



GFI OneConnectTM

ADMINISTRATOR GUIDE

Find out how to configure GFI OneConnect in different environments, and learn how to set up advanced features.



The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

GFI and GFI OneConnect are trademarks or registered trademarks of GFI Software or its affiliates in the US and other countries. Any other trademarks contained herein are the property of their respective owners.

GFI OneConnect is copyright of GFI Software Ltd. - 1999-2017 GFI Software Ltd. All rights reserved.

Document Version: 1.3

Last updated (month/day/year): 12/29/2017

Contents

1 About GFI OneConnect	5
1.1 How it works	5
1.2 Installable Components	5
2 Getting Started with GFI OneConnect	7
2.1 Signing up to GFI OneConnect	7
2.2 System Requirements of installable components	9
2.2.1 Hardware requirements	9
2.2.2 Software requirements	9
2.2.3 Component communication prerequisites	10
2.2.4 Virtualization	11
2.3 Email routing	11
2.4 Service account permissions	12
2.4.1 Microsoft Exchange management scope role	13
2.5 Installing the service components	15
2.5.1 Secondary installation	18
2.5.2 How GFI OneConnect communicates with Microsoft Exchange	21
2.6 Setting up the SyncManager	21
2.6.1 Configuring SyncManager	23
2.7 RecoveryManager	25
2.8 RedirectorAgents & Partial activation	26
2.8.1 Installing RedirectorAgents	26
2.8.2 Monitoring Redirectors status	27
2.8.3 Removing RedirectorAgents	28
2.9 Logging into GFI OneConnect	28
2.9.1 Logging in as Administrators	28
2.9.2 Logging in as a user	29
2.10 Administrator dashboard	29
3 Using GFI OneConnect	32
3.1 GFI OneConnect Continuity	32
3.1.1 Continuity States	33
3.1.2 Activating Continuity	34
3.1.3 Using WebMail	35
3.1.4 Recovering from an Activation	37
3.1.5 Monitoring Continuity	44
3.1.6 Continuity Configuration	47
3.1.7 Outlook Extension	58
3.2 GFI OneConnect Archiving	66
3.2.1 Working with retention policies	67
3.2.2 Using On-premise archiving	73
3.2.3 Archiving from Cloud services	87
3.2.4 Reviewer Groups	89
3.2.5 Restoring emails from Archive	95
3.2.6 Import Manager	105
3.2.7 Retention Policy Storage Report	116
3.3 GFI OneConnect Security	118
3.3.1 Security Dashboard	119
3.3.2 Domain Policies	120

3.3.3 User Policies	124
3.3.4 Domain Whitelist & Blacklist	127
3.3.5 Quarantine	128
3.3.6 Security Reports	130
4 System settings	137
4.1 User Administration	137
4.1.1 Promoting users to GFI OneConnect administrators	138
4.1.2 Reviewing a user's contact information	138
4.1.3 Reset User Passwords	139
4.1.4 Creating Aliases	142
4.1.5 Defining User Sets	143
4.1.6 Export users information	144
4.1.7 Exclude Users or Mailboxes	146
4.1.8 Resolve User ID Conflicts	148
4.2 Authenticating to GFI OneConnect	149
4.2.1 Windows Authentication	150
4.2.2 Custom Authentication	152
4.2.3 Lockout settings	156
4.3 Email domains	157
4.3.1 Adding a new domain	157
4.3.2 Editing a domain	158
4.3.3 Recipient Verification	160
4.3.4 Enabling Recipient Verification in Microsoft Exchange	162
4.3.5 Deleting a domain	164
4.4 Downloads page	165
4.5 Uninstalling the components	166
5 Troubleshooting and support	167
6 Glossary	168
7 Index	173

1 About GFI OneConnect

GFI OneConnect provides a hosted solution for email Continuity, email Security and email Archive.

Continuity is an alternative email service that takes the place of your primary email system during a planned or emergency outage, allowing your end users to continue using email seamlessly.

The Archive feature ensures that sent and received emails are captured and stored in the GFI OneConnect Data Center for the time established by the retention policies.

The Security service filters emails for spam, malware, viruses and other threats before they reach your network.

The software is made up of:

- » A hosted Data Center - Each client-side component of the suite interacts with software that resides in the **Data Center**. Your organization's administrators and users can access these data center features and functions using the web-based **GFI OneConnect Admin Console**.
- » Components installed on your organization's infrastructure (Client-side components). For more information, refer to [Installable Components](#) (page 5).
- » End-user plug-ins installed on users' machines to allow them to continue using email during an outage. For more information, refer to [End user plug-ins \(optional\)](#) (page 6).

1.1 How it works

To view an interactive slide show of how GFI OneConnect works, go to http://go.gfi.com/?pageid=oneconnect_help#cshid=howitworks

1.2 Installable Components

GFI OneConnect includes a number of required and optional components that are installed in your organization's infrastructure.

GFI OneConnect Server (required)

A number of components are installed on a [server](#) in your network. The purpose of these components is to run background services such as synchronization of data, mail redirection, and user authentication.

These components are installed at one go when running the GFI OneConnect server wizard. After [installing](#) and setting up these components, you can perform most day-to-day administrative functions directly from the [web-based Admin Console](#).

Component	Description
SyncManager	A service that synchronizes your local directory, calendar and contact information with the data center. You can configure synchronizations to occur on a regular schedule, or manually trigger synchronizations at unscheduled times. For more information, refer to Setting up the SyncManager (page 21).
RecoveryManager	Software that restores email back into your mail system after an activation of Continuity. For more information, refer to Recovering from an Activation (page 37).
Windows Authentication Manager	Allows end users to log in to the GFI OneConnectAdmin Console using their Windows user name and password. Windows Authentication Manager is installed in your environment only if you use Windows authentication as your login method. For more information, refer to Windows Authentication (page 150).

Exchange Redirector Agents (optional)

To switch on Continuity to a subset of users or mailboxes only (Partial activation), RedirectorAgents must be installed on all Exchange Hub Transport Servers. RedirectorAgents are transport agents that enable dynamic rerouting of messages in Exchange environments. Without RedirectorAgents, Continuity can only be switched on for all mailboxes.

Exchange RedirectorAgents are optional, and required only when using Partial Activation.

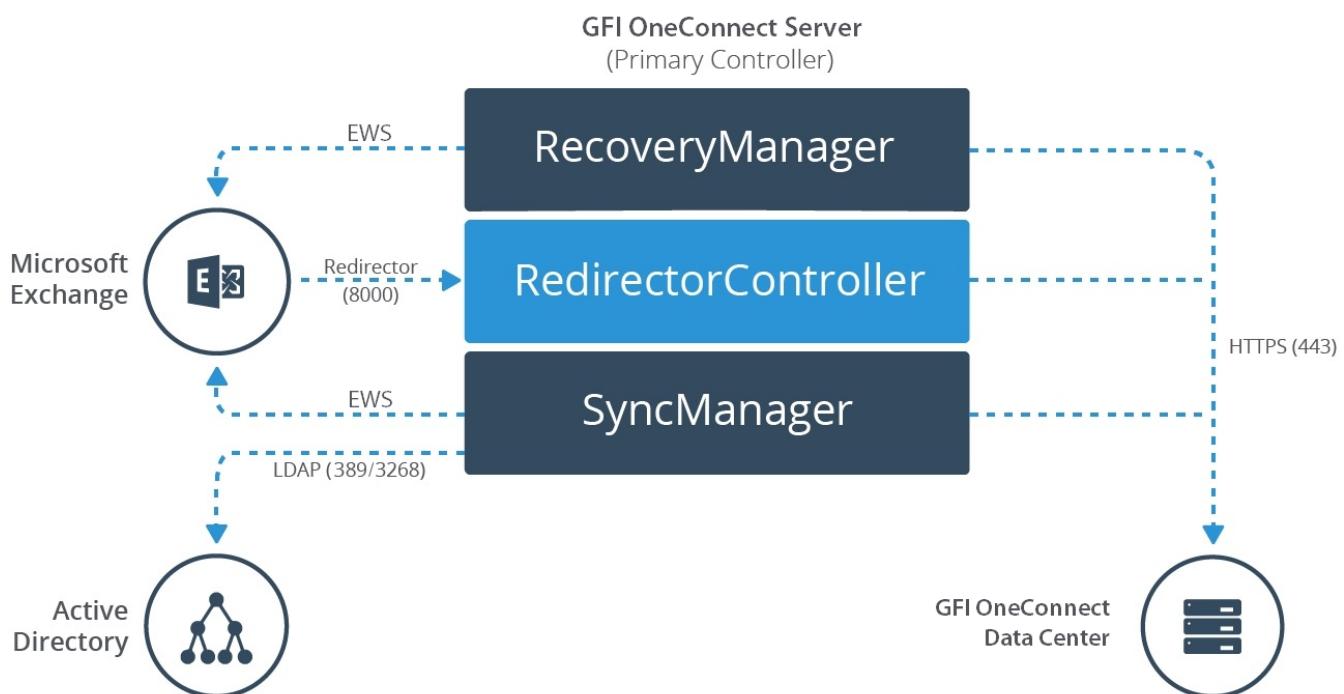
For more information, refer to [RedirectorAgents & Partial activation](#) (page 26).

End user plug-ins (optional)

Plug-in	Description
Outlook® Extension	A Microsoft Outlook plugin that provides access to email via Microsoft Outlook during an outage. Users that have the Outlook Extension installed can continue using Microsoft Outlook to send and receive emails seamlessly during an outage. For more information, refer to Outlook Extension (page 58).
Mobile plug-ins	GFI OneConnect includes Android and iOS apps for end-users to access the Continuity Web Mail when Continuity is activated. This provides a quick and easy way for your end-users to continue using email directly from their mobile devices. For more information, refer to Continuity mobile apps (page 64).

Interaction of components

The diagram below shows the interaction between the installable components and services, your infrastructure and the GFI OneConnect data center. Port numbers are shown in parentheses.



Screenshot 1: Communications Protocols and Port Numbers

2 Getting Started with GFI OneConnect

Want to try out GFI OneConnect? This topic provides a quick list of actions to help you set up a GFI OneConnect account.

1 Sign up to GFI OneConnect

Go to http://go.gfi.com/?pageid=OneConnect_Trial and sign up for GFI OneConnect. Follow the instructions to have your account created. For more information, refer to [Signing up to GFI OneConnect](#) (page 7).

2 Log in to the GFI OneConnect Admin Console

Go to <https://oneconnect.gfi.com/>. Use the credentials specified when registering to GFI OneConnect (Root Account) to log in to the Admin Console.

3 Prepare GFI OneConnect server

Choose a server within your network where to install the [client-side components](#). These components run numerous background services, such as synchronization of contact and directory information with the data center.

Ensure that the server meets or exceeds the [system requirements](#). Login to the server using an account that has a number of [special permissions](#).

4 Download and install the client-side components

Log in to the Admin Console and download the components installer. Run the package on the GFI OneConnect server. For more information, refer to [Installing the service components](#) (page 15).

5 Set GFI OneConnect users

Ensure that all user mailboxes were successfully synchronized by SyncManager and are available in GFI OneConnect. For more information, refer to [User Administration](#) (page 137).

Users are now able to login, so choose how they can authenticate to GFI OneConnect. For more information, refer to [Authenticating to GFI OneConnect](#) (page 149).

6 Configure mail routing

Set up your mail flow in such a way that inbound emails are routed to the GFI OneConnect data center. This configuration depends on your email setup. For more information, refer to [Email routing](#) (page 11).

7 Enable archiving

To start archiving emails to GFI OneConnect, configure journaling on your mail server to forward a copy of all sent and received emails to the Data Center.

[On-premise Microsoft Exchange](#)

[Microsoft Office 365](#)

8 Review & Monitor

Your system should now be up and running. Launch the web admin console to monitor the status of each service.

In Continuity you can go review the system status to ensure that your system is ready in the event of an email outage. For more information, refer to [Readiness Checks](#) (page 46).

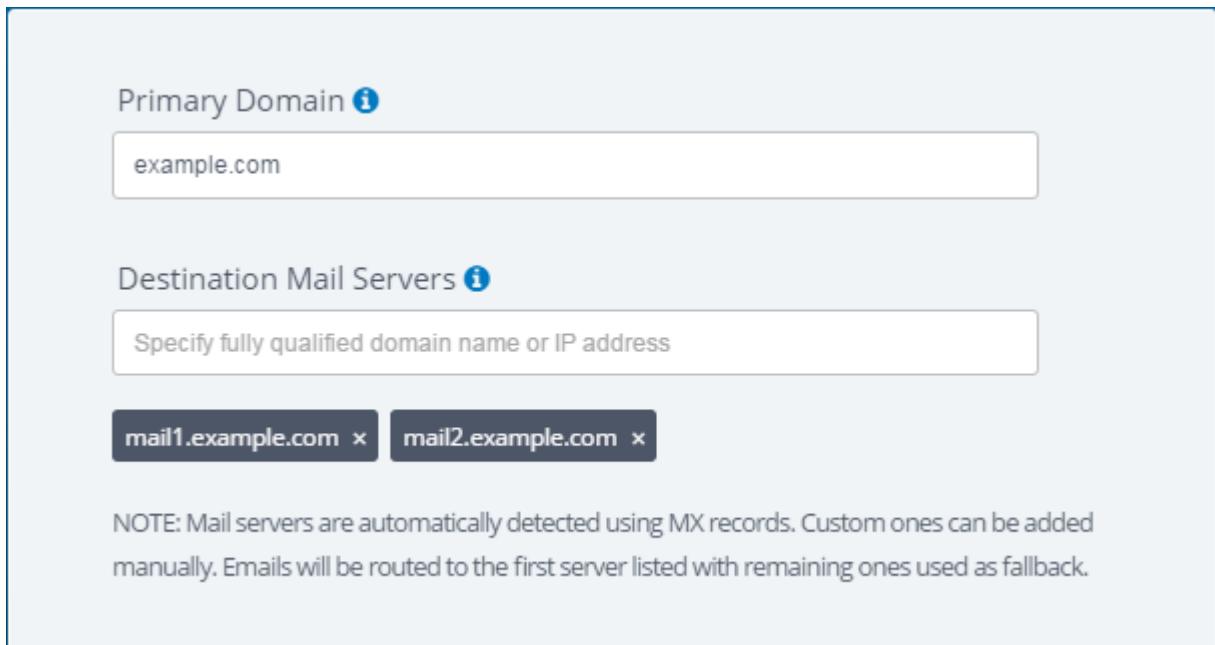
In Security you can start reviewing quarantined emails and manage the organization's filtering mechanisms. For more information, refer to [GFI OneConnect Security](#) (page 118).

In Archive you can search your personal or company emails. For more information, refer to [Creating Recovery Archive](#) (page 95).

2.1 Signing up to GFI OneConnect

Create a GFI OneConnect account to enable you to start using the software. Sign up to the service following the steps in this topic:

1. Go to http://go.gfi.com/?pageid=OneConnect_Trial and fill in your account information. Note that in this step you will be creating your Administrator Account that is used to login to GFI OneConnect the first time.
2. Click **Submit**.
3. An email is sent to your account. Click the link in the email to verify your account.
4. Login using the email address and password set up in step 1.



Screenshot 2: Specify your primary email domain & destination mail server

5. Key in your primary email domain. More email domains can be added to GFI OneConnect at a later stage accessing **Settings > Domains**. For more information, refer to [Adding a new domain](#) (page 157).
6. GFI OneConnect retrieves the current list of MX records configured for the domain. Review the list to configure destination mail servers where it will route inbound emails after processing. To add a new server address, key in the destination server's IP or FQDN and then press ',' (comma) to add the server to the list.

IMPORTANT

The order of addresses shown is important since GFI OneConnect attempts to route emails to the first entry in the list in a failover approach. If the attempt fails, it tries to route to the next server.

7. Click **Next**.
8. Select your timezone from the drop-down menu. This is important to ensure that all dates shown by GFI OneConnect are in your timezone.
9. Click **Next**.
10. Review and confirm your account details. Click **Confirm** to proceed.
11. GFI OneConnect now starts creating your account on the data center. This process can take a couple of minutes. When your account is created, you will receive another email. Click the link in the email.
12. Login using the email address and password set up in step 1 to finalize the account creation process. Complete the wizard steps to [login to the Admin Console](#).

Next steps:

Check that you have the prerequisites in place:

1. Choose a server within your network that meets or exceeds the [system requirements](#) of the [installable components](#). This server runs various background services, such as synchronization of contact and directory information with the data center.
2. Change the MX records for the domain to point to GFI OneConnect and prepare the network to allow connections. For more information, refer to [Email routing](#) (page 11).

3. Prepare an account with the necessary permissions to install and run the GFI OneConnect services. For more information, refer to [Service account permissions](#) (page 12).

2.2 System Requirements of installable components

The client-side server where to install the GFI OneConnect server components must meet or exceed the following requirements:

2.2.1 Hardware requirements

The below requirements are for GFI OneConnect components only, over and above requirements of the operating system or third-party software.

Component	Minimum Required
Processor	2GHz or more
Memory	2GB or more
Disk Space	40GB or more, depending on the number of users

2.2.2 Software requirements

Supported Operating Systems

The GFI OneConnect server must use one of the operating systems:

Operating System	Supported editions and notes
Windows Server 2016	Standard and Datacenter
Windows Server 2012 R2	Standard and Datacenter
Windows Server 2012	Standard and Datacenter
Windows Server 2008 R2	Standard & Enterprise
Windows Server 2008	Standard & Enterprise Note: only the 64-bit version of this operating system is supported

NOTES

- » GFI OneConnect components cannot be installed on the Microsoft Exchange server so it cannot be installed on Microsoft Small Business editions of the above operating systems that include Microsoft Exchange.
- » Next version of GFI OneConnect will drop the support for some Operating Systems. For further information refer to <https://www.gfi.com/support/products/gfi-oneconnect/OneConnect-Changes-in-System-Requirements>

Supported Mail Servers

GFI OneConnect components work with the following versions of Microsoft Exchange:

Mail server	Notes
Microsoft Exchange Server 2016	
Microsoft Exchange Server 2013	If using Service Pack 1, install this patch on the Microsoft Exchange server: http://go.gfi.com/?pageid=Exc2013_sp1
Microsoft Exchange Server 2010	<ul style="list-style-type: none"> » Configure Offline Address Book for Outlook 2003. » If the Exchange server was not installed with support for pre-Microsoft Outlook 2007 clients, you must create a Public Folder store. Refer to: http://go.gfi.com/?pageid=Exc2010_PF
Microsoft Exchange Server 2007	<ul style="list-style-type: none"> » Configure Offline Address Book for Outlook 2003. » If the Exchange server was not installed with support for pre-Microsoft Outlook 2007 clients, you must create a Public Folder store. Refer to: http://go.gfi.com/?pageid=Exc2007_PF

IMPORTANT

The GFI OneConnect components cannot be installed on the Microsoft Exchange server but on a server within the network that can communicate with Microsoft Exchange.

Other required software

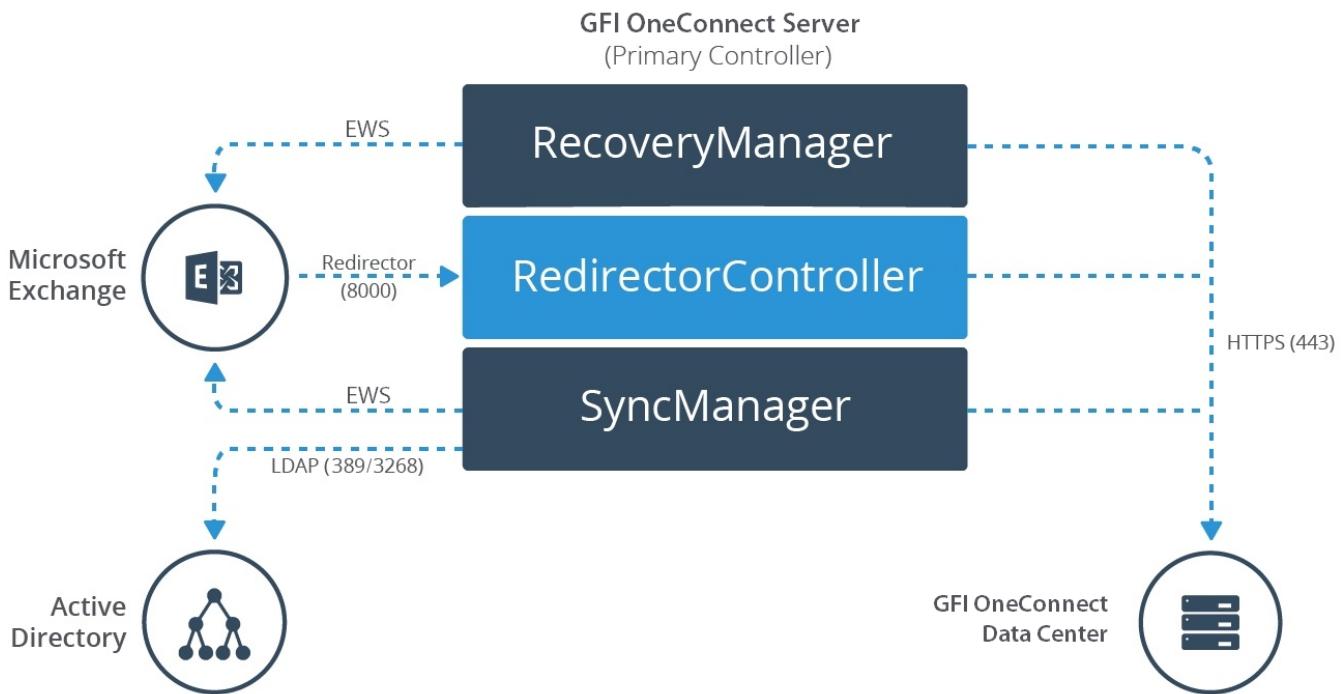
Software	Notes
.NET Framework v. 4.5	If not already present on the GFI OneConnect server, this is automatically installed by GFI OneConnect but requires a reboot before you can proceed with the wizard.
Microsoft Data Access Components (MDAC) 2.7 or later	If not already present on the GFI OneConnect server, this is automatically installed by GFI OneConnect but requires a reboot before you can proceed with the wizard.

