**.

Step 3: Configure the O365 side

To configure a non-hybrid Office 365 for CMN's F/B Connector in a single/shared namespace environment:

1. In O365, configure an outbound send connector to point to CMN's Mail Connector, to facilitate mail flow apart from free/busy.
2. Configure an Autodiscover website for CMN 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 CMN website could be, for example, *coexist.x.y*. The CMN 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 *Add-AvailabilityAddressSpace* cmdlet for the CMN Autodiscover address ("*coexist.x.y*") configured in step 2 above.
4. In DNS, make sure the *coexist* domain has an A record pointing to CMN.
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 O365 for multiple subdomains

CMN's Free/Busy Connector can facilitate the flow of free/busy information among multiple subdomains supported by both the Exchange and Domino servers. To support this scenario, run the *Add-AvailabilityAddressSpace* cmdlet on O365 for each Domino SMTP domain supported.

Step 4: Configure CMN's FBC Web Server

To configure CMN's FBC Web Server:

- 4-1: Physically install the CMN 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 (conditional): Configuring CMN's FBC for Domino clusters
- 4-6: Run CMN's Management Console to configure FBC components

4-1: Physically install the CMN FBC components

All CMN FBC components are installed by the AutoRun utility that accompanies the CMN product kit.

The AutoRun installer automatically checks the environment to verify CMN prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command before executing.

For a typical configuration:

- ***On the CMN FBC Web Server:*** Run AutoRun to install the Autodiscover, EWS and the Domino FBC Service on the CMN FBC Web Server.
- ***On either the same CMN FBC Web Server or a separate CMN Exchange FBC Server:*** Run AutoRun to install the CMN Exchange FBC Service.

To configure CMN's F/B Connector for multiple Domino servers

For Exchange queries for Domino F/B information, the simplest approach is to dedicate a separate CMN FBC server for each Domino server, with all the CMN servers feeding into the single Exchange server. It is technically possible, but somewhat more complicated, to configure a single instance of the Domino FBC Service, EWS and

Autodiscover to process free/busy traffic to and from multiple Domino servers—an approach that requires more elaborate Domino configurations.

4-2: Obtain and install web services certificates

CMN Web Server components must accept SSL connections from the mail systems. 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 Notes Server. The certificate is valid for the Autodiscover and EWS web services.

You can obtain a certificate from either of two sources:

- 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.

> **NOTE:** You can request a certificate using Web enrollment pages. For more information, see http://support.microsoft.com/kb/931351.
>
> **If you need a multi-domain certificate:** See To create a SAN certificate.

When you receive the certificate, you must install it on the appropriate server.

To configure the certificate for multi-domain support

The Free/Busy Connector can facilitate the exchange of free/busy information among multiple subdomains supported by both the Exchange and Domino servers. For a multi-domain scenario, ensure the certificate used on the CMN Web Server has subject alternate names for all associated autodiscover host names.

To request and install a certificate using IIS 7.0

To request a certificate using IIS 7.0:

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. For more information, see To request a certificate from a local CA or To request a certificate from a public CA.

To install the certificate using IIS 7.0:

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**.

> ***To create an https binding for the web site using IIS 7.0:***
>
> 1. From the *Connection* pane in IIS, select **Default Web Sites**.
> 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 request and install a certificate using IIS 6.0

To request a certificate using IIS 6.0:

1. From Internet Information Services (IIS) Manager dialog box, right-click **Default Web Site**, and select **Properties**.
2. From the Directory Security tab, select **Server Certificate** to open the Web Server Certificate Wizard.
3. Click **Next**.
4. Select **Create a new certificate request**, and click **Next**.
5. Select **Prepare the request now, but send it later**, and click **Next**.
6. Accept the defaults. Ensure **Select cryptographic service provider (CSP) for this certificate** is checked, and click **Next**.
7. Select **Microsoft RSA SChannel Cryptographic Provider**, and click **Next**.
8. Select or enter your organization's name and organizational unit, and click **Next**.
9. Enter *autodiscover.*<*smtpdomain*> —or— <*smtpdomain*> as the common name, for the primary domain and all required subdomains. Then click **Next**.
10. Enter the geographical information, and click **Next**.
11. Specify a file name to save the certificate request, and click **Next**.
12. Review the information, and click **Next**. Then click **Finish**.
13. Request a certificate using a local CA or public CA. For more information, see To request a certificate from a local CA or To request a certificate from a public CA.

To install the certificate using IIS 6.0:

1. From Internet Information Services (IIS) Manager dialog box, right-click **Default Web Site**, and select **Properties**.
2. From the Directory Security tab, select **Server Certificate** to open the Web Server Certificate Wizard, and click **Next**.
3. Select **Process the pending request and install the certificate**, and click **Next**.
4. Browse to the location of the text file, and click **Next**.
5. Leave the default port as 443, and click **Next**.
6. Review the certificate summary. Click **Next**, then click **Finish**.
7. From Internet Information Services (IIS) Manager dialog box, right-click **Default Web Site**, and select **Properties**.
8. From the Directory Security tab, select **Edit**.
9. Select the **Require secure channel** check box, and click **OK**.

To request a certificate from a local CA

1. From a web browser, enter *https://<Local_Certification_Authority_computer>/certsrv*
2. Click **Request a certificate**, then **Advanced certificate request**.
3. 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**.
4. Open the text file where you save the certificate request.
5. 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.
6. In the **Certificate Template** box, select **Web Server**. Click **Submit**.