2.2.3 Component communication prerequisites

Ensure that the firewall (if any), allows the following traffic:

- » **Port 8000** between all instances of RedirectorAgent installed on Microsoft Exchange Servers and the GFI OneConnect server hosting the RedirectorController.
- » **Port 10709** for communication between the GFI OneConnectData Center and the GFI OneConnect server hosting the RedirectorController.
- » **Port 443** between the GFI OneConnect server and the GFI OneConnect Data Center. The Data Center IP addresses are **52.19.21.57** and **52.30.238.60**
- » **Port 3268 or Port 389** for communications between SyncManager and the Active Directory server for user lookups, depending on the lookup method chosen.
- » **Port 2525** between your mail server and the GFI OneConnect Data Center when using the Recipient Verification feature in Microsoft Exchange 2013 and later. For more information, refer to [Enabling Recipient Verification in Microsoft Exchange](#) (page 162).

The diagram below shows the interaction between the installable components and services, your infrastructure and the GFI OneConnect data center. Port numbers are shown in parentheses.



Screenshot 3: Communications Protocols and Port Numbers

2.2.4 Virtualization

GFI OneConnect can be installed in a virtual environment that meets the requirements as a non-virtual environment, as defined in the previous sections.

VMware and Hyper-V are the only supported platform for virtualization.

2.3 Email routing

Use this information to help you plan and set up the mail flow configuration for operation with GFI OneConnect.

Inbound Mail Routing Requirements

Configure your email domain's MX records to point to GFI OneConnect. This enables all inbound email to get filtered by the Security service, and when your mail system is down, redirect emails automatically to the Continuity service.

To do this, replace your current MX records with the following records:

MX Record	MX Preference
<code>mx1.oneconnect.gfi.com</code>	5
<code>mx2.oneconnect.gfi.com</code>	10

This ensures that all inbound emails get routed and processed by GFI OneConnect before reaching your infrastructure.

NOTE

Secondary or other MX records are not usually required. Be aware that spammers sometimes target secondary or lower priority MX records which may not be protected by spam/virus filtering.

NOTE

GFI Software Ltd does not configure or maintain your MX records. Ensure that your MX records are correctly configured as described above. If your MX records are incorrectly configured, mail could be delayed, spam or malicious emails may get routed to your email infrastructure, or email may be lost during a Continuity activation.

After emails are processed by GFI OneConnect, emails are routed to the respective domain destination mail servers. Destination mail servers can be set directly in the GFI OneConnect web interface from **Settings > Domain**. For more information, refer to [Email domains](#) (page 157).

Ensure that your mail server accepts inbound messages from the GFI OneConnect Data Center. If your gateway server blocks inbound messages that use your domains in the **From:** field, add an exception to this rule to accept messages originating from GFI OneConnect. For example, if your domain is `mydomain.com` and you block all inbound mail with an SMTP address of `*@mydomain.com` as spam, modify this policy to exclude the GFI OneConnect Data Center. GFI OneConnect sends emails from:

- » `mx1.oneconnect.gfi.com` (IP: 52.208.1.91 - Security service)
- » `mx2.oneconnect.gfi.com` (IP: 52.58.249.172 - Security service)
- » `oneconnect-mtas2-1.gfi.com` (IP: 52.18.79.254 - Continuity service)
- » `oneconnect-mtas2-2.gfi.com` (IP: 52.31.67.15 - Continuity service)

Firewall configuration

Configure your firewall to accept inbound SMTP traffic (port 25) from GFI OneConnect. Also, configure GFI OneConnect IP addresses to be a trusted forwarder, but not safe-listed.

GFI OneConnect sends emails from:

- » `mx1.oneconnect.gfi.com` (IP: 52.208.1.91 - Security service)
- » `mx2.oneconnect.gfi.com` (IP: 52.58.249.172 - Security service)
- » `oneconnect-mtas2-1.gfi.com` (IP: 52.18.79.254 - Continuity service)
- » `oneconnect-mtas2-2.gfi.com` (IP: 52.31.67.15 - Continuity service)

Mail Routing Inbound - Store & Forward

If the destination mail servers configured in GFI OneConnect are not accessible, the Security service routes inbound emails to the Continuity service.

The Continuity service queues inbound emails until your email system is back online OR until you [activate](#) Continuity.

2.4 Service account permissions

An Active Directory user account is required to run all GFI OneConnect service processes on the server running the GFI OneConnect components. This user must have a number of special permissions pre-configured on the account.

User requirements:

- » User must be a member of the domain in which the GFI OneConnect server is installed.
- » User has a Microsoft Exchange mailbox.
- » User must be a member of the local administrator group on the GFI OneConnect server, but not a domain administrator. To do this, on the GFI OneConnect server launch the Local Users and Groups applet (**Start > Run > lusrmgr.msc**) and add the user to **Groups > Administrators**.

- » In Microsoft Exchange 2010 and higher, the user account must also be a member of the Organization Management and Recipient Management security groups. For more information refer to http://go.gfi.com/?pageid=Exc2010_2016_Admin.
- » In Microsoft Exchange 2007, the User Account must be a member of the Exchange Organization Administrator security group. For more information refer to http://go.gfi.com/?pageid=Exc2007_Admin.
- » The user must be assigned a Microsoft Exchange management scope role that has access to all mailboxes (impersonation rights). For more information on how to create the management scope role, refer to [Microsoft Exchange management scope role](#).

2.4.1 Microsoft Exchange management scope role

The account specified during the installation of the GFI OneConnect components, must be assigned a Microsoft Exchange management scope role that has access to all mailboxes (impersonation rights).

This management scope role is utilized by [SyncManager](#) to access the list of Microsoft Exchange mailbox names and synchronize them with the data center. It is also used by [RecoveryManager](#) to restore emails that were sent or received during an email outage, back into their Exchange mailboxes.

Microsoft Exchange 2016

To manually assign impersonation rights to the GFI OneConnect user account, run the following cmdlet in the Microsoft Exchange 2016 Management Shell.

```
New-ManagementRoleAssignment -name:<role_name> -Role:ApplicationImpersonation -User:<impersonator>
```

Replace the following entries with these values:

- » Replace <role_name> with a friendly name to the role being assigned, for example: `impersonate_role`
- » Replace <impersonator> with the username of the user which will run the GFI OneConnect services.

For example:

```
New-ManagementRoleAssignment -name:impersonate_role -Role:ApplicationImpersonation -User:OneConnectUser
```

Microsoft Exchange 2013 & 2010

To manually assign impersonation rights to the GFI OneConnect user account, you must first create a new management scope which groups all recipients that have a mailbox, and then create a new management role that allows a particular user to have impersonation rights on that management scope.

Run the following two cmdlets in the Microsoft Exchange Management Shell.

Step 1: Creating a new management scope

Run the following cmdlet to create a new management scope which groups all recipients that have a mailbox:

```
New-ManagementScope -name <scope_name> -RecipientRestrictionFilter {RecipientType -eq "UserMailbox"}
```

Replace <scope_name> with the name of the scope given for all user mailboxes.

For example:

```
New-ManagementScope -name user_mailboxes -RecipientRestrictionFilter {RecipientType -eq "UserMailbox"}
```

NOTE

If a management scope that covers all Microsoft Exchange mailboxes already exists, then you cannot create another similar scope that covers all mailboxes. In this case, either skip the above step and use the existing scope, or else remove the current scope before creating a new one. Use the `Get-ManagementScope` command to retrieve the list of management scopes and use `Remove-ManagementScope` command to remove an existing scope.

Step 2: Create a new management role

Run the following cmdlet to create a new management role which allows the GFI OneConnect user to have impersonation rights on the previously created management scope:

```
New-ManagementRoleAssignment -name <role_name> -role:ApplicationImpersonation -  
user <impersonator> -CustomRecipientWriteScope <scope_name>
```

Replace the following entries with these values:

- » Replace `<role_name>` with a friendly name to the role being assigned, for example: `impersonate_role`
- » Replace `<impersonator>` with the email address of the GFI OneConnect user.
- » Replace `<scope_name>` with the name of the scope specified in step 1 above, for example `user_mailboxes`

For example:

```
New-ManagementRoleAssignment -name impersonate_role -  
role:ApplicationImpersonation -user oneconnectuser@example.com -  
CustomRecipientWriteScope user_mailboxes
```

Exchange 2007

To manually assign impersonation rights to the GFI OneConnect user account, run the following two cmdlets in the Microsoft Exchange 2007 Management Shell.

```
Add-ADPermission -identity "Mailbox Store" -User "<OneConnect_User>" -  
AccessRights GenericAll
```

Replace `<OneConnect_User>` with the domain and username of the user which will run the GFI OneConnect services.

For example:

```
Add-ADPermission -Identity "Mailbox Database" -User "example.com\oneconnectuser" -  
AccessRights GenericAll
```

Next, run the following cmdlet:

```
foreach ($exchangeServer in Get-ExchangeServer){if ($exchangeServer.ServerRole -  
match 'ClientAccess'){Add-ADPermission -Identity  
$exchangeServer.DistinguishedName -User '<OneConnect_User>' -ExtendedRights ms-  
Exch-EPI-Impersonation}}
```

Replace `<OneConnect_User>` with the domain and username of the user which will run the GFI OneConnect services.

For example:

```
Example: foreach ($exchangeServer in Get-ExchangeServer){if  
($exchangeServer.ServerRole -match 'ClientAccess'){Add-ADPermission -Identity  
$exchangeServer.DistinguishedName -User 'example.com\oneconnectuser' -  
ExtendedRights ms-Exch-EPI-Impersonation}}
```

2.5 Installing the service components

This topic describes how to install the GFI OneConnect components the first time, on a server within your network infrastructure.

Important notes before installation

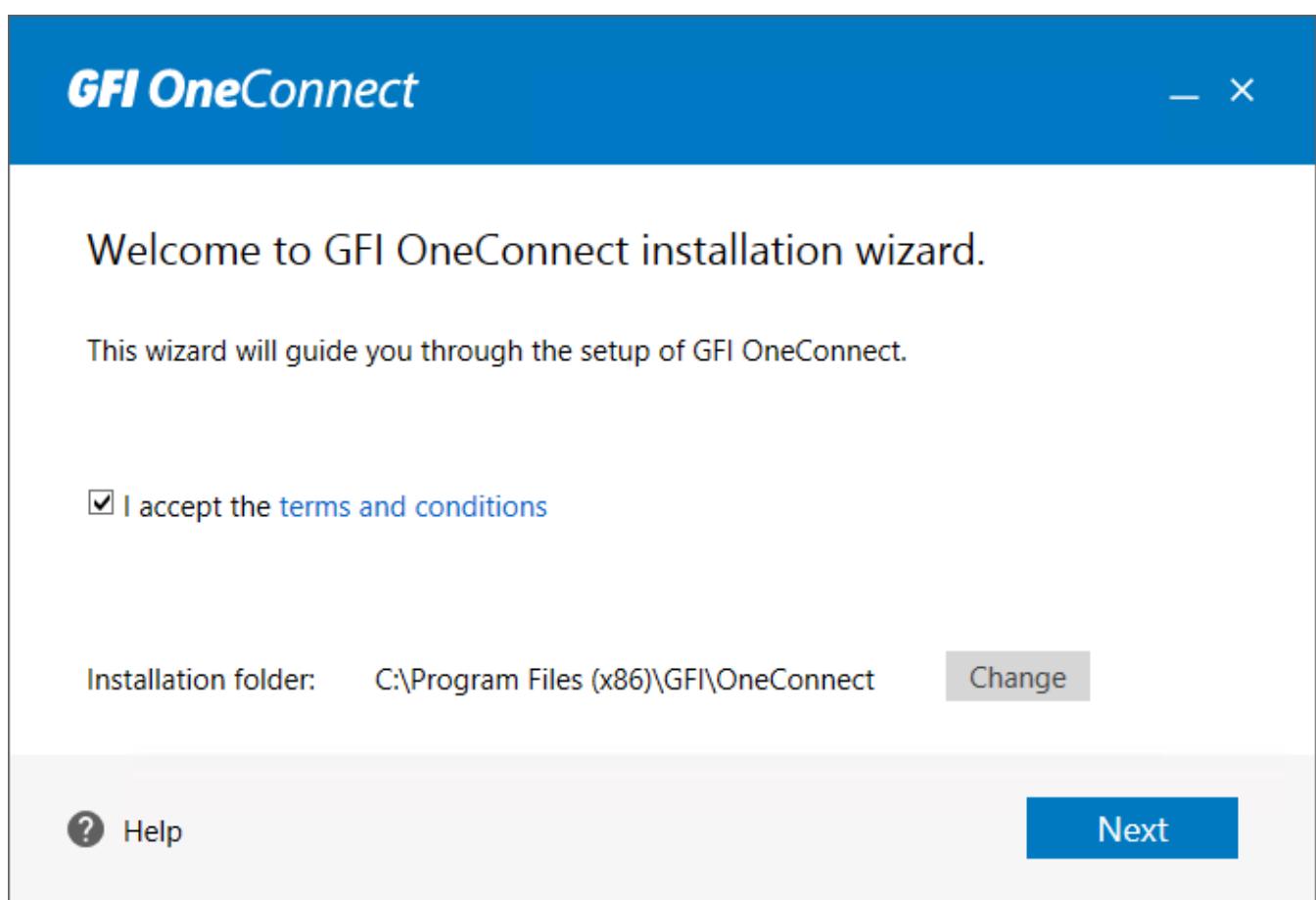
Before running the GFI OneConnect installation:

1. Change the MX records for the domain to point to GFI OneConnect and prepare the network to allow connections. For more information, refer to [Email routing](#) (page 11).
2. Prepare an account with the necessary permissions to install and run the GFI OneConnect services. For more information, refer to [Service account permissions](#) (page 12).

Installation procedure

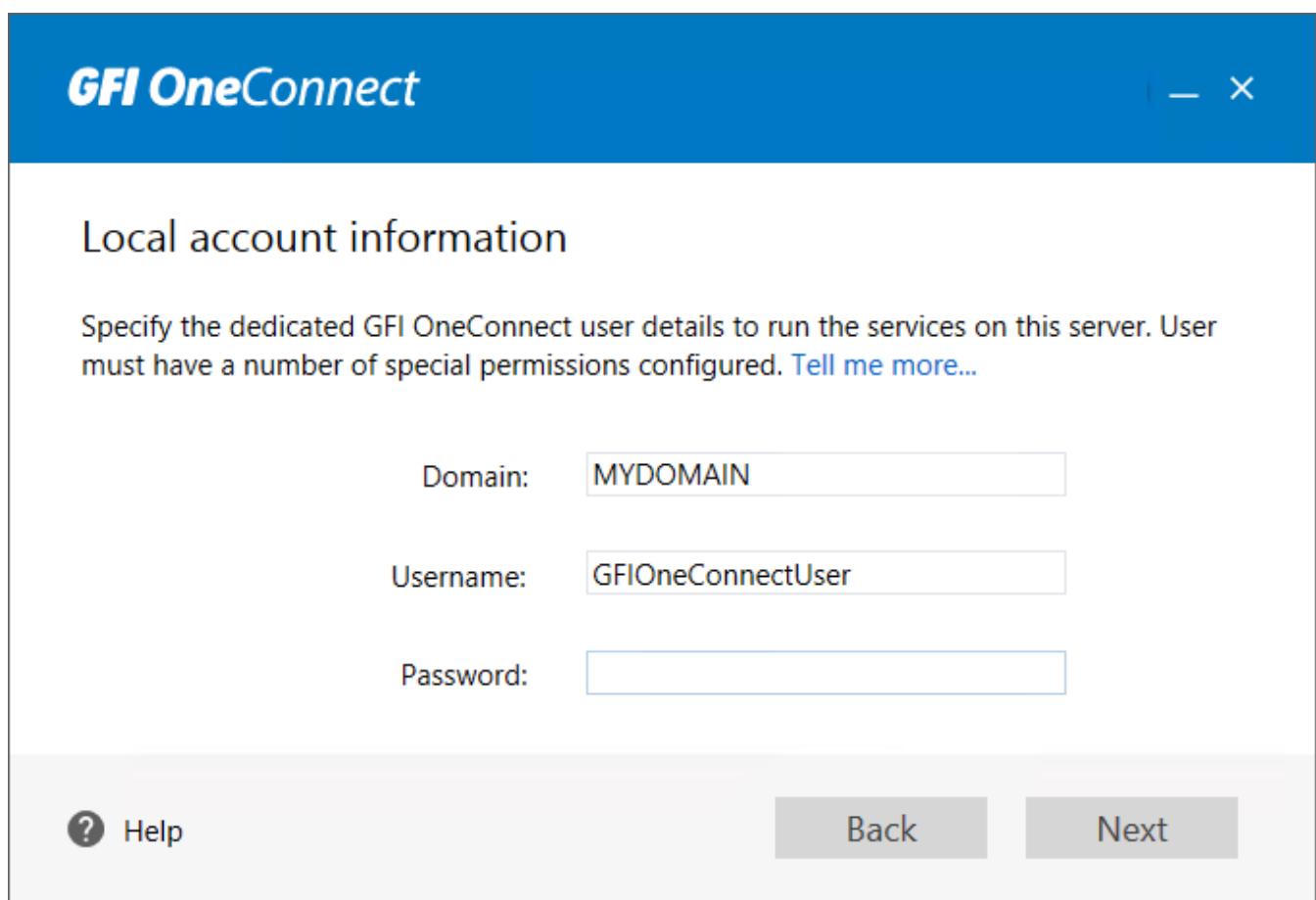
To install the GFI OneConnect components:

1. Log in to the server using the GFI OneConnect [Service Account](#).
2. Right-click the GFI OneConnect installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.
3. Double-click the installer to start the installation wizard.



Screenshot 4: The GFI OneConnect installer Welcome screen

4. In the welcome screen, read the **terms and conditions**. Select **I accept the terms and conditions** if you agree.
5. Choose the folder where to install the components from the **Installation folder** area or use the default location. Click **Next**.
6. In the authentication window, key in your Administrator account username and password. These are the same credentials used to register to GFI OneConnect. Click **Next**.
7. The wizard checks if another instance of GFI OneConnect was already installed by your account. If another installation is detected, the wizard offers the option to set this new installation as secondary or primary. For more information, refer to [Secondary installation](#) (page 18).
8. The setup now runs numerous tests to ensure that your server meets the [system requirements](#). If any of these tests fail, troubleshoot and apply the necessary corrective actions. Re-run the tests by clicking **Re-check**. When all tests are successful click **Next**.



Screenshot 5: Local account information

9. In the **Local account information** screen, key in the GFI OneConnect [Service Account](#) credentials that accesses your primary email environment. The installer should automatically populate the **Domain** and **Username** credentials since you should be logged in using this account. If these are not automatically populated, ensure that you are logged in using this account. Key in the account's **Password** and click **Next**.

Server information

The following server details have been automatically detected. Review these details and change if necessary.

Fully qualified domain name:

Friendly name:

TCP Port:

?

Help

Back

Next

Screenshot 6: Specify the local server details

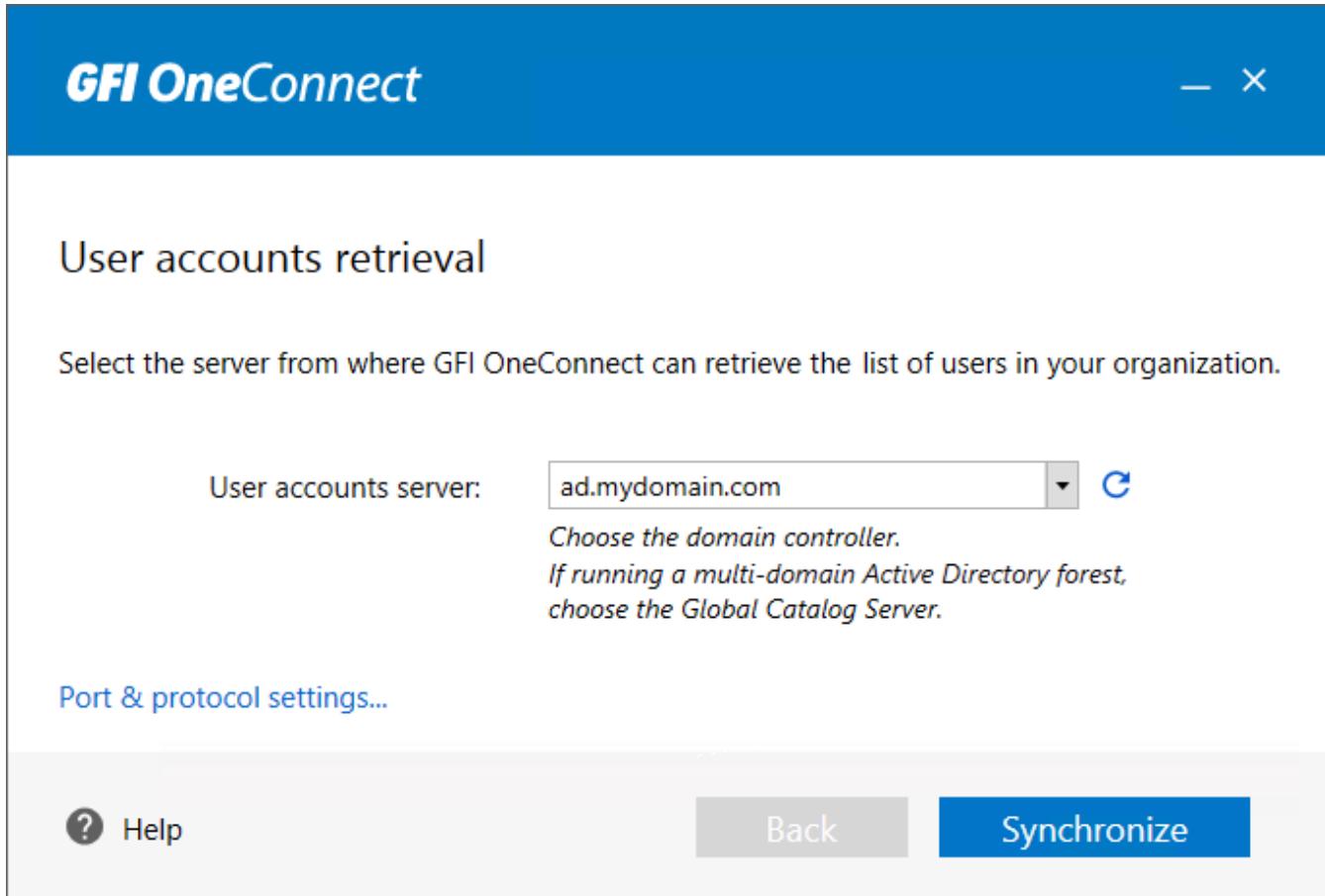
10. Key in the following server details:

Option	Description
Fully Qualified Domain Name	Key in the FQDN of the local server. Ensure that the FQDN detected by the installer is correct and that the Microsoft Exchange servers can resolve this FQDN value.
Friendly name	Specify a friendly name for this server. This value is shown in the Continuity Admin Console to identify this server.
TCP Port	Key in a port that is not used by any other application to be used by the RedirectorController. The default port number is 10709.