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

8 Save the file.

To request a certificate from a public CA

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

To create a SAN certificate

This procedure lets you configure a single certificate to answer for multiple addresses. 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 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 it later on the list. 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 default first website:

1 On the CMN F/B computer, in IIS Manager: Select **Default Web Site**.

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 CMN 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, CMN is installed with the *log4net* utility to generate log files of CMN components' activity. This information is critical to diagnosing any configuration issues that may arise. Logging is enabled by default for all CMN components.

The default configurations will be suitable for most organizations and circumstances, but you can customize logging features. The *log4net* utility may be configured to work a particular way with each CMN component. Configuration instructions are nearly identical for all components, so we present the instructions separately, in Appendix C of the *User Guide*.

4-5 (conditional): Configuring CMN's FBC for Domino clusters

CMN supports Domino server clusters (ClusterNode1 and ClusterNode2) that provide Lotus Notes mail service in an active/standby redundancy configuration. In this case, a single CMN Web Server is required to support both Domino Servers. Follow the procedures below to set up this configuration. Initially, ClusterNode1 is the active Domino server.

To install and configure CMN's FBC for the active Domino server in a cluster:

1 Ensure that the Domino Admin client installed in the CMN Web Server is able to connect to both Domino servers.

2 Install and configure CMN to support ClusterNode1, as per normal procedures.

3 Ensure that Free/Busy information is retrieved correctly in both directions using ClusterNode1.

To enable the second Domino server in a cluster to support retrieval of Domino F/B information by Exchange:

1. Failover to the standby server in the Domino Server cluster. (ClusterNode2 is now active.)
2. Ensure the Domino Admin client is connected to ClusterNode2.
3. At the CMN Web Server, stop the CMN Domino F/B Connector service.
4. At the CMN Web Server, open the PowerShell and type:
   Set-CmnDominoFreeBusyConfig -DominoServerName <ClusterNode2ServerName>
5. Restart the CMN Domino Free/Busy Connector service.
6. Ensure that Domino Free/Busy information is retrieved correctly by Exchange users (using ClusterNode2).
7. Failover to the standby server in the Domino Server cluster. ClusterNode1 is now active.
8. Ensure that Domino Free/Busy information continues to be retrieved correctly by Exchange users (using ClusterNode1).

To enable the second Domino server in a cluster to retrieve Exchange free/busy information:

1. Install QCalCon in ClusterNode2. See 2-1: Physically install the CMN QCalCon task. (QCalCon was installed in ClusterNode1 during step 2 of the initial procedure of this series.)
2. Configure QCalCon in ClusterNode2 to point to the CMN Exchange Server (where the CMN Exchange F/B Connector Service is installed).
3. Failover to the Standby server in the Domino Server cluster to make ClusterNode2 the active server (if it is not already the active server).
4. Ensure that free/busy information from Exchange is retrieved correctly by Domino users (using ClusterNode2).
5. Perform final tests to ensure that free/busy information from Exchange is successfully retrieved using either Domino server in the cluster.

4-6: Run CMN's Management Console to configure FBC components

Use CMN'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 CMN *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 CMN Free/Busy Connector components, instead of CMN's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Configuring and troubleshooting the F/B Connector with PowerShell in chapter 1 of this *Scenarios Guide*.

Step 5: Configure and test connections among Notes/Domino, O365 and CMN's FBC Web Server

5-1: Synchronize Office 365 and Domino directories

Before running any of CMN's F/B Connector subcomponents, you must synchronize Notes/Domino users as Office 365 contacts, and O365 users to Domino. CMN's Directory Connector does not support directory

synchronizations directly between Domino 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 for this purpose. See Microsoft's *Azure* documentation for instructions and guidance in this synchronization.

5-2: Configure Office 365 connections

Configure and verify the link from Office 365 to the domains/subdomains supported by the Domino Server. This procedure tests whether the certificate on the CMN Web Server is trusted by O365.

To configure the O365 link to the CMN Web Server and verify that certificates are 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 CMN. For more information, see this Microsoft article.

Configure DNS (Domain Name System)

Configure DNS to point *autodiscover.<smtpdomain.com>* to the computer where CMN's Autodiscover service is installed. For each domain, Office 365 connects to predefined Autodiscover URLs using DNS host entries.

For Office 365 to get free/busy information from the domain supported by a Domino server, through the CMN Free/Busy Connector, you must make the CMN Autodiscover Web Service resolvable to this URL:

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

5

Non-hybrid O365 using separate namespaces

Follow these steps, in order as presented here, to install and configure CMN's Free/Busy Connector for a non-hybrid Office 365 environment with separate (multiple) namespaces:

- Step 1: Plan your FBC installation and configuration
- Step 2: Configure the Notes/Domino side
- Step 3: Configure the O365 side
- Step 4: Configure CMN's FBC Web Server
- Step 5: Configure and test connections among Notes/Domino, O365 and CMN's FBC Web Server

Step 1: Plan your FBC installation and configuration

To plan your overall FBC installation and configuration:

- 1-1: Verify system requirements
- 1-2: Make a configuration map
- 1-3: Complete the CMN FBC Planning Worksheet

1-1: Verify system requirements

Review the system requirements (in the CMN *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.

1-2: 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 decide how these will be addressed.