Click **Next**.

11. Review the installation summary details and click **Install** to start the installation.

12. On install completion, click **Open** to load the GFI OneConnect Configuration wizard.



Screenshot 7: User accounts retrieval

13. In the **User account retrieval** screen, the wizard automatically detects the Active Directory global catalogs or domain controllers available for use. Select the **User accounts server** that is physically closest to the machine. GFI OneConnect uses this server to auto-discover the list of user mailboxes. By default, GFI OneConnect uses the Global Catalog protocol (forest) to query the accounts server. If the appropriate user accounts server is not automatically detected, click **Port & protocol settings...** to configure the settings used to retrieve the accounts server.
14. Click **Synchronize** when the appropriate user accounts server is selected. The wizard first checks the [impersonation rights](#) of the user account. The wizard attempts to access the user's own mailbox using Exchange Web Services. If the check fails, ensure that the user entered in step 8 above meets the [Service account permissions](#) required by GFI OneConnect. If the check succeeds, the wizard synchronizes your user data with the GFI OneConnect data center. The sync duration depends on the size of your user base.
15. When the synchronization is complete, click **Launch Admin Console** to open the GFI OneConnect Admin Console in a web browser. For more information, refer to [Logging into GFI OneConnect](#) (page 28). Alternatively you can click **Synchronization & scheduling...** to launch SyncManager. For more information, refer to [Setting up the SyncManager](#) (page 21).

2.5.1 Secondary installation

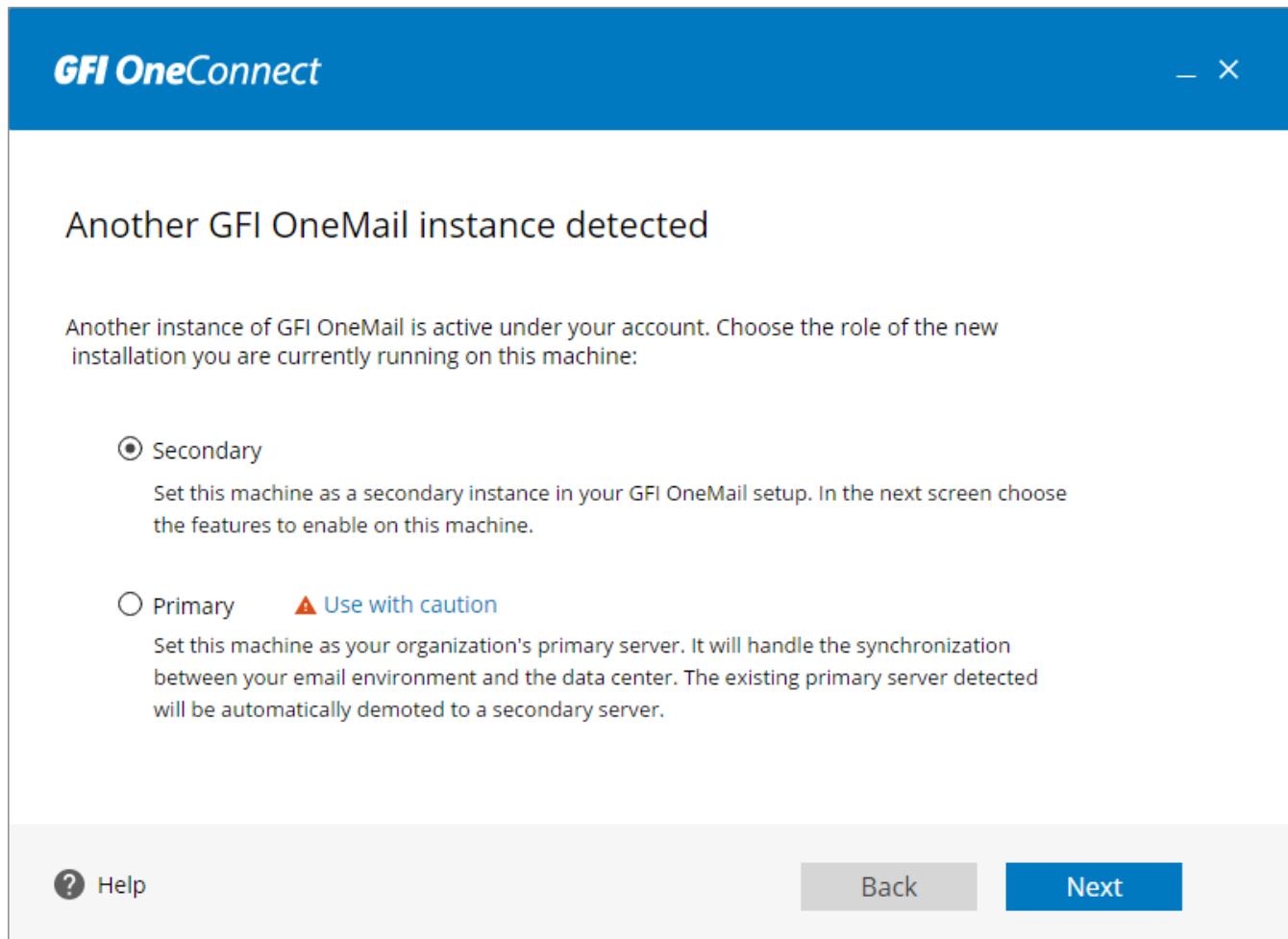
The GFI OneConnect components come in one single installer. During the first installation, all components are deployed, including the SyncManager which synchronizes directory data with the data center.

After the initial deployment of all components, you can use the same installer to perform any one of these functions:

- » Install the individual components. For example, when using Windows Authentication it is recommended to install multiple instances of Windows Authentication Manager in different geographic regions to provide redundancy and shorter login times.

- » Since GFI OneConnect requires only one server to synchronize directory data, you can stop directory synchronization by the existing instance of SyncManager, and allocate a new server as your primary directory synchronization server.

When re-running the installer, the wizard detects that GFI OneConnect was already installed and asks you to choose the role of this new installation.



Screenshot 8: Choosing the GFI OneConnect server role

Choose the role of this GFI OneConnect server:

- » [Secondary role](#)
- » [Primary role](#)

Secondary role installation

Use the **Secondary** role to install individual components.

In this role, your existing GFI OneConnect installation remains as your primary server that synchronizes directory information and that provides communication for Microsoft Exchange [RedirectorAgents](#). The secondary components installed are used to sustain your existing installation.

When the wizard detects the other instance, select the **Secondary** role and click **Next**.

Secondary GFI OneMail server

Choose the features to enable on this server:

Synchronize Contacts & Calendar

Installs a secondary instance of SyncManager on this machine for Contacts and Calendar synchronization. User Directory is only synchronized by primary instance of SyncManager.

Email Recovery

Installs RecoveryManager which is used to recover emails sent or received during an email outage, from the GFI OneMail server to Microsoft Exchange.

Windows Authentication

Allows end users to log in to the GFI OneMail WebMail using their Windows user name and password.

 Help

Back

Next

Screenshot 9: Choosing the secondary components to install

In the next screen choose the components to install:

Option	Description
Synchronize Contacts & Calendar	Installs another instance of SyncManager that synchronizes contact and calendar information. Directory information continues to be synchronized by your other instance of SyncManager. This component can be installed in environments with a large user base to relieve the synchronization load from your primary SyncManager instance. This option can be considered if synchronization of data on your primary server takes a very long time (e.g. more than 20 hours) to complete.
Email Recovery	Installs another instance of RecoveryManager, the component used to recover emails back into your mail system after a Continuity activation.
Windows Authentication	Installs another instance of Windows Authentication Manager, to enable users to log in to GFI OneConnect using their Windows credentials. Additional Authentication Managers provide redundancy and shorter login times. Ensure that any machine housing Authentication Managers are able to access a Domain Controller capable of authenticating a given user.

Primary installation

GFI OneConnect requires only one server that synchronizes directory information. If another instance of the components is detected during installation, the wizard offers the option to demote your existing installation and set your new server as the primary installation of GFI OneConnect. When a new installation is set as primary, demoting an existing server:

- » SyncManager stops synchronizing directory information on your existing installation. Directory synchronization is done by the new primary instance.
- » A RedirectorController service is installed on the new installation, serving RedirectorAgent communications and updates with the data server for partial activation. During installation of RedirectorAgents on Exchange Hub Transport servers, configure the address of the new primary server.
- » No changes are applied to the RecoveryManager and Windows Authentication Manager components installed on the existing server. These components, however, are also installed on the new server when set as primary.

Because of the extent of changes that this feature applies, it is recommended to use it with caution. Sometimes it may be safer to just uninstall the existing GFI OneConnect installation and re-install a new instance.

To set this server as a primary instance and demote the existing installation to secondary, when the wizard detects another GFI OneConnect instance, choose **Primary**. Click **Yes** in the warning screen and proceed with the installation.

2.5.2 How GFI OneConnect communicates with Microsoft Exchange

GFI OneConnect uses Microsoft Exchange Web Services (EWS) to communicate with Microsoft Exchange.

Exchange Web Services (EWS) is an API that allows applications to integrate with Microsoft Exchange data and mailboxes.

The GFI OneConnect SyncManager and RecoveryManager use EWS to communicate with the Microsoft Exchange server to retrieve user information, contacts & calendar and also to recover emails back into mailboxes after a Continuity activation.

GFI OneConnect relies on the Microsoft Exchange Autodiscover service to obtain information on the EWS service.

If GFI OneConnect fails to communicate with Microsoft Exchange, it is recommended to run the following troubleshooting checks:

- » Ensure that the user running the GFI OneConnect services has [all the required permissions](#), including [impersonation rights](#).
- » Troubleshoot Autodiscover in Microsoft Exchange. For more information refer to http://go.gfi.com/?pageid=Exc_autodiscovery and http://go.gfi.com/?pageid=Exc_autodisc_more

2.6 Setting up the SyncManager

The GFI OneConnect SyncManager synchronizes your local directory, calendar and contact information with the data center. You can configure synchronizations to occur on a regular schedule, or run synchronizations at unscheduled times.

Launch SyncManager from **Start > Programs > GFI OneConnect > SyncManager**.

NOTES

- » When loading SyncManager, it attempts to connect to the data center using the credentials specified during installation or during the last launch. If authentication fails, for example, because the account password was changed from the Admin Console, re-enter your account credentials.
- » If the post-install configuration wizard was skipped or closed, SyncManager launches the wizard. For more information about these steps refer to [SyncManager Configuration Wizard](#).

GFI OneConnect SyncManager

Directory Sync

Processed 11 accounts: 0 additions, 0 changes, 0 deletions. Encountered 0 error(s). Marked as deleted: 0 distribution lists, 0 global contacts.

Last manual run on 6/9/2016 5:22:51 AM.
Next run at 6/10/2016 3:58:27 AM.
Scheduled daily between 3 AM and 4 AM

Sync Now Sync Test Edit Schedule ... Reset Sync

Mailbox Data Sync

Contacts

Syncing contacts for Jane

Last manual run on 6/9/2016 8:18:04 AM.
Next run at 6/10/2016 4:58:27 AM.
Scheduled daily between 4 AM and 5 AM

Sync Now Edit Schedule ... Reset Sync

Calendar

Starting ...

Last manual run on 6/9/2016 8:18:07 AM.
Next run at 6/10/2016 5:58:27 AM.
Scheduled daily between 5 AM and 6 AM

Sync Now Edit Schedule ... Reset Sync

Outlook Authentication Update

Outlook Authentication Update

Overwrite Token Authentication is disabled, No account was updated. 11 accounts were not updated.

Last scheduled run on 6/9/2016 6:58:32 AM.
Next run at 6/10/2016 6:58:27 AM.
Scheduled daily between 6 AM and 7 AM

Update Now Edit Schedule ... Reset

Screenshot 10: SyncManager

From the summary screen, you can monitor the status of the synchronizations and configure their schedules:

Category	Description
Directory Sync	Monitor and configure the way that SyncManager synchronizes the user directory data. This is important to ensure that the list of users and the user data available in the Admin Console is always updated with changes applied in your AD and Exchange infrastructures. Note that directory data cannot be synchronized while Continuity is activated.
Mailbox Data Sync - Contacts	Synchronizes the Microsoft Exchange Contacts information so that the updated list of contacts is available in WebMail if Continuity is activated.
Mailbox Data Sync - Calendar	Synchronizes the Microsoft Exchange Calendar information, such as meetings and reminders, with the GFI OneConnect data center. This ensures that this information is available in WebMail if Continuity is activated. SyncManager synchronizes all calendar activities scheduled for the future, including future instances of recurring meetings, as well as activities that occurred during the past seven days.
Outlook Authentication Update	The Continuity Outlook Extension uses an authentication token stored in registry. Use SyncManager to register a token for all users on a recurring schedule, or run manually for either a single user or all users. A manual single-user run can be useful when troubleshooting errors that occur when writing the token to a mailbox. For more information, refer to Outlook Extension (page 58).

The following functions are available in the individual sync sections:

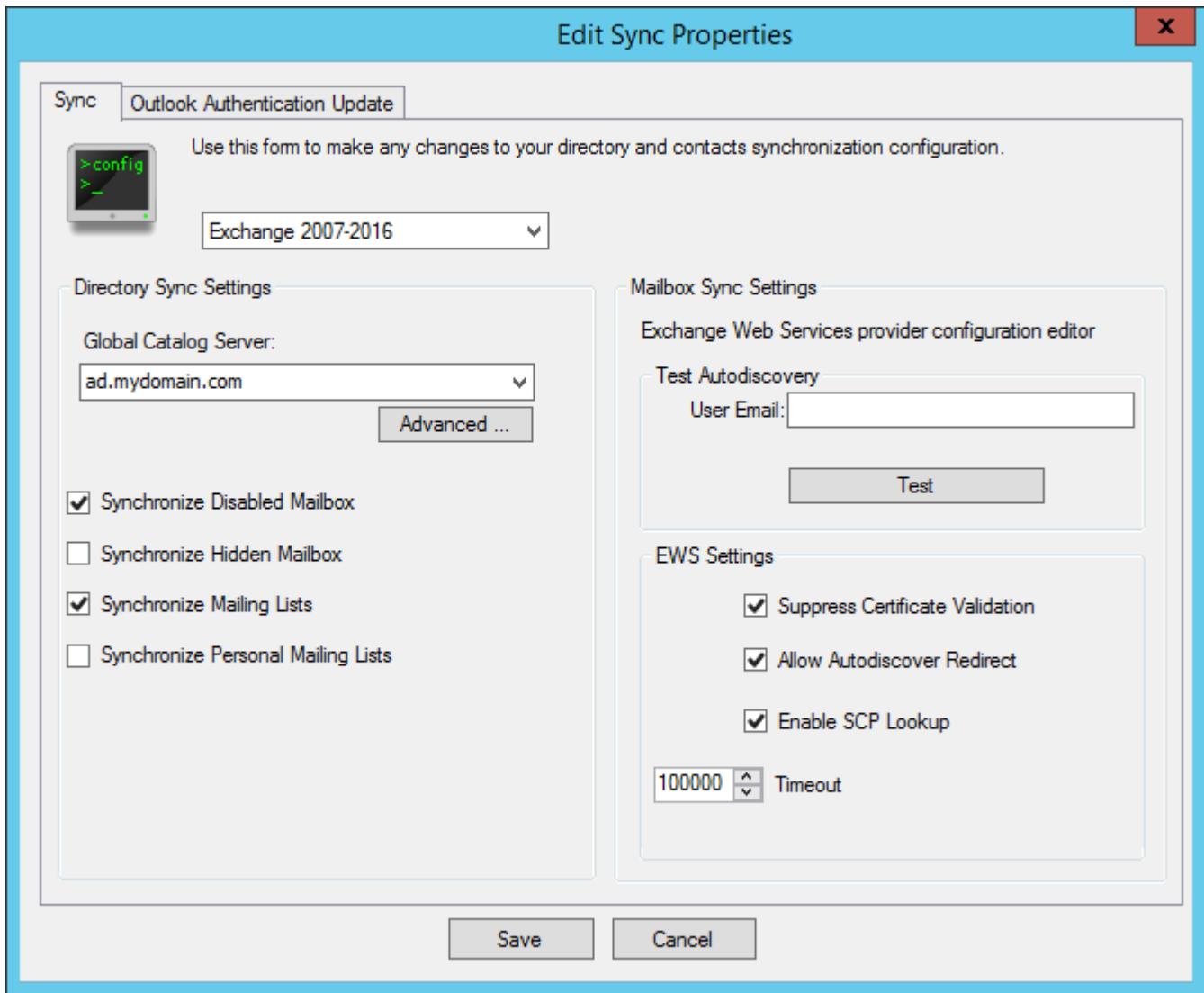
Option	Description
Sync Now	Triggers a manual synchronization process. The shown window displays the synchronization status. You can close the window to run the synchronization in the background.
Sync Test	This option is available for Directory Sync only. Use this option to simulate a directory sync and verify operation. However, the data is not stored in the GFI OneConnect data center.
Edit Schedule...	Click to change the frequency and time when the sync runs. Note that it is important that synchronization is run frequently to ensure that the data on the GFI OneConnect data center is always updated with the latest information. When an email outage occurs, the information available on the data center is up to the last synchronization. For example, mailboxes created between the last directory sync and the outage will not have access to GFI OneConnect. On installation, SyncManager automatically configures the schedules to run daily during the night. It is recommended to run synchronizations during off-peak hours and not run the schedules at the same time. In the Sync Schedule box configure the following options: <ul style="list-style-type: none">» Run Scheduled? - Select to enable synchronizations to run automatically on a schedule. It is NOT recommended to switch off this option.» Scheduling Period - Select the frequency of the schedule. Running a Daily sync is recommended.» Day - If choosing a Weekly schedule, select the day of the week when to run the sync. If using a Monthly schedule, choose the day of the month when to run the sync.» Start Hour - The time when to start the sync.
Reset Sync	Resets the synchronized data and restarts SyncManager. All synchronized data is lost and must be re-synchronized. A sync reset is not usually required, and it is recommended to reset the sync only on recommendation of GFI Support. After resetting the sync, it is recommended to manually trigger synchronization and not wait for the scheduled sync, to make sure that data is always available on the data center.

From the SyncManager main window you can also click **Configure** to set various SyncManager options, such as how it retrieves the list of users and how it communicates with the chosen server. For more information, refer to [Configuring SyncManager](#) (page 23).

2.6.1 Configuring SyncManager

This topic describes how to configure the options available in SyncManager.

Launch SyncManager from **Start > Programs > GFI OneConnect > SyncManager** and click **Configure** to launch the properties window.



Screenshot 11: SyncManager settings

From the left pane of the **Sync** settings configure the **Directory Sync Settings**:

Option	Description
Global Catalog Server	Configure the server from where SyncManager retrieves the list of users and how it communicates with the chosen server. Select the Global Catalog Server that is physically closest to the SyncManager machine and that has access to ALL users in your organization. SyncManager uses this server to auto-discover the list of user mailboxes. If the required server is not available in the drop down list or you need to configure how SyncManager communicates with the server, click Advanced . Configure the following options: <ul style="list-style-type: none"> » Query type - Choose whether to query the Global Catalog (forest) or search the domain via LDAP. » Port - Choose the query port. By default, LDAP uses port 389 and Global Catalog queries use port 3268. » Max Results - The maximum number of results to return. » Domain trees - List of domains that SyncManager searches when synchronizing servers and users. Click Requery to retry obtaining the list of domains.
Synchronize Disabled Mailboxes	Choose this option to synchronize disabled mailboxes.
Synchronize Hidden Mailboxes	Choose this option to synchronize hidden mailboxes.

Option	Description
Synchronize Mailing Lists	Choose this option to synchronize mailing lists.
Synchronize Personal Mailing Lists	Choose this option to synchronize personal mailing lists. Note that SyncManager only synchronizes Personal Mailing Lists created or edited in Microsoft Outlook. It does not synchronize Personal Mailing Lists created or edited in Outlook Web Access (OWA).

From the right pane of the **Sync** settings configure the **Mailbox Sync Settings**.