Then sketch out a configuration map to show which FBC components will reside on which computers. For technical reasons, the QCalCon component of the Free/Busy Connector *must* be installed on a Domino server. But if the Domino environment contains more than one Domino server, QCalCon is installed on only one server. (Other Domino servers can find and use a single QCalCon instance on a "bridgehead" server.) The other four Free/Busy Connector components can be installed on a single computer, although deployment to two separate computers will improve performance in environments with higher volumes of F/B queries and replies.

When Free/Busy Connector components are deployed to two computers, they are typically installed like this:

- Computer 1, for Domino queries of Exchange users (and Exchange replies with F/B info): hosts the CMN Exchange Free/Busy Service.

- Computer 2, for Exchange queries of Domino users (and Domino replies with F/B info): hosts the CMN Domino Free/Busy Service, and the CMN Autodiscover and EWS web services.

1-3: Complete the CMN FBC Planning Worksheet

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

Step 2: Configure the Notes/Domino side

A particular configuration of the Notes/Domino environment works best in most environments for compatibility with CMN's Free/Busy Connector. This section explains how to achieve the recommended configuration.

To configure the Notes/Domino side:

- 2-1: Physically install the CMN QCalCon task
- 2-2: Configure Domino Person documents
- 2-3: Add the domain documents
- 2-4: Set up the foreign SMTP document
- 2-5: Set up the server connection document
- 2-6: Add TCP/IP connection documents

If configuring CMN to support Domino clusters

CMN supports Domino server clusters (ClusterNode1 and ClusterNode2) that provide Lotus Notes mail service in an active/standby redundancy configuration. In this case, a single CMN Web Server is required to support both Domino Servers.

Some Domino configuration steps are required for this scenario, but they occur only after the CMN FBC Web Server is configured (in Step 4 below). Complete the steps here to configure the rest of the Notes/Domino side, and then you will configure support for Domino clusters later in Step 4.

2-1: Physically install the CMN QCalCon task

CMN's QCalCon is a Domino server task that facilitates communications between the Domino and Exchange servers, for transmitting Domino F/B queries to Exchange, and receiving F/B information from Exchange.

Run the CMN Autorun installer to install QCalCon to the Domino server. AutoRun offers the choice of a 32-bit or 64-bit edition of QCalCon. Choose the edition that matches the local Domino software edition (32- vs. 64-bit). (The host computer's operating system is irrelevant to this choice.)

The AutoRun installer automatically checks the environment to verify CMN prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command before executing.

To configure CMN's F/B Connector for multiple Domino servers

In a Domino environment containing more than one Domino server, QCalCon is typically installed on only one "bridgehead" server. A Domino admin then configures the non-QCalCon servers to route their local users' F/B queries to the QCalCon bridgehead server.

NOTE: Some admins with multiple Domino 6.5.x servers (only) report that non-bridgehead Domino 6.5.x servers are unable to route F/B queries to a QCalCon bridgehead server. IBM (in this article) says only: "Domino [6.5.x or earlier] does not support this type of configuration for free time lookup." Despite the IBM disclaimer, CMN's Free/Busy Connector does work in many such environments if its QCalCon server task is installed on *all* Domino 6.5.x servers.

2-2: Configure Domino Person documents

NOTE: This configuration is necessary in most environments, but in most cases it would be impractical to repeat these steps for every Exchange user. Instead, consider using CMN's Directory Connector to automate this task. The CMN Directory Connector correctly synchronizes the contacts to support Free/Busy Connector operations in our recommended configuration.

IMPORTANT: CMN's F/B Connector requires that each user's SMTP forwarding address appear in the Domino *User name* field, although it can appear in any position within that field (first, middle or last).

For each user, begin with the semi-standard settings, including the calendar domain on the *Miscellaneous* tab. Then:

1. Set the **Mail system** to *Notes*, so the **Mail server** field can be populated with a server that is valid in the environment. (There is no need to specify a **Mail file**; only the **Mail server** must be modified.)
2. **Save & Close** the contact.
3. Reopen the contact, and change the **Mail system** back to **Other Internet Mail**. (This will hide the **Mail server** field, but the field is still populated even though it does not appear—necessary only when creating contacts manually.)
4. **Save & Close** the contact.

2-3: Add the domain documents

You will need a foreign domain with a name that matches the name in the **Calendar system** field.

Add a Notes foreign domain document. The *Mail Information* and *Calendar Information* tabs should have the gateway and calendar server name pointing to the location of the QCalCon server, using the Notes qualified server name. (QCalCon should already be installed and configured according to the *CMN User Guide* instructions.) The **Gateway mail file name** (on the *Mail Info* tab) and **Calendar system** (*Calendar Info* tab) must both be set to *Mail.box*. In environments that use multiple *mail.box* files, the name should match one of those files (typically *mail1.box*, *mail2.box*, etc.).

2-4: Set up the foreign SMTP document

The configuration settings for CMN are all on the *Routing* tab. All the settings on the other tabs are left at their respective defaults.

1. The **Internet Domain** field must be set to the name of the domain you will use for the Exchange users. Note that the **Internet Domain** value must begin with an asterisk as the first character of the name, *with no dot*—just an asterisk and then the FQDN.
2. The **Domain name** must be entered as *CMNOUT*, to match with a connection document that will be set up next.

2-5: Set up the server connection document

This Connection Document is used both for the Free/Busy Connector and for mail-routing.