Option	Description
Test Autodiscovery	Use this feature to check whether the SyncManager service account has sufficient permissions to access a mailbox via EWS. Enter an email address in User Email and click Test . If the test fails, check the GFI OneConnect services user account's permissions. For more information, refer to Service account permissions (page 12). The user account used to run GFI OneConnect services can be identified by launching the Services applet (Start > Run and type <code>services.msc</code>). Right click on one of the services that starts with GFI OneConnect and click Properties . From the Log On tab identify the user account used to run the service.
Suppress Certificate Validation	When selected, SyncManager ignores certificate errors encountered when communicating with Microsoft Exchange. This is useful when Microsoft Exchange is not set to use a certificate that is trusted on all computers. Default setting: True
Allow Autodiscover Redirect	This options allows Autodiscover to follow redirects when a server responds with a 302 Redirect status. Default setting: True
Enable SCP lookup	Indicates if EWS should perform a service connection point (SCP) lookup when it is determining the service URL. Default setting: True
Timeout	The HTTP connection timeout value in milliseconds. SyncManager stops trying to connect to Exchange using EWS if the HTTP response takes longer than this timeframe. Default value: 100,000 milliseconds (100 seconds)

Click **Save** to apply settings.

By default, an Outlook Authentication Update does not overwrite an existing Outlook Authentication token, which means that only users without the token will be updated. You can configure SyncManager to always overwrite the token at each sync run.

To overwrite the Outlook Authentication token:

1. Select the **Outlook Authentication Update** tab.
2. Check the **Overwrite Token Authentication** box.
3. Click **Save**.

2.7 RecoveryManager

RecoveryManager is required for all GFI OneConnect installations and is installed during the Server Components install. For more information, refer to [Installing the service components](#) (page 15).

RecoveryManager restores mail sent or received during an activation of Email Continuity into your primary mail system after the activation is over. This process is called recovery. For more information, refer to [Recovering from an Activation](#) (page 37).

RecoveryManager restores historical mail from data center archives into your primary mail system. For more information, refer to [Using RecoveryManager to restore Archives](#) (page 99).

GFI OneConnect RecoveryManager does not support an Office 365 mailbox as the target mailbox. In order to restore recovered email from archive or continuity, it is necessary first to import these emails into an on-premises mailbox and subsequently export them into an Office 365 mailbox using Outlook or another 3rd-party tool.

To access Recovery Manager:

1. On your GFI OneConnect server that hosts RecoveryManager, go to **Start > Programs > GFI OneConnect > RecoveryManager**.
2. Log into the RecoveryManager using a GFI OneConnect Administrator account with sufficient [permissions on the Exchange server](#).

2.8 RedirectorAgents & Partial activation

To switch on Continuity to a subset of users or mailboxes only (Partial activation), RedirectorAgents must be installed on all Exchange Hub Transport Servers. RedirectorAgents are transport agents that enable dynamic rerouting of messages in Exchange environments. Without RedirectorAgents, Continuity can only be switched on for all mailboxes.

NOTE

Before installing RedirectorAgents, ensure that the GFI OneConnect components are [installed](#) and that the **RedirectorController Status** in the [Readiness Check](#) shows as **Connected**.

2.8.1 Installing RedirectorAgents

Notes about RedirectorAgents:

- » .NET Framework 2.0 - SP1 or newer is required on Microsoft Exchange 2007 & 2010 servers.
- » .NET Framework 4.5 or newer is required on Microsoft Exchange 2013 & 2016 servers.
- » RedirectorAgents communicate with the GFI OneConnect server where components are installed through port 8000. Ensure that there is connectivity through this port.
- » RedirectorAgents cannot be installed on Edge servers.
- » During installation, the Microsoft Exchange Transport service stops and restarts automatically. Make sure that you install the agent at a time when a brief stop in this service is not disruptive to your organization.
- » If you are running other transport agents (such as anti-spam or anti-virus agents) on your Microsoft Exchange servers, you must set the RedirectorAgent to the lowest priority; otherwise you may impede mail flow.
- » Installation of Exchange 2013 Cumulative Update 1 and 2 can change the priority of 3rd party Transport Agents. Check the priority of the RedirectorAgent using the following cmdlet: `Get-TransportAgent`. If the RedirectorAgent is not the lowest priority Transport Agent, then either change the priority using the following cmdlet: `Set-TransportAgent` or reinstall the Transport Agent.

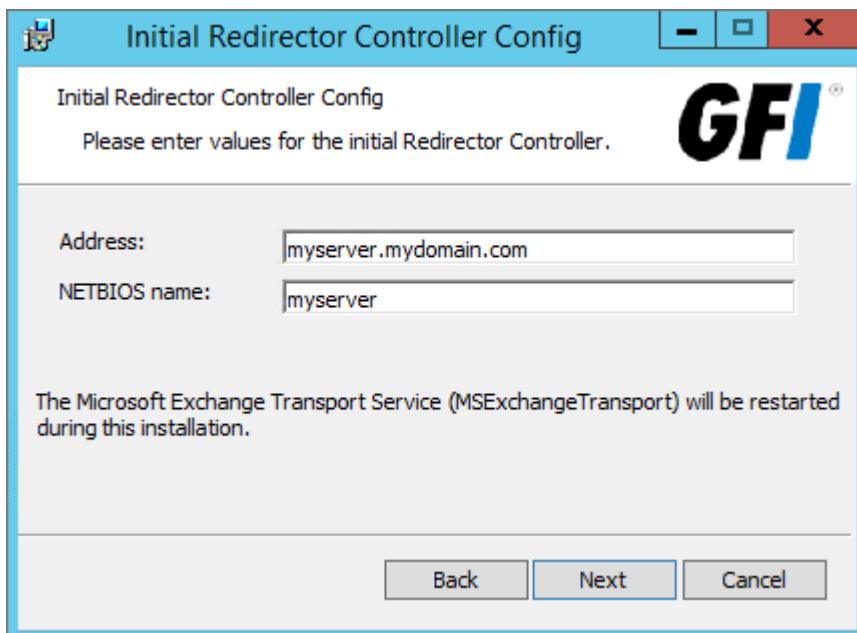
Installing RedirectorAgents:

To obtain the RedirectorAgent installer, [login](#) to the GFI OneConnect using an Administrator Account. Go to **Settings > Downloads** node and download the **GFI OneConnect Exchange Redirector** installer. Copy the installer to the Microsoft Exchange Hub Transport servers and install:

1. Right-click the GFI OneConnect Redirector Agent installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.
2. Launch the installer.

3. Click **Next** in the Welcome screen.

4. Read the license agreement. Select **I accept the terms in the License Agreement** if you agree. Click **Next**.



Screenshot 12: Entering the RedirectorController server details

5. Key in the following fields:

Option	Description
Address	Specify the fully-qualified domain name of your GFI OneConnect server.
NETBIOS name	Specify the NetBIOS name of your RedirectorController server.

6. The setup verifies the fields entered in the previous step. If verification fails, ensure that the RedirectorAgent machine can communicate with the GFI OneConnect server via port 8000 and that the server details are correct.

7. Select the location where to install the RedirectorAgent and click **Next**.

8. Click **Install** to start installation.

9. Click **Finish** on completion.

Repeat this procedure on all Exchange Hub Transport Servers.

2.8.2 Monitoring Redirectors status

1. Log in using an Administrator account and navigate to **Manage > Continuity**.

2. Go to **Readiness Check** and find entry **OneConnect Redirectors**. Click **Details...**

3. Review the status of the RedirectorControllers and RedirectorAgents.

The following statuses are available:

Status icon	Description
	GFI OneConnect Redirector Controller connected to the server.

Status icon	Description
	GFI OneConnect Redirector Controller NOT connected to the server.
	GFI OneConnect Redirector agent not installed on the Exchange server.
	GFI OneConnect Redirector agent status reporting disabled.
	Server has users in Active state.
	Server does NOT have any users in Active state.

2.8.3 Removing RedirectorAgents

1. On the Microsoft Exchange server, go to **Control Panel**.
2. Click **Programs and Features**.
3. From the list of installed software select **GFI OneConnect Exchange Redirectors** and click **Uninstall**.
4. Follow on-screen instructions.
5. Removal is complete after a system restart.

2.9 Logging into GFI OneConnect

Log in to GFI OneConnect to manage, configure and use the system.

When user information is available in the Data Center and user permissions have been configured, all other organization users can also log in to GFI OneConnect.

If the organization uses Windows Authentication, and one or more instances of Windows Authentication Manager are installed and functional, users can authenticate using their Windows credentials. If using Custom authentication, run the Welcome process to ask users to set a GFI OneConnect password. For more information, refer to [Authenticating to GFI OneConnect](#) (page 149).

NOTE

In the GFI OneConnect login page you can click **Mobile sign-in** to load a version of WebMail which is optimized for mobile devices. Signing-in with mobile is only available to access your mailbox when Continuity is activated.

2.9.1 Logging in as Administrators

There are two types of administrators in GFI OneConnect that can access the Admin Console:

- » **Root account:** The account used to register for the service. This account can log in to GFI OneConnect using the credentials used to register to the service.
- » **Administrators:** Organization users that are assigned administrative privileges can login to GFI OneConnect using the [authentication](#) method configured. For more information, refer to [Promoting users to GFI OneConnect administrators](#) (page 138).

From your favorite web browser, go to <https://oneconnect.gfi.com> and key in your username and password. When logged in, the dashboard shows an overview of the system. Use the top menu bar to navigate to any screen in the system. For more information, refer to [Administrator dashboard](#) (page 29).

2.9.2 Logging in as a user

From your favorite web browser, go to <https://oneconnect.gfi.com> and key in your username and password.

For more information refer to the GFI OneConnect user help from http://go.gfi.com/?pageid=oneconnect_user_help

Welcome to GFI OneConnect for MyCompany Inc.

 Your profile is 0% complete. Please take a few minutes to complete your notification and contact settings so that notifications can be sent to you when important events occur.

[Configure notification & contact settings](#)

Continuity

In the event of an outage of your primary mail system, continuity will be activated to provide you with uninterrupted access to your email and other critical information.

 Continuity is not active at this time.

Security

Email security provides protection against spam, viruses and unwanted content.



[Configure security](#)

Preferences

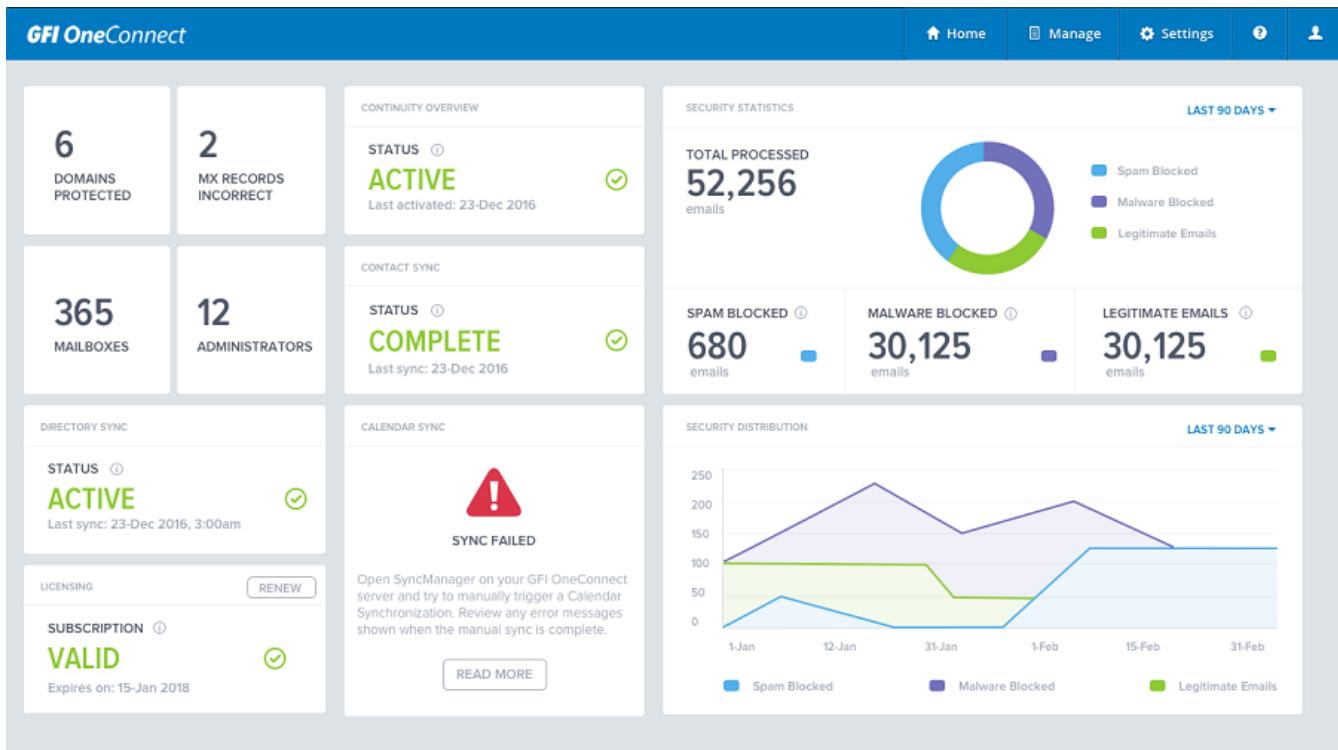
Change your personal account preferences.

[Configure notification & contact settings](#) [Change password](#)

Screenshot 13: GFI OneConnect user home page

2.10 Administrator dashboard

The GFI OneConnect Home page offers a view of all the operations and processes carried out by GFI OneConnect. The view is organized in widgets that display an overview of the GFI OneConnect configuration and general performance. Additionally, some of these widgets enable you to access the various configuration nodes directly from this dashboard, offering easy access to the configuration from a single console.



Screenshot 14: GFI OneConnect Dashboard page.

Use an administrator account to access the Dashboard. From your favorite web browser, go to <https://oneconnect.gfi.com> and key in your username and password.

The following is a list of available widgets:

Widget	Description
Domain protected	Count of domains protected by GFI OneConnect. The widget gives direct access to the Domains page, where domains can be edited, added or removed. For more information, refer to Email domains (page 157).
MX records incorrect	Count of domains that have an incorrect MX records configuration. To ensure that mail flows properly, the MX records of these domains must be updated. For more information, refer to Inbound Mail Routing Requirements (page 11).
Mailboxes & Administrators	Count of how many mailboxes and administrators are present in GFI OneConnect. Both widgets give direct access to Users page, where users and their roles can be configured. For more information, refer to User Administration (page 137).
Continuity overview	Overview of the status of the Continuity service. The statuses available are: <ul style="list-style-type: none"> » Ready: Email system is online. Continuity can be activated. » Active: Email system is down. Continuity is activated. » Recovery: Email system is back online. Emails stored during Continuity are ready to be restored to Microsoft Exchange. For more information, refer to Continuity States (page 33).
Directory Sync	Displays the status of the directory synchronization function in SyncManager. If this widget shows an error, check with SyncManager why this occurs. For more information refer to http://go.gfi.com/?pageid=oneconnect_help#cshid=syncfail
Contact Sync	Displays the status of the contacts synchronization function in SyncManager. If this widget shows an error, check with SyncManager why this occurs. For more information refer to http://go.gfi.com/?pageid=oneconnect_help#cshid=syncfail

Widget	Description
Calendar Sync	Displays the status of the calendar synchronization function in SyncManager. If this widget shows an error, check with SyncManager why this occurs. For more information refer to http://go.gfi.com/?pageid=oneconnect_help#cshid=syncfail
Security Statistics	Pie chart showing the percentage of legitimate emails compared with blocked spam and malware. The widget also shows the totals of each category. The period of time can be adjusted to the last 90, 30 or 7 days, or the last 24 hours.
Security Distribution	Line chart showing distributions of email types over time comparing legitimate emails, blocked spam and malware. The period of time can be adjusted to the last 90, 30 or 7 days or 24 hours.
Licensing	Displays the subscription status and the expiration date. If your license is approaching expiration or is expired, click Renew to extend the subscription.

3 Using GFI OneConnect

This topic contains information about:

3.1 GFI OneConnect Continuity	32
3.1.1 Continuity States	33
3.1.2 Activating Continuity	34
3.1.3 Using WebMail	35
3.1.4 Recovering from an Activation	37
3.1.5 Monitoring Continuity	44
3.1.6 Continuity Configuration	47
3.1.7 Outlook Extension	58
3.2 GFI OneConnect Archiving	66
3.2.1 Working with retention policies	67
3.2.2 Using On-premise archiving	73
3.2.3 Archiving from Cloud services	87
3.2.4 Reviewer Groups	89
3.2.5 Restoring emails from Archive	95
3.2.6 Import Manager	105
3.2.7 Retention Policy Storage Report	116
3.3 GFI OneConnect Security	118
3.3.1 Security Dashboard	119
3.3.2 Domain Policies	120
3.3.3 User Policies	124
3.3.4 Domain Whitelist & Blacklist	127
3.3.5 Quarantine	128
3.3.6 Security Reports	130

3.1 GFI OneConnect Continuity

GFI OneConnect Continuity is a high availability messaging system that ensures continuous mail flow of your organization in the event of an unexpected disruption of the primary email system.

In the case of an email flow disruption, you have three options to access to your email:

- » [Webmail](#)
- » [Mobile App](#)
- » [Outlook Extension](#)

You can send and receive email messages through these interfaces until normal service is restored to your primary email system.

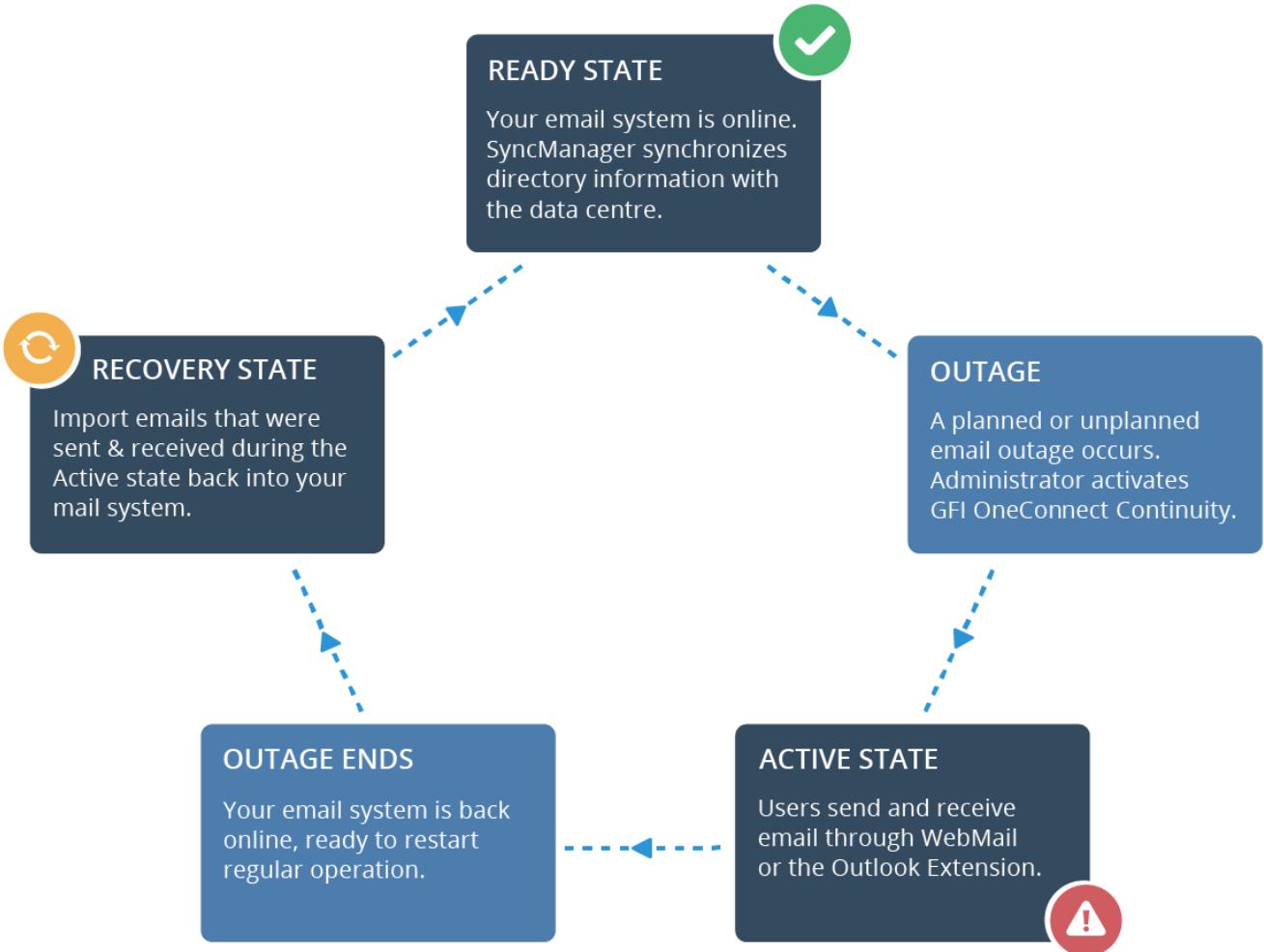
Once normal email flow is reestablished, any emails sent or received during the time of the outage can be restored to your organization's email system, ensuring that no messages are lost in the transition.

GFI OneConnect Continuity provides the following features and functions:

Feature	Description
Email service during scheduled or emergency email outages	Continuity provides an email service when your email infrastructure is down, without impacting your organization's operations.
Web access to emails	The Continuity WebMail functionality allows users to access their email through a secure browser-based interface. Users can send and receive email messages through this interface until normal service is restored to their primary email system. For more information, refer to Using WebMail (page 35).
Users continue using Microsoft Outlook during outages	You can also allow your mail users to access their mail during an activation by installing the optional Outlook Extension client software on user desktops. This allows mail users to access their mail through Outlook during the activation. For more information, refer to Outlook Extension (page 58).
Partial activation	Activate Continuity for a subset of your users only, for example, activate Continuity for mailboxes hosted on a particular mail server during maintenance but leave mailboxes on other mail servers operating normally. This optional feature requires installation of Redirector Components. For more information, refer to RedirectorAgents & Partial activation (page 26).
Audit reports	An audit trail of actions taken within the system, such as Continuity Activations. For more information, refer to Audit Reports (page 50).

3.1.1 Continuity States

Continuity is always in one of three states: **READY**, **ACTIVE**, or **RECOVERY**. Status is changed when an email outage occurs and when the outage ends. Track the Continuity status from the GFI OneConnect Admin Console.



Screenshot 15: Process of Continuity transitioning between states

3.1.2 Activating Continuity

When your primary mail system experiences a disruption of service, you can activate Continuity and allow end users to continue using email without disruption, either via the [web-based email client](#) or the [Outlook Extension](#).

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. In the **Current OneConnect State** section, click **Activate**.
4. To notify users that Continuity is being activated, select **Send notification message to all users**. Edit the **Subject** or **Text** of the message. Notifications are sent to the users' alternate contact addresses which are configurable by users in the Admin Console user profiles. Alternatively, you can select **Don't send a notification message** to not send an email notification. You may also send a [custom notification](#) at a later time. Click **Next**.

NOTE

It is recommended to use this notification to inform users about the alternate forms of using email, such as information about WebMail, how to log in to GFI OneConnect or about the Outlook Extension (if available). Setting clear expectations will help limit the number of user queries during an activation.

5. In the **Confirm** page, review the summary of the activation steps, then click **Activate** to start activation.

During an activation, the Admin Console shows the **Current OneConnect State** of the service as **ACTIVE**.

Current OneConnect State

OneConnect is currently active. All users are receiving mail in their OneConnect mailboxes. OneConnect should now represent the primary messaging location for all of your users.

When servers for active users are back online and receiving mail, click **Start Recovery** to notify these users and generate recovery archive to import their messages from OneConnect back into the primary mail system.

Start Recovery

Screenshot 16: Continuity set to active state

Use the **OneConnect Activity Log** section to track all activity.

In this state, the service functions as the mail system for your environment. This state continues until the activation is ended.

NOTE

Emails addressed to your domain where the username is not found in GFI OneConnect, are routed to the Continuity Dropbox. The Dropbox can be accessed during an activation by GFI OneConnect Administrators from the Admin Console.

Next steps:

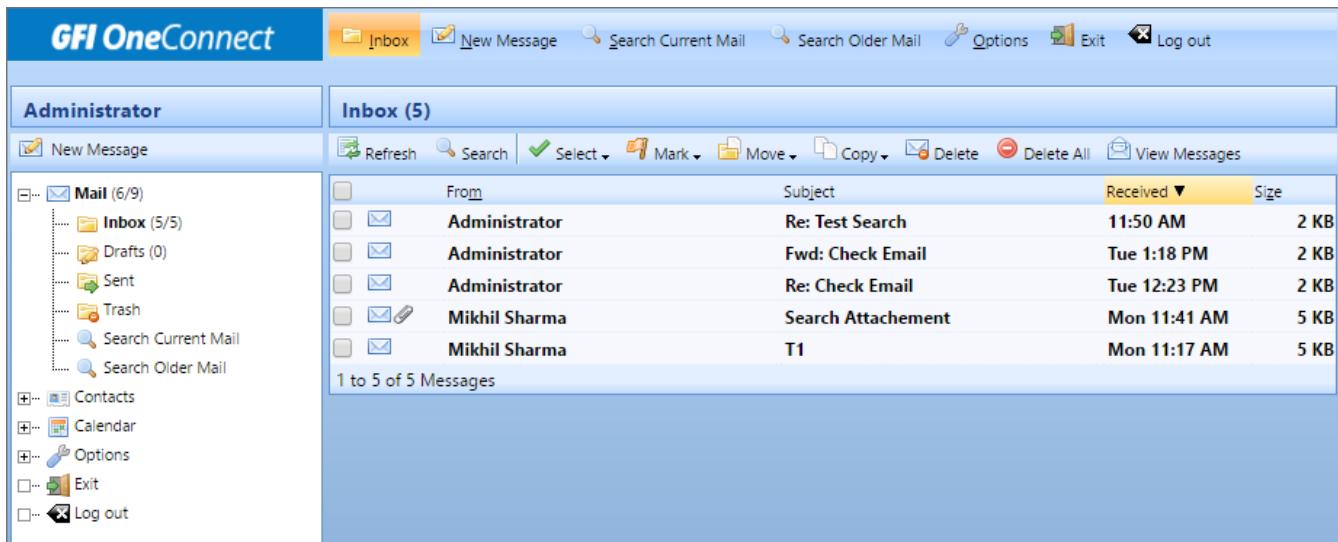
- » [Using WebMail during an activation](#)
- » [Outlook Extension](#)
- » [Using Mobile WebMail](#)
- » [Stopping activation and starting recovery](#)

3.1.3 Using WebMail

When Continuity is active, all users that have a mailbox can send and receive emails using WebMail, by [logging in](#) to GFI OneConnect.

When logged in during a Continuity activation, users can click **Access your emergency mailbox** under the **Continuity** section to launch WebMail. Administrators can access their mailbox from the top bar of the Admin Console.

Users can access their archived emails clicking the link **Search Old Mail**.



Screenshot 17: The Continuity WebMail Inbox

Use the WebMail like most other email applications. Features available:

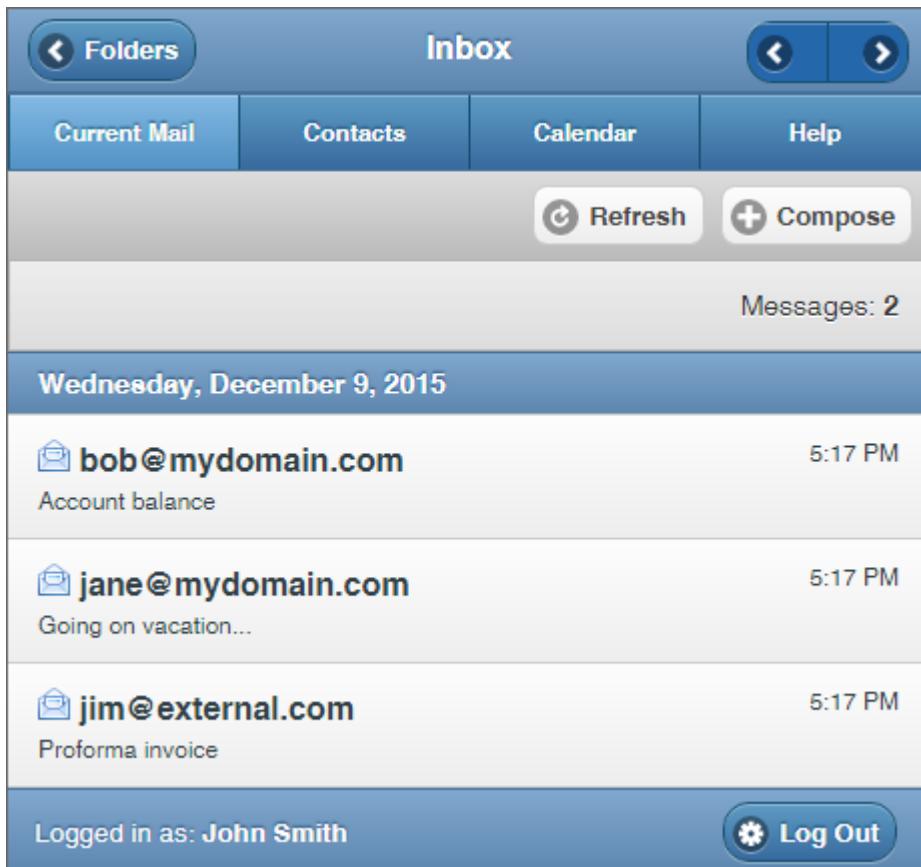
- » Forward, reply and compose emails, including the use of attachments, address book and email priority.
- » Delete, flag, move, copy and search through emails in mailbox.
- » View and search through global and personal contacts.
- » View your calendar.
- » Various customization options

Click **WebMail Help** for more information on using WebMail.

Using WebMail on a mobile device

To access WebMail using a mobile device, go to your GFI OneConnect login page and click **Mobile Sign-in**. Key in your credentials and click **Login**. GFI OneConnect presents a simplified interface of WebMail that lets users do basic email tasks.

Click **Help** for more information on using Mobile WebMail.



Screenshot 18: The mobile version of the Continuity WebMail interface

3.1.4 Recovering from an Activation

The recovery process allows you to reintegrate all emails handled by Continuity during an activation, back to your email system. The recovery process typically begins after the organization's email infrastructure is back online and tested. Items that are recovered include:

- » Messages received between the mail server outage and the Continuity activation process.
- » Messages sent or received by active users during an activation of Continuity.

Refer to information in this topic for information on how to complete Recovery.

NOTE

GFI OneConnect implements industry standard RFC-2231-encoded fields. However, certain email clients such as Microsoft Outlook do not properly decode RFC-2231-encoded fields. Therefore on recovery, some attachment filenames may be renamed. However, no information or attachments are lost.

Steps in the recovery process:

- » Step 1: Restore and test your email system
- » Step 2: Terminate Continuity activation
- » Step 3: Restore Mail to Users' Mailboxes
- » Step 4: End recovery and delete data

Step 1: Restore and test your email system

Confirm that your email system is back online, ready for user activity and able to send and receive internal and external

email.

Step 2: Terminate Continuity activation

1. Login to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. In the **Current OneConnect State** section, click **Start Recovery**.



Screenshot 19: Starting the recovery process

4. If partial Continuity activation is enabled, choose whether to recover for all activated users or a subset of users and click **Next**. If recovering for just a subset of users, choose the users to recover in the next screen.
5. Notify users entering the recovery process that the Continuity service is no longer active and that they can resume using the primary email system. This notification is sent on deactivation of a user's Continuity mailbox. Edit the **Subject** or **Text** of the message as required. Remind users that the email data they sent and received during the activation period will be restored to their primary email. You may also inform that users must manually run any custom rules that they have for filtering mail. Alternatively, you can select **Don't send a notification message** to not send an email notification and send a [custom notification](#) at a later time. Click **Next**.



Screenshot 20: Specifying a recovery archive name

6. In the **Archive Name** box, key in a friendly name for the archive file that helps you identify it when using RecoveryManager to complete recovery (for example, `ContinuityArchive_20160101`). Click **Next**.
7. In the **Confirmation** page click **Start Recovery**.

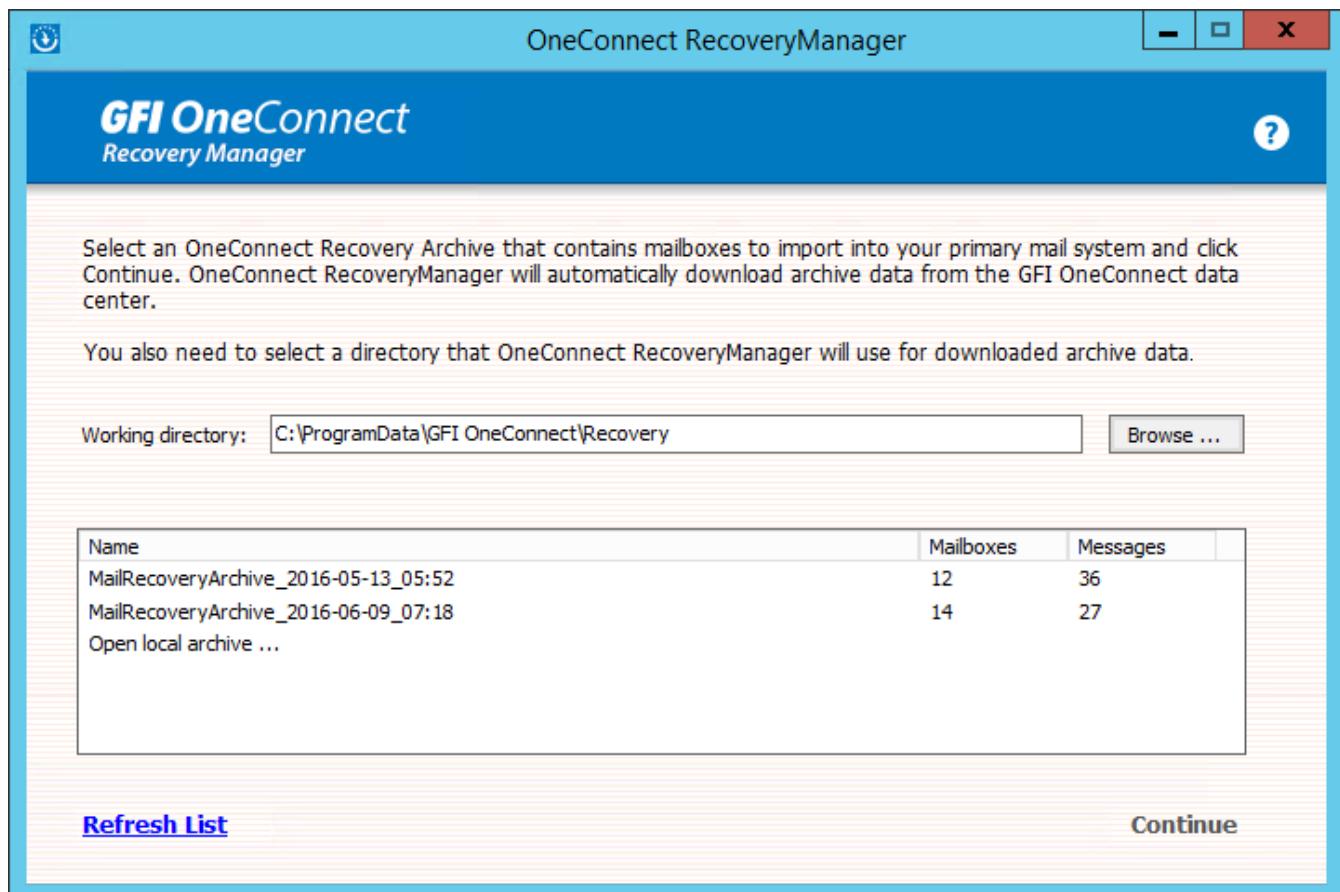
NOTE

Recovery archives are available for 30 days after they are created. After that time, they are purged and no longer available. Be sure that you complete the recovery process within 30 days.

Step 3: Restore Mail to Users' Mailboxes

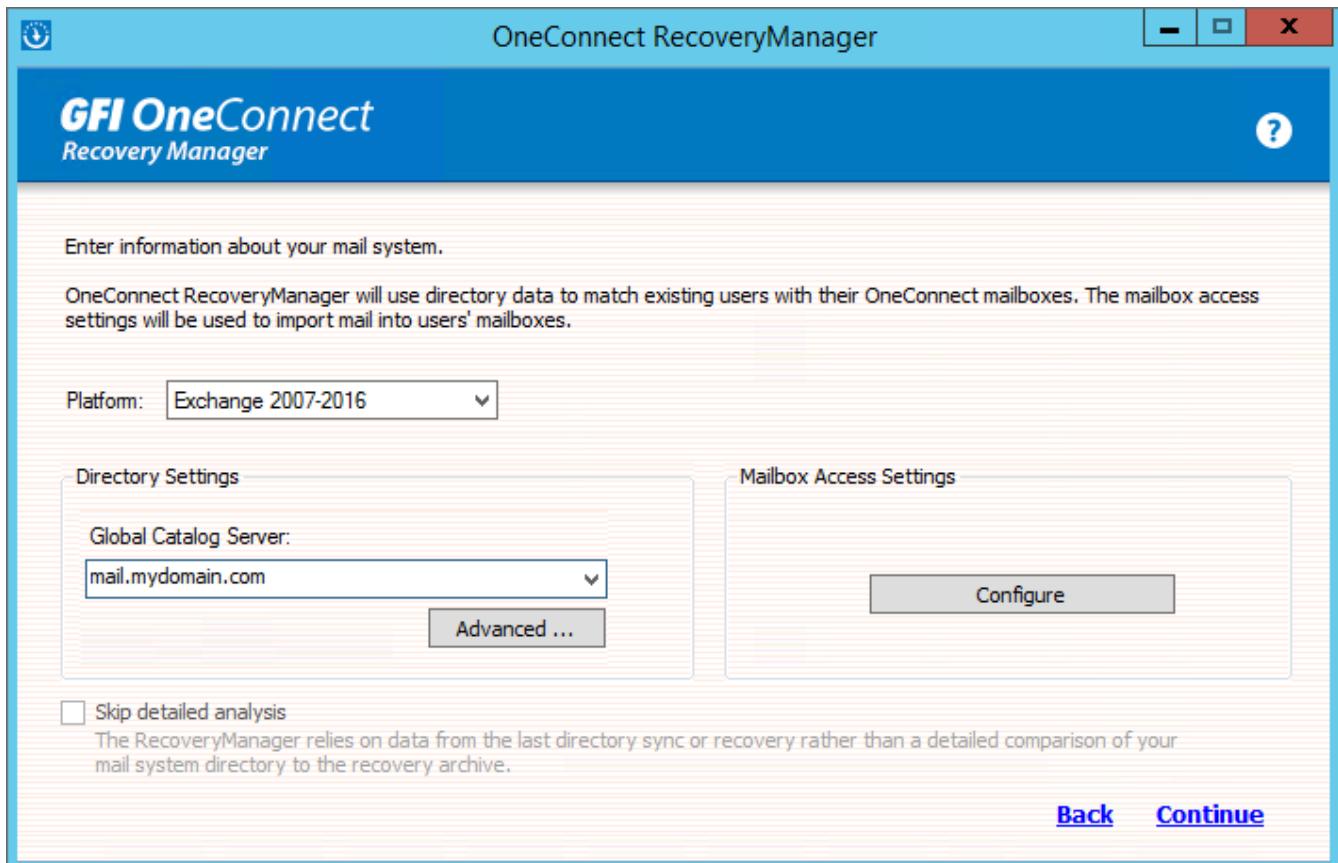
Use the RecoveryManager to restore email activity back to your email infrastructure.

1. On your GFI OneConnect server that hosts RecoveryManager, go to **Start > Programs > GFI OneConnect > RecoveryManager**.
2. Log into the RecoveryManager using a GFI OneConnect Administrator account with sufficient [permissions on the Exchange server](#).
3. Click **Start Recovery**.
4. Select the **Working directory** for RecoveryManager to use as a temporary data store during the import process. Ensure that the directory chosen has sufficient disk space for all mail items. Also ensure that there is no anti-virus or backup software that may be scanning this folder, since it may block important temporary files causing errors. Refer to the anti-virus or backup software's instructions for how to exclude directories from scans. The default path is: <system drive>\ProgramData\GFI OneConnect



Screenshot 21: Choosing the mail archive to recover

5. From the list of available recovery archives, choose the archive created in [Step 2](#) above. If you see no archives available, make sure you have created a recovery archive and check in the Continuity dashboard that the creation of the recovery archive is completed. For more information, refer to [Step 2: Terminate Continuity activation](#) (page 38). Click **Continue**.
6. The RecoveryManager downloads the archive metadata into the working directory. Actual mail data is downloaded for each user later in the process.



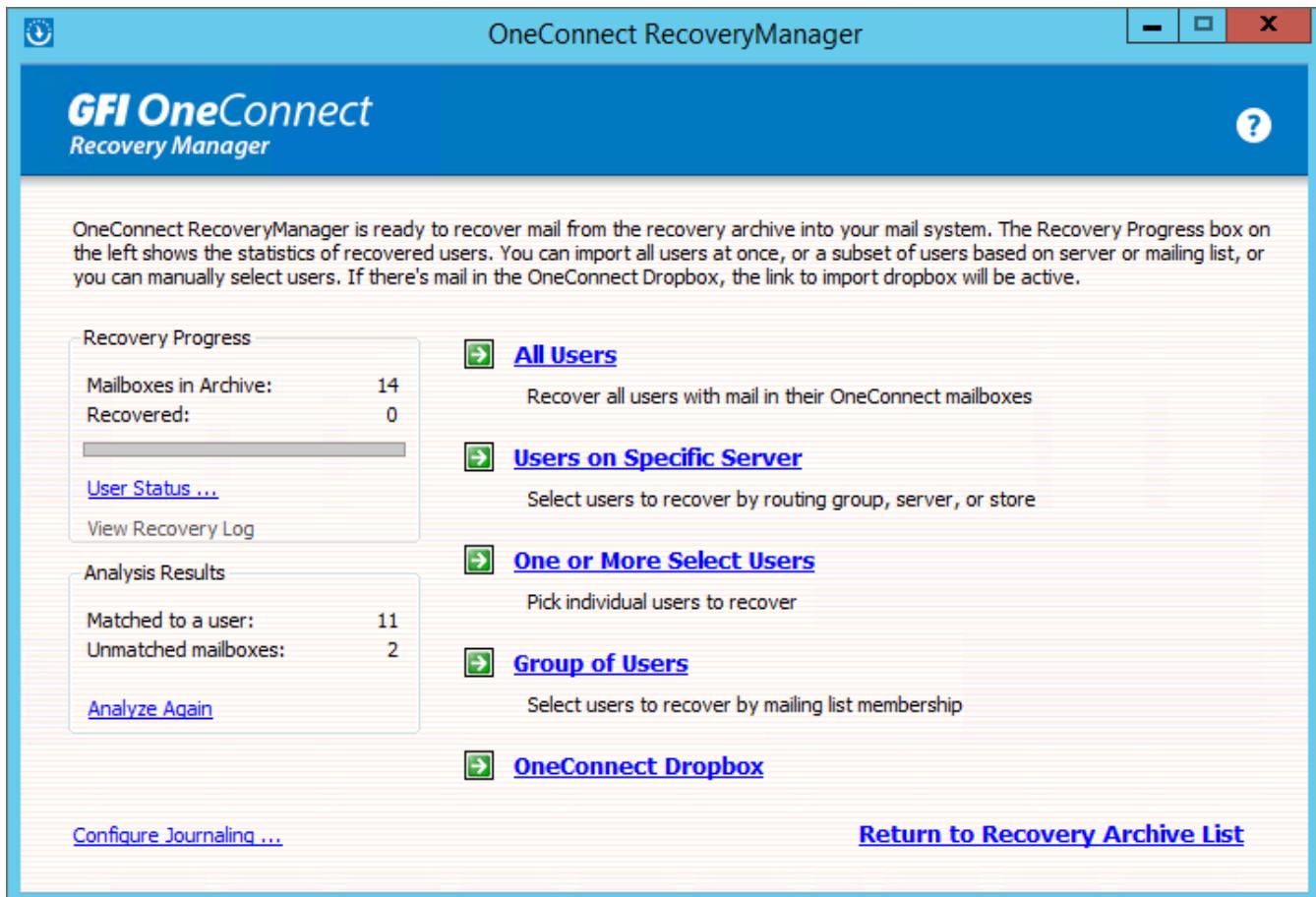
Screenshot 22: RecoveryManager global catalog settings

7. RecoveryManager uses platform information pulled from SyncManager to access the primary email system. Typically these settings are correct for recovery. If, however, there were changes applied to the mail system, such as changes to the global catalog server or EWS connection settings, click **Configure** to adjust these settings.