1. On the *Basics* tab: Set the **Connection type** to *SMTP*, and the **Source server** is the server where the F/B request will originate.
2. To accommodate multiple mail servers, set up just one *Server Connection* document with the **Source server** set so that any of those servers can use this same document:
   - ***Source Domain*** (field appears in some but not all Domino versions): The Domino domain.
   - ***Connect via:*** Set to *Direct connection*.
   - ***Destination server:*** Can be any arbitrary name you want to assign.

- ***Destination domain:*** Should be set to *CMNOUT*, to match the **Domain name** in the *Foreign SMTP Document* (set up in the preceding section). You can use some other value, but the **Destination domain** value here must match the **Foreign SMTP Domain** name. Note this is a "virtual domain," not a real domain. It doesn't really exist or go anywhere, but we use these fields to get Domino to match documents and route mail the way we want.

3 Set the **SMTP MTA relay host** to the IP address of the CMN Mail Connector.

4 On the *Replication/Routing* tab (for the same connection document): The **Replication task** should be *Disabled*, and the **Routing task** should be set to *Mail Routing* or *SMTP Mail Routing*, depending on the setup of your environment.

5 On the *Schedule* tab (for the same connection document): Set this connection document to be enabled 24 hours per day.

2-6: Add TCP/IP connection documents

In some environments, free/busy lookups may also require that you add TCP/IP Connection documents in both directions between the Domino servers housing mail databases (mailbox servers) and the Domino server running the QCalCon Domino Server Task.

NOTE: This step may not be necessary if internal TCP/IP communications are already established in the environment. The bottom-line requirement is that the QCalCon server must be able to communicate with other servers.

To add TCP/IP connection documents: In Domino Admin, expand *Configuration*, expand *Messaging* and then click **Connections**. Add a connection, and then:

1 On the *Basics* tab:

- ***Connection type:*** Local Area Network.
- ***Source Server:*** name of the Domino server (in the Notes / Domino format, e.g. source_Notes_mail_database_server/DOMINODOMAIN).
- ***Use the port(s):*** TCP/IP.
- ***Usage priority:*** Normal.
- ***Destination server:*** the Domino server hosting the QCalCon Domino Server Task (in the Notes / Domino format, e.g. *target_Notes_QCalCon_server/DOMINODOMAIN*).
- ***Destination domain:*** DOMINODOMAIN of the server running the QCalCon Domino Server Task.
- ***Optional network address:*** IP address of the destination server.

IMPORTANT: Remember that a TCP/IP Connection document is required in both directions. The *Basics* tab settings must be reversed on the other TCP/IP Connection document to define a connection in the other direction. The net result of this configuration with a Domino mail database server and the QCalCon Domino Server Task running on a separate Domino server is that you will have two TCP/IP Connection documents, with one document pair for each Domino mail database server.

2 On the *Replication/Routing* tab:

- ***Replication task:*** Disabled.
- ***Routing task:*** Mail Routing.
- ***Route at once if:*** 1 messages pending.

3 On the *Schedule* tab: Modify the settings on this tab to meet sending requirements (24 hours).

4 Click **Save and Close**.

Step 3: Configure the O365 side

To configure a non-hybrid Office 365 for CMN's F/B Connector in a separate/multiple namespace environment:

1. In DNS, make sure the *coexist* domain has an A record pointing to CMN.
2. Configure an Autodiscover website for CMN (for example, *Autodiscover.x.y*, where the "*x.y*" domain is the SMTP address to the right of the @ symbol). The CMN 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 CMN 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 O365 for multiple subdomains

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

Step 4: Configure CMN's FBC Web Server

To configure CMN's FBC Web Server:

- 4-1: Physically install the CMN 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 (conditional): Configuring CMN's FBC for Domino clusters
- 4-6: Run CMN's Management Console to configure FBC components

4-1: Physically install the CMN FBC components

All CMN FBC components are installed by the AutoRun utility that accompanies the CMN product kit.

The AutoRun installer automatically checks the environment to verify CMN prerequisites, but you can bypass the prerequisites check by running the installer from the command line and appending *ignoreprerequisites=1* to the command before executing.

For a typical configuration:

- ***On the CMN FBC Web Server:*** Run AutoRun to install the Autodiscover, EWS and the Domino FBC Service on the CMN FBC Web Server.
- ***On either the same CMN FBC Web Server or a separate CMN Exchange FBC Server:*** Run AutoRun to install the CMN Exchange FBC Service.

To configure CMN's F/B Connector for multiple Domino servers

For Exchange queries for Domino F/B information, the simplest approach is to dedicate a separate CMN FBC server for each Domino server, with all the CMN servers feeding into the single Exchange server. It is technically possible, but somewhat more complicated, to configure a single instance of the Domino FBC Service, EWS and Autodiscover to process free/busy traffic to and from multiple Domino servers—an approach that requires more elaborate Domino configurations.

4-2: Obtain and install web services certificates

CMN Web Server components must accept SSL connections from the mail systems. 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 Notes Server. The certificate is valid for the Autodiscover and EWS web services.

You can obtain a certificate from either of two sources:

- 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.

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

If you need a multi-domain certificate: See To create a SAN certificate.

When you receive the certificate, you must install it on the appropriate server.

To configure the certificate for multi-domain support

The Free/Busy Connector can facilitate the exchange of free/busy information among multiple subdomains supported by both the Exchange and Domino servers. For a multi-domain scenario, ensure the certificate used on the CMN Web Server has subject alternate names for all associated autodiscover host names.

To request and install a certificate using IIS 7.0

To request a certificate using IIS 7.0:

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. For more information, see To request a certificate from a local CA or To request a certificate from a public CA.

To install the certificate using IIS 7.0:

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**.

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

1. From the *Connection* pane in IIS, select **Default Web Sites**.
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 request and install a certificate using IIS 6.0

To request a certificate using IIS 6.0:

1. From Internet Information Services (IIS) Manager dialog box, right-click **Default Web Site**, and select **Properties**.
2. From the Directory Security tab, select **Server Certificate** to open the Web Server Certificate Wizard.
3. Click **Next**.
4. Select **Create a new certificate request**, and click **Next**.
5. Select **Prepare the request now, but send it later**, and click **Next**.
6. Accept the defaults. Ensure **Select cryptographic service provider (CSP) for this certificate** is checked, and click **Next**.
7. Select **Microsoft RSA SChannel Cryptographic Provider**, and click **Next**.
8. Select or enter your organization's name and organizational unit, and click **Next**.
9. Enter *autodiscover.*<*smtpdomain*> —or— <*smtpdomain*> as the common name, for the primary domain and all required subdomains. Then click **Next**.
10. Enter the geographical information, and click **Next**.
11. Specify a file name to save the certificate request, and click **Next**.
12. Review the information, and click **Next**. Then click **Finish**.
13. Request a certificate using a local CA or public CA. For more information, see To request a certificate from a local CA or To request a certificate from a public CA.

To install the certificate using IIS 6.0:

1. From Internet Information Services (IIS) Manager dialog box, right-click **Default Web Site**, and select **Properties**.
2. From the Directory Security tab, select **Server Certificate** to open the Web Server Certificate Wizard, and click **Next**.
3. Select **Process the pending request and install the certificate**, and click **Next**.
4. Browse to the location of the text file, and click **Next**.
5. Leave the default port as 443, and click **Next**.
6. Review the certificate summary. Click **Next**, then click **Finish**.
7. From Internet Information Services (IIS) Manager dialog box, right-click **Default Web Site**, and select **Properties**.
8. From the Directory Security tab, select **Edit**.
9. Select the **Require secure channel** check box, and click **OK**.

To request a certificate from a local CA

1. From a web browser, enter *https://<Local_Certification_Authority_computer>/certsrv*
2. Click **Request a certificate**, then **Advanced certificate request**.
3. 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**.
4. Open the text file where you save the certificate request.
5. 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.
6. In the **Certificate Template** box, select **Web Server**. Click **Submit**.

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

8 Save the file.

To request a certificate from a public CA

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

To create a SAN certificate

This procedure lets you configure a single certificate to answer for multiple addresses. 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 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 it later on the list. 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 default first website:

1 On the CMN F/B computer, in IIS Manager: Select **Default Web Site**.

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 CMN 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, CMN is installed with the *log4net* utility to generate log files of CMN components' activity. This information is critical to diagnosing any configuration issues that may arise. Logging is enabled by default for all CMN components.

The default configurations will be suitable for most organizations and circumstances, but you can customize logging features. The *log4net* utility may be configured to work a particular way with each CMN component. Configuration instructions are nearly identical for all components, so we present the instructions separately, in Appendix C of the *User Guide*.

4-5 (conditional): Configuring CMN's FBC for Domino clusters

CMN supports Domino server clusters (ClusterNode1 and ClusterNode2) that provide Lotus Notes mail service in an active/standby redundancy configuration. In this case, a single CMN Web Server is required to support both Domino Servers. Follow the procedures below to set up this configuration. Initially, ClusterNode1 is the active Domino server.

To install and configure CMN's FBC for the active Domino server in a cluster:

1 Ensure that the Domino Admin client installed in the CMN Web Server is able to connect to both Domino servers.

2 Install and configure CMN to support ClusterNode1, as per normal procedures.

3 Ensure that Free/Busy information is retrieved correctly in both directions using ClusterNode1.

To enable the second Domino server in a cluster to support retrieval of Domino F/B information by Exchange:

1. Failover to the standby server in the Domino Server cluster. (ClusterNode2 is now active.)
2. Ensure the Domino Admin client is connected to ClusterNode2.
3. At the CMN Web Server, stop the CMN Domino F/B Connector service.
4. At the CMN Web Server, open the PowerShell and type:
   Set-CmnDominoFreeBusyConfig -DominoServerName <ClusterNode2ServerName>
5. Restart the CMN Domino Free/Busy Connector service.
6. Ensure that Domino Free/Busy information is retrieved correctly by Exchange users (using ClusterNode2).
7. Failover to the standby server in the Domino Server cluster. ClusterNode1 is now active.
8. Ensure that Domino Free/Busy information continues to be retrieved correctly by Exchange users (using ClusterNode1).

To enable the second Domino server in a cluster to retrieve Exchange free/busy information:

1. Install QCalCon in ClusterNode2. See 2-1: Physically install the CMN QCalCon task. (QCalCon was installed in ClusterNode1 during step 2 of the initial procedure of this series.)
2. Configure QCalCon in ClusterNode2 to point to the CMN Exchange Server (where the CMN Exchange F/B Connector Service is installed).
3. Failover to the Standby server in the Domino Server cluster to make ClusterNode2 the active server (if it is not already the active server).
4. Ensure that free/busy information from Exchange is retrieved correctly by Domino users (using ClusterNode2).
5. Perform final tests to ensure that free/busy information from Exchange is successfully retrieved using either Domino server in the cluster.