8. During recovery, directory information is compiled as part of the process. If SyncManager is installed, and if the most recent Directory sync was successful, RecoveryManager can use the cached results from the Directory sync for the recovery process. To use this cached data, check the **Skip detailed analysis** check box.

9. Click **Continue**.

10. RecoveryManager analyzes the archive to match up mailboxes in the archive to users' mailboxes in the primary mail system. The duration of this process depends on the number of mailboxes. Click **Continue**.



Screenshot 23: RecoveryManager mailbox and archive statistics

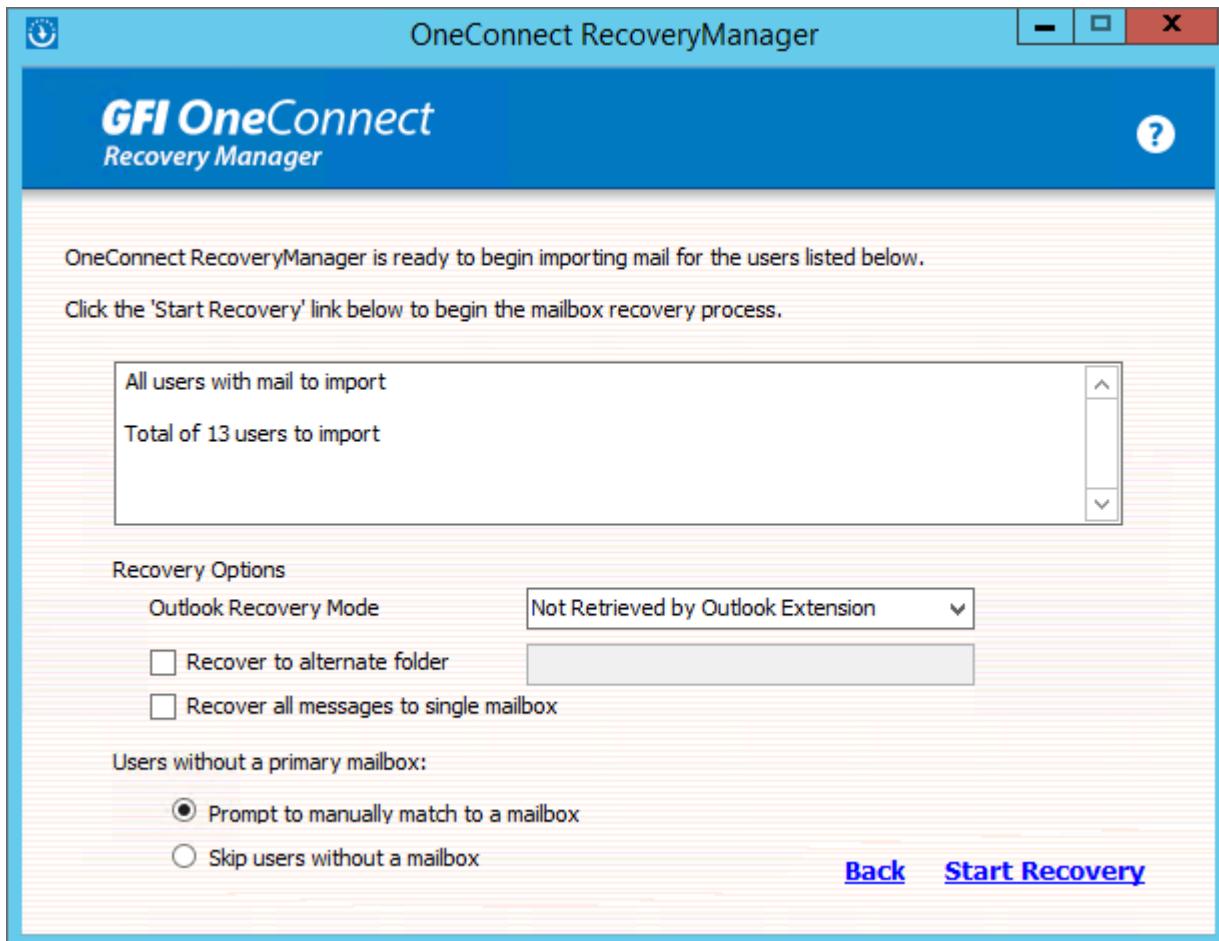
11. RecoveryManager shows mailbox and archive statistics to choose how to recover the archive:

Option	Description
Mailboxes in Archive	The total number of mailboxes in the archive.
Recovered	The number of mailboxes for which mail has been recovered.
User Status	Click to review a detailed status of each user, including usernames per server, user accounts with email data for recovery, and user accounts that cannot be matched to an account on the primary mail system.
Matched to a user	The number of user accounts that can and cannot be matched to an account on the primary mail system.
Unmatched mailboxes	The number of mailboxes that cannot be associated with a user in the primary mail system.
Analyze Again	Click to re-analyze the archive mailboxes.

Option	Description
Configure Journaling	<p>Click to specify a journaling mailbox where to store a copy of all messages transmitted during activation. This is useful for example when using a mail archiving solution such as GFI Archiver which retrieves mail from a journaling mailbox. Select the group, server or store you want to configure journaling for and click Change. Select the journaling mailbox where to copy all messages to and click OK.</p> <p>Also configure:</p> <ul style="list-style-type: none"> » BCC Journaling: Usually, the identity of a recipient in BCC is not exposed when mail is recovered to a journaling mailbox. Select this option to append the recipient's email address to the BCC field in email recovered to the journaling mailbox. If you're recovering the mail to an alternate mailbox, the alternate mailbox's address will be appended as well. Note that recipient's email address and alternate mailbox address (if applicable) are always added irrespective if original email contained recipients in BCC or not. » Save configuration for future use: Select this option to save these journaling settings for future recovery operations.

12. In the user selection area, select the users to run recovery for and click **Continue**.

User set	Description
All Users	Recover email data for all users who were activated during the outage and for which data has not yet been recovered.
Users on Specific Server	Recover email data for users on a selected message store, server, or group of servers. Check any combination of individual mail stores, servers, or server groups for recovery. (Servers without users that need recovery are grayed out.) Click Continue .
One or More Select Users	<p>Recover the mailbox of one user or the mailboxes of selected users by name. Select/Search users to recover and click Add to copy them to the user list in the right column.</p> <p>You may also override the destination of the user's restored email data. Select a user and click Properties to configure. Click Continue.</p>
Group of Users	Recover users based on distribution list membership. RecoveryManager lists all distribution lists with members who have email that needs recovery. Select groups and click Add to copy the group to the right column. Click Continue .
Dropbox	This option provides a repository for received emails sent to non-existent mailboxes or addresses not found in GFI OneConnect. If you select this option, select a server and mailbox to which all Dropbox content will be imported. Click Continue .



Screenshot 24: Recovery options

13. Choose how to restore the mail:

Option	Description
Outlook Recovery Mode	When using the Outlook Extension, emails processed during a Continuity activation are downloaded by the Outlook Extension and stored in the Microsoft Outlook OST file. When Microsoft Exchange is restored, Microsoft Outlook automatically replicates these emails with the mailbox. Choose what to do with emails processed by the Outlook Extension: <ul style="list-style-type: none"> » Not retrieved by Outlook Extension – only recovers emails that were not delivered to an Outlook Extension client. » Retrieved by Outlook Extension – only recovers emails that were delivered to an Outlook Extension client. This is useful when replication of data between Microsoft Outlook and Microsoft Exchange fails, such as when a Microsoft Outlook OST file gets corrupted. » All Messages – recovers all emails regardless of delivery method. Note that this option can create duplicates.
Recover to alternate folder	Leave this option unchecked to recover mail to the appropriate folder within a user's mailbox. To recover data to a designated folder within users' mailboxes, select this option and type a name for the folder. For example, if alternate folder name specified is <code>DisasterRecovery</code> , a new folder named <code>DisasterRecovery</code> is created in each mailbox, and all items are recovered to this folder.
Recover all messages to single mailbox	Choose this option to recover all messages from the activation to a single mailbox. Select the mailbox. For example, recover all items to an administrator mailbox for troubleshooting purposes. A folder for each user being recovered is created in the administrator mailbox.
Users without a primary mailbox	Choose how to process any unmatched mailboxes: <ul style="list-style-type: none"> » Prompt to Manually Match to a Mailbox Whenever a mailbox cannot be matched, RecoveryManager prompts to manually select the correct server and mailbox. » Skip Users: Instructs RecoveryManager to not restore data of unmatched mailboxes.

14. Click **Start Recovery** to begin importing data for selected users. RecoveryManager downloads all mail data from GFI OneConnect data center and imports it to the appropriate mailboxes and mailbox folders.

NOTE

If you click **Cancel** to stop the recovery process, RecoveryManager first completes recovery of the mailbox that is being processed before stopping.

15. Click the link **View Recovery Log** if you want to see a summary of the recovery process.

16. When the mail for all selected users has completed recovery, click **Continue**. If you need to recover additional mail, click **Select another archive to recover** to return to the RecoveryManager main screen. If not, select **Exit RecoveryManager**.

NOTE

Recovery does not import mail in user mailboxes more than once. Even if users or mailboxes belong to more than one group, their data is only imported once. The RecoveryManager skips already recovered user accounts, even if they are members of other distribution lists or groups.

Step 4: End recovery and delete data

Ensure that all email data is successfully imported into the primary mail system before ending recovery. GFI OneConnect retains recovery archives for up to 30 days or until recovery is ended.

IMPORTANT

When ending recovery, all archives are permanently deleted from Continuity and users can no longer access the data through GFI OneConnect. It is, therefore, imperative to verify that mail import was successful before running this step.

To finalize recovery and change the GFI OneConnect state to **READY**:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. In **Current OneConnect State**, click **End Recovery** to launch the Recovery Wizard.
4. Select the scope of the recovery and click **Next**.
 - **End recovery for all users in the Recovery state:** End the recovery for all users that are part of this activation.
 - **End recovery for some users:** End the recovery for a subset of users only. In the next screen select the users to terminate recovery for.
5. On the **Confirmation** page, click **End Recovery**. This purges the recovery archive from the data center and returns mailboxes to the **READY** state.

3.1.5 Monitoring Continuity

Track the status and readiness information of the Continuity service to ensure that your system is prepared in the event of an email outage.

To access the Continuity dashboard:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.

The **Admin Console Home** node shows the Continuity dashboard.

NOTE

The Continuity dashboard also displays important information related to the deployment and health of GFI OneConnect overall, including the status of the installable components and email routing.

The screenshot shows the GFI OneConnect Admin Console Home screen. The left sidebar contains links for Admin Console Home, Mobile App Administration, Outlook Extension, Mailboxes and Aliases, Mailing Lists, Notification, Audit Reports, System Settings, Your Account, and Change Password. The main content area includes sections for Readiness Check, User Statistics, Current OneConnect State, Current Tests, and OneConnect Activity Log. The Readiness Check section shows a red 'X' icon for 'Next Hop Status' and a green checkmark for '8 other status checks passed'. The User Statistics section lists sync details for DirectorySync, ContactSync, and CalendarSync. The Current OneConnect State section indicates it's in the ready state and provides an 'Activate' button. The Current Tests section shows no tests currently running and has a 'Start Test' button. The OneConnect Activity Log section shows no processes in progress.

Screenshot 25: The GFI OneConnect Admin Console

The Continuity Home screen displays the following sections:

Section Name	Description
System Updates	This section shows data center maintenance alerts. This section is only displayed when there are alerts.
Readiness Check	The service monitors the operational readiness of critical components and automatically sends notifications to designated administrators if their components are not working correctly. This section includes a detailed status list of critical components. For more information, refer to Readiness Checks (page 46).
User Statistics	This section provides data on the number of mailboxes, calendar entries, and contacts discovered by SyncManager and shows statistics on the number of users that have not been welcomed.
Current State	This section contains controls to activate and recover Continuity. When the service is active, this section displays the status of affected users, servers, or both users and servers.
Current Tests	This section contains controls that initiate and complete tests of Continuity. When a test is active, it displays the status of affected users, servers, or both users and servers.
Activity Log	This section displays the status of tasks that are currently running, as well as tasks completed in the last 24 hours. Examples include sending notification messages, updating mail routing configuration, or purging old messages from the WebMail system after a completed recovery process.

NOTE

Configurations and features displayed may vary depending on the features implemented by your organization and the permission levels of the logged on user.

Readiness Checks

The Continuity Admin Console Home page shows the status of system features at all times, known as Readiness Checks.

When a system component fails, an email is automatically sent to all email addresses listed in the fault notifications list. For more information, refer to [Fault Alerts](#) (page 48).

Readiness Check	
✗ OneConnect Controllers:	No OneConnect controller has contacted the OneConnect server. Please install at least one OneConnect controller.
ℹ Next Hop Status:	0 of 8 next hops passed. Details...
✓ 5 other status checks passed. ▾ Hide	
✓ Default Calendar Synchronization:	Default Calendar (myOneConnectServer) last synchronization completed at 15:18:58 GMT on 06-09-2016. Details...
✓ Default Contacts Synchronization:	Default Contacts (myOneConnectServer) last synchronization completed at 15:18:59 GMT on 06-09-2016. Details...
✓ Default Directory Synchronization:	Default Directory (myOneConnectServer) last synchronization completed at 12:23:23 GMT on 06-09-2016. Details...
✓ User Directory Status:	No known errors or conflicts.
✓ Fault Alert Users:	10 user(s) have been configured to receive fault alerts.
✓ MX Record (mydomain.com):	MX Record for this domain is set up correctly. Details...

Screenshot 26: Readiness checks in Continuity Home

GFI OneConnect provides the following Readiness checks:

Readiness Check	Description & Troubleshooting
Default Calendar Synchronization	Reports the last time a Calendar synchronization completed successfully. If a scheduled synchronization is more than 12 hours overdue, or if a synchronization reported as failed, this check fails. The SyncManagerService.log file on the server running the SyncManager in your environment may contain information that is useful for debugging failures. The file is located in C:\ProgramData\GFI OneConnect\Logs. For more information go to http://go.gfi.com/?pageid=oneconnect_help#cshid=syncfail
Default Contacts Synchronization	Reports the last time a Contacts synchronization completed successfully. If a scheduled synchronization is more than 12 hours overdue, or if a synchronization reported as failed, this check fails. The SyncManagerService.log file on the server running the SyncManager in your environment may contain information that is useful for debugging failures. The file is located in C:\ProgramData\GFI OneConnect\Logs. For more information go to http://go.gfi.com/?pageid=oneconnect_help#cshid=syncfail
Default Directory Synchronization	Reports the last time a Directory synchronization completed successfully. If a scheduled synchronization is more than 12 hours overdue, or if a synchronization reported as failed, this check fails. The SyncManagerService.log file on the server running the SyncManager in your environment may contain information that is useful for debugging failures. The file is located in C:\ProgramData\GFI OneConnect\Logs. For more information go to http://go.gfi.com/?pageid=oneconnect_help#cshid=syncfail
User Directory Status	Reports user ID conflicts detected by the SyncManager using a primary email address. To fix this issue, resolve the user conflicts. For more information, refer to Resolve User ID Conflicts (page 148).
Fault Alert Users	A readiness check to determine if there are users assigned to receive fault alert notifications. At least one user should be assigned to receive fault alerts to ensure error messages are not lost. For more information, refer to Fault Alerts (page 48).
MX Record (per domain)	This check verifies that the MX records for each domain include the GFI OneConnect DNS entry. If this check fails, ensure that the appropriate DNS entry exists on all public DNS servers for the domain(s). For more information, refer to Inbound Mail Routing Requirements (page 11).

Readiness Check	Description & Troubleshooting
OneConnect Authentication Manager (per server) (for Windows Authentication only)	Reports the last time a particular Authentication Manager connected to the data center. If this readiness check fails, verify that the Authentication Manager service is running on the GFI OneConnect server and that it can access the data center over port 443.
OneConnect Controller (per server)	Reports the last time a particular RedirectorController service connected to the data center. If this readiness check fails, verify that the GFI OneConnect services are running on the GFI OneConnect server and that the server can access the data center over port 443.
OneConnect Redirectors (per server)	<p>Reports the status of RedirectorAgents. Ensure that:</p> <ul style="list-style-type: none"> » all Exchange Hub Transport servers have a RedirectorAgent installed. » all RedirectorAgents are in communication with at least one RedirectorController. <p>For more information, refer to RedirectorAgents & Partial activation (page 26). If this readiness check fails, refer to http://go.gfi.com/?pageid=oneconnect_help#cshid=ts_redirector.</p>
	NOTE
	<p>After a partial activation, status updates of Redirectors can take up to three minutes to update. During this waiting period, Updating Mail Routing Configuration appears as a pending task in the Activity Log section.</p>
Next Hop Status	<p>When inbound emails are forwarded to your mail system directly, this check tests the next hop destinations over port 25. It ensures that the mail servers configured in Email Routing settings are capable of receiving messages from GFI OneConnect.</p> <p>This check is not available if inbound emails are routed using your organization's MX records. Click Details for more information.</p>
Office 365 Journaling Service	<p>This check is to verify whether or not a journaled message has been received in the last 12 hours from the Office 365 environment. If it hasn't, this warning is displayed.</p> <p>This error message could also mean there is a misconfiguration, like an improper journaling address. Verify your Office 365 environment.</p> <p>In case that Office 365 is not used on your environment, navigate to Continuity> Cloud Services and delete the journaling address clicking delete.</p>
TLS Security	<p>This check verifies whether Office 365 has received a message that was not sent using Transport Layer Security (TLS). TLS is used for email in the same way as SSL is for webpages. If this Readiness check is displayed, verify your Office 365 environment is set to send secure messages.</p>
On Premise Journaling Service	<p>This check is to verify whether or not a journaled message has been received in the last 12 hours from the Microsoft Exchange environment. If it hasn't, this warning is displayed.</p> <p>This error message could also mean there is a misconfiguration, like an improper journaling address. Verify your Exchange journaling rules.</p> <p>In case that On-premise journaling is not used on your environment, navigate to Continuity> Historical Mail > On-premise Journaling and delete the journaling address clicking delete.</p>

3.1.6 Continuity Configuration

Mailing Lists

SyncManager synchronizes your existing distribution lists from the primary mail system so that, in the event of a disruption, users can continue to send email to and receive email messages from their usual mailing lists. You can also use distribution lists as activation or recovery units. For example, it might be best to activate the members of a building-specific distribution list or to recover a small set of users before a full-scale recovery.

Distribution lists can contain both internal email addresses (users with Continuity accounts) and external email addresses.

Continuity requires that distribution list names contain 128 characters or fewer. Distribution lists with names longer than 128 characters will not receive messages through Continuity. Messages sent to these distribution lists will not archive correctly and can prevent messages from being received by other users during an activation.

To view mailing lists and members of each list:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. Navigate to **Mailing Lists**.
4. To locate a specific mailing list, in the **Search** box type the email address or name and click **Search**.
5. To view the individual members of a mailing list, in the **List Name** column click the name of the list. The listing expands to include all members. Account members display with full names; external members display with only email addresses.

Notifications

Configure how Continuity sends notifications to your organization.

Fault Alerts

The Continuity fault alerts list includes users who should receive notifications of problems identified by the system. Fault alerts are emailed to these users when:

- » Certain data center readiness checks fail. For more information, refer to [Readiness Checks](#) (page 46).
- » The percentage of users or mailing list members exceeds the configured threshold. For more information, refer to [Sync Notify Settings](#) (page 56).

To add a user to the fault alerts list:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. Go to **Notification > Fault Alerts**.
4. In the **Search** box, type the email address or name of the user to add.
5. Click **Search**.
6. In the search results, select the user to add.
7. Click **Add**.

To remove a user from the fault alerts list:

1. In the Continuity Admin Console, go to **Notification > Fault Alerts**.
2. Select the user to remove from the top section.
3. Click **Remove**.

Continuity Transition Alerts

The Continuity transition alert list identifies users who should automatically receive notifications whenever Continuity changes state, for example, when:

- » Continuity is activated.
- » Continuity is put into test mode.

- » Starting Continuity recovery.
- » Continuity is returned to READY state.

You can use this function to inform appropriate users when there is an activation of Continuity for an actual outage or a test. Use [Audit Reports](#) to see reports on state transitions.

To add users to the Continuity transition alerts list:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. Go to **Notification > Transition Alerts**.
4. In the **Search** box, type the email address or name of the user. Click **Search**.
5. In the search results, locate the listing for the user. Select the checkbox next to the name.
6. Click **Add** to add the newly added user in the top section.

To remove a user from the transition alerts list:

1. In the Continuity Admin Console, go to **Notification > Transition Alerts**.
2. Locate the listing for the appropriate user in the top section and select the **Remove** check box next to the name.
3. Click **Remove**.

[Send Custom Notifications](#)

GFI OneConnect administrators can use the service to send email messages to users. You can send custom notifications to both primary email addresses and/or alternate email addresses.