4-6: Run CMN's Management Console to configure FBC components

Use CMN'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 CMN *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 CMN Free/Busy Connector components, instead of CMN's Management Console as described here. For information about using PowerShell to configure the Free/Busy Connector, see Configuring and troubleshooting the F/B Connector with PowerShell in chapter 1 of this *Scenarios Guide*.

Step 5: Configure and test connections among Notes/Domino, O365 and CMN's FBC Web Server

5-1: Synchronize Office 365 and Domino directories

Before running any of CMN's F/B Connector subcomponents, you must synchronize Notes/Domino users as Office 365 contacts, and O365 users to Domino. CMN's Directory Connector does not support directory

synchronizations directly between Domino 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 for this purpose. See Microsoft's *Azure* documentation for instructions and guidance in this synchronization.

5-2: Configure Office 365 connections

Configure and verify the link from Offi ce 365 to the domains/subdomains supported by the Domino Server. This procedure tests whether the certificate on the CMN Web Server is trusted by O365

To configure the O365 link to the CMN Web Server and verify that certificates are 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 CMN. For more information, see this Microsoft article.

Configure DNS (Domain Name System)

Configure DNS to point *autodiscover.<smtpdomain.com>* to the computer where CMN's Autodiscover service is installed. For each domain, Office 365 connects to predefined Autodiscover URLs using DNS host entries.

For Office 365 to get free/busy information from the domain supported by a Domino server, through the CMN Free/Busy Connector, you must make the CMN Autodiscover Web Service resolvable to this URL:

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

Appendix: FBC Planning Worksheet

Use this worksheet to gather and organize the information you will need to enter into CMN's Management Console application to configure the Free/Busy Connector (FBC).

QCalCon Domino Server Task | Qcalcon Settings

Gateway Mail File Name: Name of the gateway mailbox DB on the Domino server (e.g., *mail.box*). This should be the same as the Calendar system name.

Quest Exchange Free/Busy Connector Host Name: Name of the computer running the Exchange Free/Busy Connector Service.

Notes F/B Connector | Domino Free/Busy Settings

Domino Server Name: Name of the Domino server, used to gather F/B information of Notes users. For example, *NotesHost/NotesDomain* or *NotesHost*

Domino User Smtp Domain: Name of the Domino domain. For example, *domino.sitraka.com*

Domino Id File Path: Use the **Browse** feature (**[...]** button) to select the path and filename of the ID file that will be used to request F/B data from Domino, or just enter the path and filename into the text box.

Notes F/B Connector | Quest Web Services

Web Service Prefix: The first element of the name of the web service for the Domino Free/Busy Connector component. Typically this value is *autodiscover*, but this field permits an alternate web service prefix, to accommodate F/B coexistence with Exchange 2013 or Office 365 (Wave 14 or 15) where the prefix is configurable.

Quest Autodiscover Host Name: Host configured in DNS to run the CMN services and return Domino F/B information.

Quest EWS URL: The URL to the Quest Free/Busy Connector's EWS. For example: *https://<HostName>/EWS/Service.asmx*

Quest Domino Free/Busy Connector Host Name: Name of the computer where the Domino Free/Busy Connector is installed—typically this same computer (*localhost*).

Exchange F/B Connector | Exchange Free/Busy

Exchange Server Location: How should CMN's F/B Connector route free/busy queries to the coexisting Exchange environment? Mark (or circle) one of these, and collect the information associated with that option:

- **EWS Endpoint:** Select this option if you will coexist with an on-premises Exchange 2013 or 2010 environment with a single Exchange EWS whose location (URL) is fixed relative to CMN'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.

> **NOTE:** All queries for Exchange users' F/B information must pass through an Exchange EWS, which facilitates communications between Exchange and the CMN 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 E‘WS 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, CMN service will have to search the network for the connection.

- **Autodiscover Endpoint:** Select this option if you have an on-premises Exchange 2013 or 2010 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 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). If you select this option, you must also specify:
  - **Exchange Autodiscover URL:** Location of Autodiscover service on the Exchange server (or, for O365, of the MS Autodiscover URL, as noted below).

    > **NOTE:** ***If coexisting with Microsoft’s Office 365:*** Select the **Auto-discover 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 subject to change*, in which case this connection and the Free/Busy Connector would fail. Remember this if you set the Exchange Autodiscover URL to the Microsoft URL, and CMN’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 **Autodiscover Only** (below) instead.

- **Autodiscover Only:** Select this option if you will coexist with an Exchange 2013 or 2010 environment where you don't know the location of either the EWS or Autodiscover, such as in Microsoft's Office 365. 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 somewhat slower than either alternative above.

Exchange Username: Admin account the F/B Connector should use to access data and features in Office 365. Leave this field empty unless you are connecting to Office 365, or to a local on-premises Exchange that isn't in the same domain as the CMN admin server. In those cases an entry here is mandatory.

Appendix: Troubleshooting the FBC

This Appendix describes the most common problems encountered when installing and using CMN'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.** CMN problems are often traced back to inconsistences 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 CMN system requirements. System requirements are documented in the *Release Notes* that accompany every CMN RTM release.
- **Always ask yourself:**
  - **Is this a known limitation or known issue?** Check the *Known Limitations* appendix of the CMN *User Guide*, and the *Known Issues* section of the current CMN *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.

Free/Busy Connector Issues

F/B Connector does not run

A likely cause is insufficient IIS Virtual Memory. Try increasing IIS Virtual Memory to 768MB and perform an IIS Reset for the change to take effect.

Outlook crashes upon F/B lookup

If an Outlook client repeatedly crashes during F/B lookups, and you are running an Exchange 2013 or 2010 Client Access Server, the cause may be a known issue in the combination of .NET Framework 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.

Notes-to-Exchange F/B query connection fails with Office 365

If you are coexisting with Office 365, and CMN'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 the *Exchange Free/Busy* screen notes for the Exchange F/B Connector in CMN's Management Console, CMN *User Guide* chapter 4) 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 F/B 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 CMN's Free/Busy Connector has been configured, the cause likely is a name mismatch in the certificate. 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.

Lotus Notes users cannot see free/busy information for Exchange users

On the Domino server:

- Ensure the Person documents created for the Exchange users have the proper CalendarDomain property set. To do this:
    a Open the Domino Directory in Lotus Notes.
    b Right-click the Person Document for the Exchange user and click **Document Properties**
    c Ensure the CalendarDomain property matches the Calendar System specified in the Foreign Domain document.
- Ensure the Foreign Domain document has been created. The procedure to do this is in the respective scenario chapters, step 5-1 (*Synchronize Exchange and Domino directories*), under the heading *To synchronize Exchange mail users to Domino contacts*. After making changes to the Foreign Domain Document, restart the Domino server.
- Check connectivity between the Domino server and the computer running the CMN Free/Busy Connector.
- Make sure the QCalCon Domino Server task is running: From the Domino Console, type **Show Tasks**.

On the computer hosting the Exchange free/busy connector:

- Ensure the Exchange Free/Busy connector service is running as a domain user with access to the Exchange server. Try one of the following options:
    - Set the service logon credentials for the Quest CMN Exchange Free/Busy Connector service (see the *Exchange Free/Busy* screen notes for the Exchange F/B Connector in CMN's Management Console, CMN *User Guide* chapter 4).
    - Set the Exchange credentials using the *Set-CmnExchangeFreeBusyConfig* cmdlet.

  Try each of these methods if you are seeing errors in your event log when testing free/busy.
- Ensure the *EwsUrl* is properly configured to the Exchange Web Services URL for your Exchange server. If you are using a hosted Exchange or do not know what the Exchange Web Services URL is, use the *Get-CmnExchangeWebServicesUrl* cmdlet (see PowerShell to configure the F/B Connector).
- After verifying the *EwsUrl* is correct, navigate to the URL using a Web Browser such as Internet Explorer. Verify that you can access the URL using the same credentials used by the Exchange service without any additional credential prompts and without any certificate errors.
- Ensure the appropriate port is open on the Exchange Free/Busy Connector service computer for TCP/IP communication.
- If you see the following error message in the event log:

    The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel.

  ... on the computer running the CMN Exchange Free/Busy Connector service, perform the following:
    a Open CMN Free/Busy Connector Management Shell.
    b Type *get-CmnExchangeFreeBusyConfig*.
    c Ensure the URL specified by the *EwsUrl* property resolves properly in Internet Explorer with no certificate errors. If a certificate error is found, add the Exchange certificate to the *Trusted Root Certification Authorities* folder.

Outlook/OWA users cannot see free/busy information for a large number of users

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 Domino user, edit the *Web.Config* file in the EWS folder on the CMN Web Server:

- Add the *maxReceivedMessageSize* property to the file and set it to a large value:

```
<netTcpBinding>
<binding name="CMNFreeBusyClientSettings"
openTimeout="00:01:00"
receiveTimeout="00:01:00"
sendTimeout="00:01:00"
closeTimeout="00:01:00"
maxReceivedMessageSize="655360">
<security mode="None"/>
</binding>
</netTcpBinding>
```

Lotus users cannot see free/busy information for a large number of users

Error message: *The maximum message size quota for incoming messages (65536) has been exceeded.*

This means you must increase the quota by using the *MaxReceivedMessageSize* property on the appropriate binding element.

If you are using Lotus Notes and querying Free/Busy information for an Exchange user, edit the *QCalCon.exe.Config* file on the Domino server:

1. Increase the *maxReceivedMessageSize* property to a larger value:

```
<netTcpBinding>
<binding name="CMNFreeBusyClientSettings">
openTimeout="00:01:00"
receiveTimeout="00:01:00"
sendTimeout="00:01:00"
closeTimeout="00:01:00"
maxReceivedMessageSize="655360">
<security mode="None"/>
</binding>
</netTcpBinding>
```

2. Restart QCalCon.

Users cannot see free/busy information due to timeout errors

Error message: *This request operation sent to net.tcp://localhost:8960/FreeBusyService did not receive a reply within the configured timeout (00:01:00).The time allotted to this operation may have been a portion of a longer timeout. This may be because the service is still processing the operation or because the service was unable to send a reply message. Please consider increasing the operation timeout (by casting the channel/proxy to IContextChannel and setting the OperationTimeout property) and ensure that the service is able to connect to the client.*