To send a custom message:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. Go to **Notification > Custom Notification**.
4. Click **Send a custom message** and fill in the following message fields:

Message field	Description
From	Key in an email address that the message will be sent from. It is highly recommended to enter an alias within your organization so that any users who reply with questions are directed to an administrator.
Subject	Type the message subject.
Text	Type the message body text.

5. Click **Next**.
6. In the **Select Recipients** screen, click the appropriate tab to identify recipients by Server, Mailing List, or individually by User.
7. Select recipients and click **Add**. Repeat until all recipients are listed in the right list.
8. Click **Next**.
9. In the **Select Recipient Options** screen select the addresses to use for the custom notification:

Recipient email address	Description
Primary addresses in your mail environment	Send notifications to the users' organization email address.
Notification addresses	Email addresses that users have provided as alternate contact information.
Both Primary and notification addresses	Send notifications to both the users' organization email address and email addresses that users have provided as alternate contact information.

10. Click **Next**.

11. To see a list of recipients, click **Show Affected Users**. Review the message text.

12. Click **Send**.

Audit Reports

Continuity provides an audit trail of actions taken within the system.

There are several categories of Continuity audit reports available:

- » **Continuity Activation reports** provide a history of full and partial Continuity activations. For more information, refer to [Continuity Audit Reports](#) (page 50).
- » **User administration reports** provide audit information on actions taken on Continuity user accounts, such as password resets, permission changes, user ID conflict resolution, and exports. For more information, refer to [User Administration Reports](#) (page 52).
- » **Notification reports** provide audit information on changes to Continuity notification lists and users welcomed via Continuity. For more information, refer to [Notification Reports](#) (page 53).
- » **System settings reports** provide audit information on network restriction settings and customizations to the Continuity home page and email disclaimer text. For more information, refer to [System Settings Reports](#) (page 53).

Continuity Audit Reports

Continuity audit reports provide a history of Continuity activations and Continuity state transitions. The reports provide the name of user who initiated each state transition along with the time and date of the transition, the login status of users during an activation, and, if a recovery archive has been generated for the activation, the name and size of the archive.

Continuity audit reports show all available historical data collected for your organization.

To view a Full, Partial or Test Activation History Report:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. Navigate to **Audit Reports**.
4. Under the **Email Continuity** section, click **Activation History Report** to view full or partial activations or **Test Activation History Report** to view test activations.
5. All logged events are shown in the report page. Further views are available:

View	Description
State Transitions	Expand State Transitions to show the date, time and user of each state change of a particular activation.

View	Description
View login records during this activation	Click View login records during this activation to see users who logged into the service during an activation.
Search	Click Search to narrow the records displayed to include only specific users by entering the username or email address. You can use % as a wildcard in search

6. To exclude users from a report, click **Exclude** in the **Action** column next to a user.

7. Click **Export to file** to download all logged events to a CSV file.

NOTE

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

Historical Mail

The Archive Searches History Report includes information on searches of the organization's historical email.

Searches which users conduct of their personal email archives are not recorded or able to be audited.

To view events related to historical mail archived:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. Navigate to **Audit Reports**.
4. Under the **System Settings** section, click the name of the report you want to view:

Report	Description
Archive Searches	To view the history of archive search audited events. Only search performed by administrators or members of reviewer groups are audited.
Archive Activity	To view a list of Recovery Archive files created during Continuity or via discovery archive.
Recovery Archives	To view a list of Recovery Archive audited events.
Retention Policies	To view a list of audited events related to the creation, edition or deletion of retention policies.
Reviewer Groups	To view a detailed list of Reviewer Group permissions audited events.

These reports show the following data:

Column	Description	Notes
Event	The action taken.	The event type may vary according to the report function.
Actor	The user responsible for the event.	
Date	The time and date the event was initiated.	Time is shown using hh:mm:ss AM/PM format, based on a 12-hour clock and your time zone. Date is shown in MM-DD-YYYY format.
Originating IP	The IP address of the system used for the event.	

On the report search page, you can narrow the report to include only events logged for specific users by entering the user name or email address in the search field and clicking **Search**. You can use % as a wildcard for any search.

To export all logged events to a CSV file, click **Export**. Choose the location where to save the export and key in a file name. Click **Save**.

NOTE

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

User Administration Reports

User administration reports provide audit information on actions taken on Continuity user accounts.

To view any of the user administration reports:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. Navigate to **Audit Reports**.
4. Under the **User Administration** section, click the name of the report you want to view:

Report	Description
Bulk Password Updates	Bulk password resets executed using the User Administration > User Information function
Bulk Flag Resets	Bulk user flag resets run using the User Administration > User Information function
User Conflicts	Resolution of user ID conflicts using the User Administration > User Conflicts function
Excluded Users	Exclusion or inclusion of users using the User Administration > Excluded Users function
User Information Exports	Exports of user information to CSV using the User Administration > Export function
User Sets	Creation or deletion of user sets using the User Administration > User Sets function

These reports show the following data:

Column	Description	Notes
Event	The action taken.	The event type may vary according to the report function.
Actor	The user responsible for the event.	
Date	The time and date the event was initiated.	Time is shown using hh:mm:ss AM/PM format, based on a 12-hour clock and your time zone. Date is shown in MM-DD-YYYY format.
Originating IP	The IP address of the system used for the event.	

On the report search page, you can narrow the report to include only events logged for specific users by entering the user name or email address in the search field and clicking **Search**. You can use % as a wildcard for any search.

To export all logged events to a CSV file, click **Export**. Choose the location where to save the export and key in a file name. Click **Save**.

NOTE

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

Notification Reports

Notification reports provide audit information on changes to Continuity notification settings and users welcomed.

To view notification audit reports:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. From the Continuity Admin Console, go to **Audit Reports**.
4. Under the **Notification** section, click the name of the report you want to view:

Report	Description
Fault and Transition Alerts	Fault or transition notifications being enabled or disabled using the Notification > Fault Alerts or Notification > Transition Alerts function.
Users Welcomed	User welcome messages that were sent using the manual Notification > Welcome New Users function. Note that if your organization uses automated, scheduled welcome messages using the Notification > Welcome New Users > Automatically welcome new users function, these automated welcome messages are not logged in this report.

These reports show the following data:

Column	Description	Notes
Event	The action taken.	The event type may vary according to the report function.
Actor	The user responsible for the event.	
Date	The time and date the event was initiated.	Time is shown using <code>hh:mm:ss AM/PM</code> format, based on a 12-hour clock and your time zone. Date is shown in <code>MM-DD-YYYY</code> format.
Originating IP	The IP address of the system used for the event.	

On the report search page, you can narrow the report to include only events logged for specific users by entering the user name or email address in the search field and clicking **Search**. You can use % as a wildcard for any search.

To export all logged events to a CSV file, click **Export**. Choose the location where to save the export and key in a file name. Click **Save**.

NOTE

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

System Settings Reports

System settings reports provide audit information on network restriction settings and customizations to the Continuity home page and email disclaimer text.

To view system settings reports:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. Navigate to **Audit Reports**.
4. Under the **System Settings** section, click the name of the report you want to view:

Report	Description
Home Page	Changes made to the end-user home page using the System Settings > End User Pages Settings function
Email Disclaimer	Changes made to the email disclaimer text using the System Settings > Email Disclaimer function

These reports show the following data:

Column	Description	Notes
Event	The action taken.	The event type may vary according to the report function.
Actor	The user responsible for the event.	
Date	The time and date the event was initiated.	Time is shown using hh:mm:ss AM/PM format, based on a 12-hour clock and your time zone. Date is shown in MM-DD-YYYY format.
Originating IP	The IP address of the system used for the event.	

On the report search page, you can narrow the report to include only events logged for specific users by entering the user name or email address in the search field and clicking **Search**. You can use % as a wildcard for any search.

To export all logged events to a CSV file, click **Export**. Choose the location where to save the export and key in a file name. Click **Save**.

NOTE

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

Managing user attributes

SyncManager imports to Continuity a number of data fields from Active Directory during synchronization. Administrators can choose which attributes to import.

To change the attributes imported from Active Directory:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. From the Continuity Admin Console, go to **System Settings > User Import**.
4. To remove an attribute, so that it is not imported from Active Directory, select the attribute's checkbox and click **Remove**.

Note that the following attributes are required and cannot be removed.

Attribute Display Value	Attribute Name
Display Name	cn

Attribute Display Value	Attribute Name
Display Name	displayName
Mailbox ID	legacyexchangedn
Email Address	mail
User ID	mailnickname
Other Mailbox	othermailbox
Other Email Addresses	proxyaddresses
Display Name	rdn
User Name	sAMAccountName
User Id	uid
<not displayed in user interface>	distinguishedname
<not displayed in user interface>	userAccountControl
<not displayed in user interface>	msExchHideFromAddressLists
<not displayed in user interface>	msExchMasterAccountSid

By default, Active Directory custom attributes are imported by SyncManager but are not available for use within the Continuity Admin Console. To add an attribute to the list that SyncManager captures:

1. In the search field, type the attribute's name.
2. Select the **By Display Name** or **By Attribute Name** radio button.
3. Click **Search**. Results appear in the section below.
4. Select the check box and click **Add**.

Global Address List (GAL) Attributes

During a Continuity activation, Global Address List attributes (synced from Active Directory) are displayed in the WebMail Contacts Global Address List. GFI OneConnect Administrators can change the attributes that are displayed.

To change the attributes displayed in Global Address List:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. From the Continuity Admin Console, go to **System Settings > Address List Display**.
4. To remove an attribute, so that it is not displayed in the Global Address List, select the attribute's check box and click **Remove**.

NOTE

You can only remove attributes from this list; you cannot add new attributes (such as custom attributes) to it.

To restore an attribute that was previously removed:

1. In the **Additional Properties** section, select the check box next to the attribute to restore.
2. Click **Add**.

Email Disclaimer

Set disclaimer text that gets automatically appended to all outbound emails sent by Continuity during an activation.

To add the disclaimer text:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. From the Continuity Admin Console, go to **System Settings > Email Disclaimer**.
4. In the **Disclaimer Text** field, type the organization's disclaimer.
5. Click **Submit** to apply.

Sync Notify Settings

During a Directory Sync, user and mailing list information is transferred by the SyncManager to the GFI OneConnect data center. Users and mailing lists are deleted from the system if their information is not provided during the sync.

This feature sends an email warning to the Faults Alerts members if the percentage of users or lists deleted during a sync exceeds the threshold amount. For more information, refer to [Fault Alerts](#) (page 48).

Configure the user/mailing list deletion percentage at which a warning message is sent:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. From the Continuity Admin Console, go to **System Settings > Sync Notify Settings**.
4. In **Deletion Threshold** field, enter the percentage of deleted users or distribution lists above which the system should send a warning message.
5. Click **Submit**.

End User Pages Settings

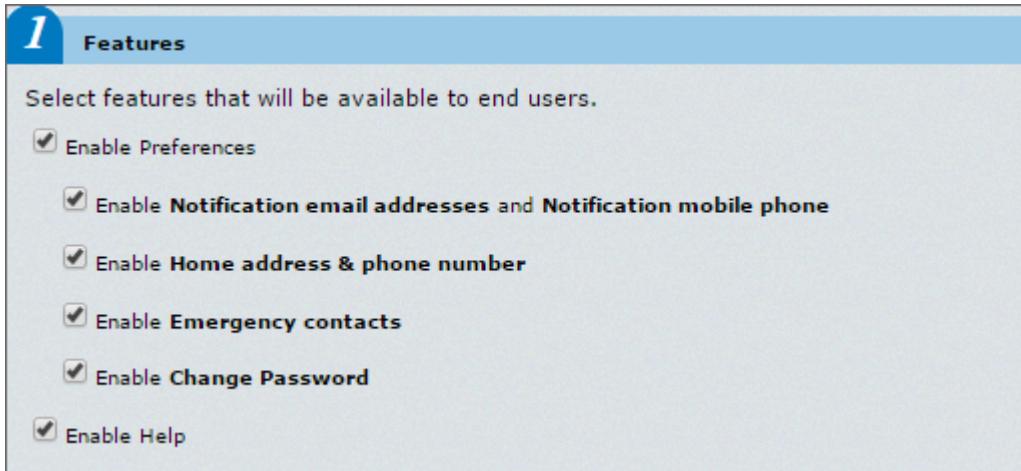
The system allows Administrators to control the information that appears to end users on the GFI OneConnect Home page.

To configure end user page settings:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. From the Continuity Admin Console, go to **System Settings > End Users Pages Settings**.

Preferences

Select which links appear in the **Preferences** section on the Home page, or hide the Preferences section entirely. Under **Features**, select the user preferences to show to end users on the Home screen.



Screenshot 27: End-user pages features list

Option	Description
Enable preferences	Show the preferences section. If this option is disabled, the following options cannot be enabled.
Notification email address & mobile phone	Users are prompted to enter one or more email addresses and a mobile phone number where to receive notifications in the event that their primary email system is down, notifying them to use GFI OneConnect.
Home address & phone number	Users are prompted to enter street address, city, state/province, zip/postal code, country and home phone number. These can be used in case of an emergency, where your organization may need to contact users at home.
Emergency contacts	Users are prompted to enter the details of up to three emergency contacts.
Change password	Allows end users to change their service password. This option is not available for organizations using Windows Authentication.
Help	Display/hide all the Help prompts from the end-user's Home page.

Click **Submit** to apply changes.

Add Additional Custom Text

Text can be added to the top of the End User Home page to give additional information to your users. In addition, if Continuity is enabled for your organization, you can add messages to be displayed to users during each of the Continuity states.

Change the text displayed to end users on the Home Page from the **Home Page Textual Content** section. Enter text in each section as desired.

Section	Description
Top of the Home Page Text	This text is displayed at the top of the page, under the headers and before the rest of the Home Page content. This text is displayed all the time, and is not related to Continuity state.
Active State Text	This text displays when Continuity is in an Active state only. To include images or links, use Bulletin Board (BB) code. For example, to add an image, include a link to the image between <code>IMG</code> tags, for example <code>[IMG]http://mydomain.com/image.png[/IMG]</code> . To add a link, include the link between <code>URL</code> tags, such as <code>[URL]http://mydomain.com[/URL]</code> .

Section	Description
Ready State Text	This text displays when Continuity is in a Ready state only. To include images or links, use Bulletin Board (BB) code. For example, to add an image, include a link to the image between <code>IMG</code> tags, for example <code>[IMG]http://mydomain.com/image.png[/IMG]</code> . To add a link, include the link between <code>URL</code> tags, such as <code>[URL]http://mydomain.com[/URL]</code> .
Recovery State Text	This text displays when Continuity is in a Recovery state only. To include images or links, use Bulletin Board (BB) code. For example, to add an image, include a link to the image between <code>IMG</code> tags, for example <code>[IMG]http://mydomain.com/image.png[/IMG]</code> . To add a link, include the link between <code>URL</code> tags, such as <code>[URL]http://mydomain.com[/URL]</code> .

Click **Submit** to apply.

3.1.7 Outlook Extension

The Outlook Extension is a plugin that provides access to email via Microsoft Outlook during an outage. Users that have the Outlook Extension installed can continue sending and receiving emails seamlessly. Through Outlook Extension user also have a link to access their archived emails.

How it works

The Outlook Extension periodically polls the data center to see if Continuity has been activated.

When Continuity is activated, the plugin switches Microsoft Outlook into offline mode, and remains offline for the duration of the activation. While Continuity is active, messages are routed and delivered to user Inboxes through GFI OneConnect.

When the activation period is over, the plugin switches Microsoft Outlook back into online mode. Messages sent and received during the activation using the Outlook Extension are resynced by Microsoft Exchange. These messages are included in the Recovery archive, but are not restored during normal recovery unless an administrator directs the RecoveryManager to do so.

Outlook Extension notes

- » End-users must log in or register with GFI OneConnect prior to using the Outlook Extension during a Continuity activation.
- » When Continuity activation is over, the Outlook Extension normally receives a state change signal from GFI OneConnect telling it to reconnect to the Microsoft Exchange server and return to regular operation. However, if Microsoft Outlook is closed during an activation and it misses the state change, it may remain offline after the activation is over. If this happens, users can reconnect to Microsoft Exchange and resume regular operation by right-clicking the **Offline** button.
- » If your organization uses proxy servers, the Outlook Extension provides basic proxy authentication. Users enter proxy server credentials (user name and password) to gain access to their email during an activation of Continuity.
- » If multiple Outlook Extensions are pointing to the same mailbox, it is likely that each instance of Outlook only receives a subset of messages received during an activation since each message is downloaded by the first Outlook Extension instance that polls for the message. It is highly recommended to have only one Outlook Extension per mailbox.
- » The Outlook Extension is not supported on Microsoft Entourage or Microsoft Outlook 2011 for Mac.

Feature comparison with WebMail

The following table compares the features and functionality available to users through WebMail and the Outlook Extension.

Microsoft Outlook Feature	Available in WebMail?	Available in the Outlook Extension?
Send and receive email	Yes	Yes
View or use the message importance feature	Yes	Yes
View or use the message sensitivity feature	No	Yes
Use message delivery options	No	No
View calendars	Yes	Yes
Receive appointments	Yes	Yes
Modify calendars	No	Yes
Send appointments	No	Yes
View contacts	Yes	Yes
Modify contacts	No	Yes
View Global Address List	Yes	Yes
View tasks	No	Yes
Modify tasks	No	Yes
View or use categories	No	Yes
Manage folders	Not applicable	Yes
Access PST folders	Not applicable	Yes
View or use the Reminders window	No	Yes
Access client-side rules (filters)	No	Yes
Access server-side rules and the Out-of-Office feature	No	No
Delegate access or view others' mailboxes	No	No

Outlook Extension Prerequisites and Limitations

Install the Continuity Outlook Extension on systems that meet or exceed the following prerequisites.

Supported Environments

Supported operating systems (32-bit or 64-bit):

- » Windows 7 SP1 or higher
- » Windows 8.1
- » Windows 10

Supported Microsoft Outlook versions (32-bit or 64-bit):

- » 2016
- » 2013
- » 2010 SP1
- » 2007 SP3 - This version is only supported on Windows 7 SP1.

Other prerequisites

The following are required to use the Outlook Extension:

- » Microsoft Outlook must be in cached mode.
- » Users must have administrative permissions on the machine where to install the Outlook Extension.

Outlook Extension Limitations

The following table describes known limitations of the Outlook Extension.

Limitation	Description
One instance per machine.	Outlook Extension does not support more than one instance of Outlook on the same machine.
When upgrading from 32-bit Outlook to 64-bit Outlook, first uninstall the Outlook Extension while still on 32-bit Outlook, and then install Outlook 64-bit, followed by re-installing the Outlook Extension.	If this upgrade procedure is not followed then the user is likely to encounter the following error message: "Microsoft Outlook 2007, or 2010 (x86) is a prerequisite of Outlook Addin (x86)". To resolve this error, the user should first downgrade back to a 32-bit Outlook version, uninstall Outlook Extension, and then install 64-bit Outlook version, followed by installing Outlook Extension.
When an active user on Outlook 2010 replies to a meeting invitation received from a user on Exchange 2010 and includes text in the body of the response, the recipient (on Exchange 2010) does not receive the response message text.	This is confirmed as a bug with Exchange 2010. The recipient's Exchange 2010 server must have the following update installed to resolve this issue: Update Rollup 5 for Exchange Server 2010 Service Pack 1 (KB2582113) or Service Pack 2 for Exchange 2010.
If two instances of Outlook Extension attempt to access the same mailbox at the same time, each instance will pick up different messages. This can confuse users who will not see all messages in both instances.	It is recommended to have only one running instance of Outlook Extension per mailbox at any time. Use WebMail to access a mailbox from a different machine while Outlook Extension is running.
During an activation, read/delivery receipts require user to click Send/Receive button in order to be delivered.	During an activation, read receipts are generated and sent when a user clicks the Outlook Send/Receive button. If a user does not click Send/Receive , the receipts are delivered after recovery.
Because of the way Microsoft encodes new lines in the Description field, meetings created using the Outlook Extension sometimes display \n characters in the text when they are restored by the RecoveryManager. For example, instead of Meeting Request for Monday 4/23 - 11:00 -11:30, the invitation reads \nMeeting Request for Monday 4/23 - 11:00 - 11:30\n.	This is purely a cosmetic issue and the display characters should not cause any malfunction or loss of data. This is under investigation for a future release.
When creating meeting invitations, you can choose conference rooms as recipients (required or optional) but cannot assign them as resources until Outlook is back online.	Outlook cannot process resource requests while offline.

Limitation	Description
The data center validates email addresses when attempting to send a message. If the address is invalid per RFC-822 specifications, the data center fails to send the message, and it remains in the Outlook Outbox during an activation. By contrast, Exchange itself would attempt to send the message even if the address did not conform to RFC-822.	This is an expected difference in behavior between the Outlook Extension and Exchange on the primary mail server.
If a client-side rule (such as move a message from a user on Exchange to a folder) is based on an Exchange address, the rule may not be processed consistently. Rules must use SMTP addresses to behave as expected.	

Installing the Outlook Extension

The Continuity Outlook Extension is provided as an MSI file usable for both GPO and manual installation methods. Outlook Extension conforms to Microsoft-approved Outlook Integration APIs and uses Extended MAPI and Outlook Object Model to interact with Outlook.

Guidelines for installing Outlook Extension:

- » Get the installer from the GFI OneConnect Admin Console. Login to GFI OneConnect using an administrator account and go to **Settings > Downloads**. Download the **Microsoft Outlook Extensions** installers provided on this page.
- » Ensure that the installation package is appropriate according to your operating system and Outlook version. There are two versions of the installation package. The x86 MSI is for 32-bit Outlook versions. The x64 MSI is for 64-bit Outlook versions.
- » Ensure that Microsoft Outlook is not running during the installation process.
- » Outlook Extension can support multiple users running on the same machine in an enterprise environment.
- » The Outlook Extension can also be deployed via GPO. For more information, refer to [Managing the Outlook Extension via GPO](#) (page 63).