If you are using OWA or Outlook and querying free/busy information for a Domino user, edit the *Web.Config* file in the EWS folder on the CMN Web Server:

- Increase the value of the *SendTimeout* property:

```
<netTcpBinding>
<binding name="CMNFreeBusyClientSettings"
...
sendTimeout="00:01:00"
...
```

```
</binding>
</netTcpBinding>
```

If you are using Lotus Notes and querying Free/Busy information for an Exchange user, edit the *QCalCon.exe.Config* file on the Domino server:

1 Increase the value of the *sendTimeout* property:

```
<netTcpBinding>
<binding name="CMNFreeBusyClientSettings">
...
sendTimeout="00:01:00"
...
</binding>
</netTcpBinding>
```

2 Restart QCalCon.

Outlook/OWA users cannot see free/busy information for Domino users

On the Exchange server:

- Verify that *Add-AvailabilityAddressSpace* has been executed on the Exchange server (for example, *Add-AvailabilityAddressSpace -ForestName <smtpdomain> -AccessMethod OrgWideFB -UseServiceAccount $true*). To verify that the cmdlet has run, type (on the Exchange Management Console): *Get-AvailabilityAddressSpace*
- Ensure you can ping <*smtpdomain*> or *autodiscover.*<*smtpdomain*> and that it resolves to the computer running the CMN 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 6.0 with an xml extension handler:

1 Open IIS Manager for IIS 6.0. Expand the Web Site where the CMN Web services are installed.

2 Right-click **Autodiscover** and click **Properties**.

3 On the *Virtual Directory* tab, click **Configuration**.

4 On the *Mappings* tab, click **Add**.

5 If you are using 32 bit IIS, click the **Browse** button and locate:

- For 32-bit IIS: *%windir%\Microsoft.Net\Framework\v2.0.50727\aspnet_isapi.dll*
- For 64-bit IIS: *%windir%\Microsoft.Net\Framework64\v2.0.50727\aspnet_isapi.dll*

6 Enter *.xml* for the extension.

7 Click **OK** on all dialog boxes.

To configure IIS 7.0 with Integrated Application pools:

1 Open IIS Manager for IIS 7.0. 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 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 CMN Free/Busy Connector.

On the computer running CMN Free/Busy web services:

- On the computer running CMN F/B Connector web services, run the *Get-CmnAutodiscoverConfig* cmdlet, and verify that the *CmnAvailabilityUrl* is set to *https://*<*host*>*/EWS/Service.asmx* （where <*host*> is either <*smtpdomain*> or *autodiscover.*<*smtpdomain*>).
- On the computer running CMN free/busy connector web services, ensure that *Get-CmnEwsConfig* is configured to communicate to the correct host and port for the computer running the CMN Domino Free/Busy connector service.

On the computer running CMN Domino F/B Connector service:

- On the computer running the CMN Domino Free/busy Connector Service, ensure the Domino service is properly configured using *Set-CmnDominoFreeBusyConfig*.
- Ensure the CMN Domino Free/busy connector service is running and there are no errors in the event log.
- Ensure Lotus Notes is properly configured to connect to your Domino server.
- If you see the following error in your event log: **NAMELookups are limited on this server to a size smaller than what would be returned. See your Domino Administrator for more information**.
    a Open the *Notes.ini* file on your Domino server and add or modify the following entry: **NAMELOOKUP_MAX_MB =<number>**.
    b Increase this value until the issue is resolved.

"Unable to generate a temporary class" error when attempting Exchange-to-Notes F/B query

An Exchange-to-Notes F/B query may 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.

Troubleshooting foreign domain issues

Check the Foreign Domain by ensuring the following:

- The Server name for the Foreign domain document is the name of the server where the QCalCon Domino server task is installed.
- The foreign domain is created in Domino, and the Calendar System property matches the *CalendarDomain* property set for the Person Documents representing the users in Exchange and the *ForeignDomainName* setting for the QCalCon server task.

Free/Busy requests do not route to registered foreign domain

In some installations, the Domino server does not properly route free/busy requests to the registered Foreign Domain. You can determine where the free/busy requests are being routed by temporarily enabling debug messages for the Domino Schedule Manager.

To enable debug messages:

1. At the Domino Server Console, enter: *Set conf debug_sched_all=1*

   — OR —

   Add *Debug_sched_all=1* to your *notes.ini* file for the Domino server.
2. Create a meeting request for an Exchange user, and try to view free/busy for that user.
3. Look for messages in the Domino Server Log such as: *<SchMsgQHandles_New> Opening queues for <FOREIGN DOMAIN>*
4. Try setting the *ForeignDomainName* in QCalCon to the value of *<FOREIGN DOMAIN>* found on the server console output.
5. Restart QCalCon.
6. Retrieve F/B information for this user again. Depending on the Domino Server installation, this value may be *LWPSCHEDGATEWAY*.
7. Once F/B is working, disable debug messages on the Domino server.

Troubleshooting Exchange Free/Busy errors

To get F/B info for an Exchange user via the FreeBusyBridge Web Service:

Get-CmnFreeBusyQCalCon *[-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 the URL of the Exchange EWS:

Get-CmnExchangeWebServicesUrl *[-EmailAddress] <String> [-Credentials <PSCredential>]*

EmailAddress: Email address of an Exchange user.

Credentials: To access the Exchange Service. Use *Get-Credential* to get the credentials.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

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