Installation procedure

To install the Outlook Extension manually:

1. Close Microsoft Outlook, if it is open.
2. Double-click the MSI file to launch the installer.
3. Follow the installer instructions. Installation may take a few minutes.
4. On install completion, launch Microsoft Outlook.

Ensure that an authentication token is created after installation. Refer to the next section [Outlook Extension token](#).

Outlook Extension token

The Outlook Extension uses an authentication token stored in the registry to allow a user to use the Extension features. Use SyncManager to register a token for all users on a recurring schedule, or run manually for either a single user or all users. A manual single-user run can be useful when troubleshooting errors that occur when writing the token to a mailbox.

To create an Outlook Authentication Update schedule for all users:

1. In the SyncManager main window, click the **Edit Schedule...** button in the **Outlook Authentication Update** area.
2. In the **Edit Outlook Authentication Update Schedule** window, check **Run Scheduled?**.

3. Choose the frequency, day and time to run the update.

4. Click **Save**.

To manually run an Outlook Authentication Update.

1. From the SyncManager main window, click **Update Now** in the **Outlook Authentication Update** area.

2. Select **All Users** to update all users or **Single User** to update a single user and key in the user's SMTP email address.

3. Click **OK**

By default, an Outlook Authentication Update does not overwrite an existing Outlook Authentication token, which means that only users without the token will be updated. You can configure SyncManager to always overwrite the token at each sync run.

To overwrite the Outlook Authentication token:

1. From the SyncManager main window, click **Configure...** in the upper-right corner.

2. In the **Edit Sync Properties** window, select the **Outlook Authentication Update** tab.

3. Check the **Overwrite Token Authentication** box.

4. Click **Save**.

Outlook Extension Administration

The Continuity Outlook Extension allows users to interface with various service features directly from their Outlook Inbox when Continuity is activated. (For information on how to use the Outlook Extension, refer to the online help provided with the Extension.) After the Outlook Extension has been [installed](#), [log in](#) to GFI OneConnect, go to **Manage > Continuity** and click the **Outlook Extension** menu button.

The screenshot shows the 'Outlook Client Information' page. At the top right is the Microsoft logo. Below it is a section titled 'Outlook Client Information' with a sub-instruction: 'View and export provisioning status of Outlook Extension for OneConnect for users in your environment. The page shows extension version for users who have installed the software and successfully connected to the OneConnect servers. You can view detailed information for each user on the list. In addition, you can disable communication between OneConnect and the Outlook Extension.' A note below states: 'Note: Any deleted users or users who haven't logged in to their Outlook Client in 15 days will not be displayed in the list below or listed in the exported CSV file.' There are two main sections: 'Export' (with a link to 'Export all Outlook client information in CSV (Microsoft Excel) format') and 'Manage features' (with a link to 'Enable or disable individual features of the Outlook Extension'). Below these are search fields for 'Search users:' and buttons for 'Search' and 'Clear'. A table lists users with columns: User, State, Extension Version, Outlook Version, and Action. Two users are listed: Jane (jane@mydomain.com) and Keith (keith@mydomain.com), both in a 'Ready' state with 'Outlook Extension 6.9.0 (6.9.0.0)' and 'Outlook Version 14.0.0.7012'. Each user has 'Details' and 'Disable' buttons next to them. Navigation buttons 'Prev' and 'Next' are at the bottom left.

User	State	Extension Version	Outlook Version	Action
Jane (jane@mydomain.com)	Ready	Outlook Extension 6.9.0 (6.9.0.0)	14.0.0.7012	Details Disable
Keith (keith@mydomain.com)	Ready	Outlook Extension 6.9.0 (6.9.0.0)	14.0.0.7012	Details Disable

Screenshot 28: The Outlook Extension management screen

The Outlook Client Information screen provides a list of users, and indicates whether they have installed the Extension and polled the data center. Various actions can be performed:

Action	Description
View Outlook Extension user information	You can search for a specific user, then click the Details button to display: » The user's login history, including which versions of the Outlook Extension and Microsoft Outlook are installed. » A list of policies that apply to the user.
Disable the extension for one user	To disable the extension for one user so that the Extension cannot be used by that user, click the Disable button adjacent to the user's name. Click OK to confirm.
Disable Outlook Extension features for all users	To enable or disable Outlook Extension features for all users, click Manage Features . Select or unselect Email Continuity to enable or disable the Outlook Extension respectively. Click Submit .
Download the list of users	To export the list of Outlook Extension users, click Export . Select to open or save the file in Excel format.

Managing the Outlook Extension via GPO

This topic describes how to install, upgrade, enable/disable and uninstall the Continuity Outlook Extension using GPO.

NOTE

It is recommended that GPO administration is attempted only by system administrators who are familiar with creating and distributing software using GPO. Not all steps in the process are documented here, as each organization's environment is unique and distribution practices may vary.

Installing the Outlook Extension using Group Policy

The Outlook Extension can be distributed through group policy. There are two versions of the Outlook Extension installer. The x86 MSI is for 32-bit Outlook versions. The x64 MSI is for 64-bit Outlook versions. For GPO deployment, you must create two policies, one for the x86 MSI and one for the x64 MSI.

This method is supported under the following guidelines:

- » The Group Policy Object Editor provides configuration settings at the Computer and User levels. Outlook Extension packages should be assigned using the Computer Configuration hierarchy.
- » The Group Policy Object Editor does not display full version numbers. Consequently, it is recommended to use the complete version number in the package name (for example, **Outlook Extension 6-3-0-8015**).

To install the Outlook Extension using Group Policy, create a new GPO package using the Outlook Extension MSI.

1. Open the package in the GPO editor.
2. Go to **Computer Configuration > Software Settings**.
3. Right-click **Software Installation** and select **New > Package**.
4. Browse for the x86 Outlook Extension MSI and click **Open**.
5. In the **Deploy Software** dialog, select **Assigned**, then click **OK**.
6. Right-click the Organizational Unit (OU) and select **Link an Existing GPO**.
7. In the **Group Policy objects:** field, click the x86 GPO and click **OK**.

Repeat this process to create a policy and select the OU for the x64 MSI.

Upgrading the Outlook Extension using Group Policy

To add a new Outlook Extension MSI to the existing policy for the x86 or x64 MSI.

1. Open the package in the GPO editor.
2. Go to **Computer Configuration > Software Settings**.
3. Right-click **Software installation** and select **New > Package**.
4. Browse for the Outlook Extension MSI, select it, and click **Open**.
5. In the left pane, click **Software Installation**. In the right pane, right-click the Outlook Extension package and select **Properties**.
6. Click **Upgrades**. In the **Upgrades** tab, **Add Packages this package will update** field, click **Add**.
7. In the **Add Upgrade Package** dialog, click **Current Group Policy**.
8. In the **Package to Upgrade** field, select **Uninstall the existing package, then install the upgrade package**. Click **OK**.
9. Restart the machines.

Enable or disable the Outlook Extension using Group Policy

These instructions allow you to disable the functionality of the Outlook Extension using Group Policy.

Follow Microsoft instructions and guidelines for distributing registry changes using Group Policy. See <http://technet.microsoft.com/en-us/library/bb727154.aspx>

- » To **disable** the Outlook Extension, set the `LoadBehavior` value to 2 under the `HKEY_LOCAL_MACHINE\Software\Microsoft\Office\Outlook\Addins\ACM.Extensibility2` key.
- » To **enable** the Outlook Extension, set the `LoadBehavior` value to 3 under the `HKEY_LOCAL_MACHINE\Software\Microsoft\Office\Outlook\Addins\ACM.Extensibility2` key.

Removing the Outlook Extension using Group Policy

These instructions allow you to remove the Outlook Extension from user systems using Group Policy.

1. Edit the Group Policy Object.
2. Go to **Computer Configuration > Software Settings** and click **Software installation**.
3. In the right panel, right-click the package and select **All Tasks > Remove**.
4. Select the **immediate removal** method, and click **OK**

Removing the Outlook Extension

To remove the Outlook Extension from users' machines manually:

1. Close Microsoft Outlook, if it is open.
2. Go to **Start > Control Panel > Programs and Features**.
3. Locate the Outlook Extension and follow the instructions to remove it.

When using GPO, you can remove the Outlook Extensions directly from GPO. For more information, refer to [Removing the Outlook Extension using Group Policy](#) (page 64).

Continuity mobile apps

GFI OneConnect includes Android and iOS apps for end-users to access the Continuity WebMail when Continuity is activated. Mobile apps provide a quick and easy way for end-users to continue using email directly from a mobile device while the email infrastructure is down. Through the Mobile apps users also have access to their archived emails.

NOTE

Users need to be given permission before they can start using the mobile apps.

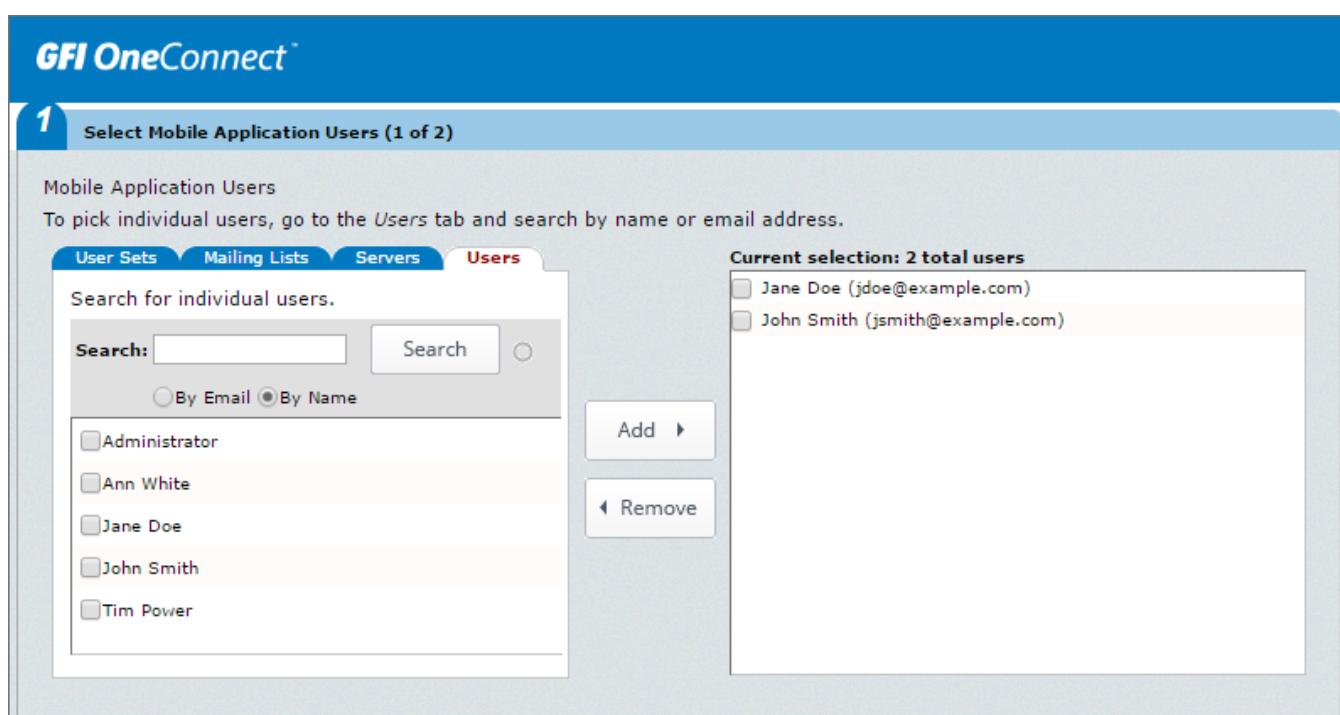
Adding users to the Mobile App list

To enable end-user access to the Mobile App, the users must be added to the Mobile Application Enabled Users list.

To establish a dynamic list of enabled users, create a mailing list or [user set](#) populated with the desired users, or select users by server. When users are added to or removed from the dynamic lists, that change is automatically reflected in the mobile app users list.

To allow users to use the Mobile App:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. On the **Mobile App Administration** tab click **Select Users**.



Screenshot 29: Enabling mobile app for users

4. Select the users to add:

Tabs	Description
User Sets	Predefined sets of users. For more information, refer to Defining User Sets (page 143).
Mailing List	Users that are part of a mailing list. For more information, refer to Mailing Lists (page 47).
Servers	Organization servers. All users that have a mailbox on that server will be included.
Users	Add users that are available in GFI OneConnect one-by-one.

5. Click **Add** to complete the select.
6. The interface displays the list of affected users. Click **Submit**.

To remove user access from the mobile apps:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. On the **Mobile App Administration** tab click **Select Users**.
4. Click the checkbox next to the group or users you want to remove.
5. Click **Remove**.
6. Click **Next** and click **Submit**.

Supported devices

The mobile apps can be installed on the following operating systems:

- » All versions of Android from version 2.3 (Gingerbread) or newer.
- » All versions of iOS from version 6.1 or newer.

Download & install the app

Download the GFI OneConnect mobile apps from the [Android Play Store](#) or the Apple iTunes App Store.

Use search to find the app named **GFI OneConnect**.

The app can be installed like any other free app.

3.2 GFI OneConnect Archiving

GFI OneConnect provides an email archiving feature that preserves all inbound and outbound email within GFI OneConnect Data Center.

GFI OneConnect Archiving ensures that your organization maintains email records for a number of years as required for legal compliance, and for litigation support. The service also helps you offload the continuous increase in storage requirements by emails from your infrastructure.

You can easily create retentions or journaling rules to ensure that email is archived and kept within GFI OneConnect Data Center for as long as necessary. You can also allow users to browse and search archived emails via the web-based interface.

GFI OneConnect Import Manager allows administrators to import historical email data into the GFI OneConnect Archive service. It can import email data from various data stores like Microsoft Exchange mailboxes, Microsoft Office 365 mailboxes, PST files and EML files. This enables to consolidate all previous archiving solutions into a single data store. For more information, refer to [Import Manager](#) (page 105).

To activate archive:

1. Set [Retention Policies](#) to determine the amount of time a message should be kept in the Data Center.
2. Configure an archiving method depending on the type of email server:

Mail server type	Description
Microsoft Exchange	Use the Microsoft Exchange envelope journaling feature to obtain a copy of every email sent or received by the mail server. The emails are then stored in the GFI OneConnect Data Center and the time they will be kept is determined by the Retention Policies. For more information, refer to Using On-premise archiving (page 73).

Mail server type	Description
Microsoft Office 365 in a hybrid environment	GFI OneConnect supports the use of Microsoft Office 365 in a hybrid environment, allowing to have user based archiving on the cloud solution besides the on-premise users of Exchange. It also works with the journaling feature of Microsoft Office 365, which captures a copy of every email and stores them in the GFI OneConnect Data Center. Retention policies are used to determine how long archived emails are kept. For more information, refer to Archiving from Cloud services (page 87).

GFI OneConnect also brings some features to facilitate archive administration:

- » Create Reviewer Groups to facilitate the administration of your company emails. For more information, refer to [Reviewer Groups](#) (page 89).
- » Restore archived emails to users mailboxes using Recovery Archive. For more information, refer to [Restoring emails from Archive](#) (page 95).
- » Monitor storage usage with the Storage Report. For more information, refer to [Retention Policy Storage Report](#) (page 116).

3.2.1 Working with retention policies

Retention policies determine how long email is kept in GFI OneConnect. During the archival process, every message is checked against the Retention Policies in place. If a match is found the message is stamped with the policies settings including the number of days the message should be retained.

A default policy of 1825 days (5 years) is used if no specific policy is applied to a message.

Changes to policy membership and policy retention periods can have a significant impact to the way that mail is stored for your organization.

Retention policy best practices

Retention policies should be carefully constructed and implemented to achieve organizational objectives. The following best practices help you avoid unintended consequences.

- » Determine your business requirements before setting up a retention policy. Before setting up any retention policies, determine what you are trying to achieve, under what constraints your organization works (financial, organizational, statutory), and rank the types of retention you want to achieve from most to least important. Planning for your needs in advance can save the time and frustration from having to change retention policies after implementation.
- » Retention policies with a higher priority always override those of a lower priority, even when the lower priority policy has a longer duration. For example, if the *Executive* retention policy specifies a retention duration of three years and is ranked higher than a *Legal* retention policy that specifies a retention of five years, then a CEO who was a member of both groups would only have his messages retained for three years.

Types of retention policies

GFI OneConnect offers the following policy types:

Policy Types	Description
Capture	<p>Under a capture-based policy, messages are retained based on the user's group membership at the time the message was sent or received.</p> <p>Capture-based policies stamp the email with the policies retention variable. Emails are maintained even if the user leaves the policy. The policy variable changes if the retention is changed. If the policy is deleted, the emails are subject to purge unless held by another policy.</p> <p>This feature is useful if your organization is subject to regulations mandating the amount of time you must store email for employees in certain roles, such as accountants, sales representatives or executives.</p>
Membership	<p>Under membership-based policies, a message is retained based on whether the sender or recipient is a member of the policy. The message is retained only as long as the user remains a member of the group to which the policy applies. When a user is no longer part of the policy group, the message is eligible for purging. Updates to membership-based policies occur after a directory synchronization or when an administrator modifies the policy. Retention rules apply to users currently in the policy. Membership-Based policies are appropriated for temporary workers.</p>
Retention Hold	<p>A Retention Hold is set up for a group of messages that are to be retained and prevented from being purged regardless of any other Retention Policies that may apply to it. This feature is particularly useful during a litigation process where messages must be kept for an undetermined period.</p> <p>When a Retention hold is created it is listed at the top of Retention Policies and ranks higher than other membership-based or capture policies.</p> <p>When a Retention Hold is deleted, messages are then available to be retained or purged based on each individual message's applicable Retention Policies.</p>
Default	<p>The default message policy holds mail for any users in the system who are not controlled by any other policy. The scope of this policy cannot be changed.</p> <p>Note that Increasing or decreasing the length of the policy may result in re-exporting messages.</p>

How to create a retention policy

Administrators can create multiple retention policies of different types to meet the organization's email retention needs.

The administrator can use the GFI OneConnect web admin interface to create membership and capture-based policies. Retention Hold is created by Reviewer group members using a search query. For more information refer to http://go.gfi.com/?pageid=oneconnect_user_help#cshid=hold.

To create a new retention policy:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.

Retention Policies

Retention policies determine how long email will be kept before being purged from the system.

Policy Types

- Membership (Membership-Based Policy):** Retention rules apply to users currently in the policy.
- Capture (Capture-Based Policy):** Retention rules apply to messages to or from users in the policy at the time the message was captured.
- Retention Hold (Query-Based Retention Hold):** An Archive Reviewer identifies specific messages (found by a query) to be retained indefinitely.
- User Classification (User Classification Policy):** Allows designated users to determine which messages are retained under the policy.
- Instant Message (Instant Message-Based Policy):** Retention rules apply to instant messages as per customer specification.
- Default (Default Policy):** The default message policy holds mail for any users in the system who are not controlled by any other policy.

Type	Policy Name	Retention	Last Updated	Statistics	Actions
1 Instant Message	Global IM Capture Policy	3650days		Statistic not yet computed.	Edit
2 Membership	Executive	365days		Statistic not yet computed.	Select Users Edit Delete
3 Capture	Legal	90days		Statistic not yet computed.	Select Users Edit Delete
4 Default	Default Retention Policy	30days		Statistic not yet computed.	Edit

See the [Storage Report](#) section for a complete list of storage across the different policies

Create a new retention policy
Create a new retention policy that will hold mail for a configurable number of days.

Reorder / Re-prioritize Policies
Policies are prioritized in the order shown in the table above, with the highest priority policies at the top of the table.
If multiple policies apply to an email, the highest priority policy will determine when the email is purged.
Click [here](#) to re-order the priority of the list of policies. Changes will not take effect until they are saved.

Screenshot 30: Retention Policies page

3. Click **Create a new retention policy**.
4. Key a name for the policy under the **Name** field.
5. Under **Retain mail for** enter the number of days to retain emails.
6. Select the policy type under the **Retention Type**. The options are:

Option	Description
Capture-Based	This policy retains all email captured for users while they are members of this policy. If a user is removed from this policy, it no longer retains user's new email but it still governs all email that were captured while the user was a member of this policy. This retention type is appropriate for regulatory compliance policies, where email captured for users must be retained regardless of a change in their status or role.
Membership-Based	This policy retains email for all users as long as they remain members of the policy. If a user is removed from the policy, this policy no longer governs any email captured for the user and the retained email are eligible for purging. Check the option Retain deleted users to retain users' email for the normal length of the policy, even after users are deleted.

7. Click **Submit**.
8. In the newly created policy, under **Actions**, click **Select Users**.
9. Select the users to be affected by the policy. The options are:

Tabs	Description
User Sets	Predefined sets of users. Creating user sets can facilitate the administration of GFI OneConnect. It is enough to add or remove users from the group instead of editing policies and other settings. For more information, refer to Defining User Sets (page 143).
Mailing List	Users that are part of a mailing list. Mailing List membership is dynamic, so the list of users in the mailing list is based on the latest sync with the Active Directory environment. For more information, refer to Mailing Lists (page 47).

Tabs	Description
Servers	Organization servers. Selects all users that have a mailbox on the selected server or group. If using an Office 365 server, you can select Office 365 users under the cloud option.
Users	Add users that are available in GFI OneConnect, one-by-one. In the Search box, type an email address or name (using % for wildcard) and search for the results.

10. Click **Submit**.

The newly created policy is automatically assigned higher priority than the Default policy, but lower priority than all the previously created custom policies. Arrange the priority of this policy depending on requirements. For more information, refer to [Changing retention policies priorities](#) (page 71).

Editing Retention Policies

Edit a retention policy to alter its configuration. The options available may vary according to the retention policy type.

The effects of changes in the Retention policies are different depending on the policy type:

Policy Type	Effect
Capture-based	Removing users from the policy does not affect the emails archive. If the retention time is shortened and an email falls out of the retention period it is set for purging.
Membership-based	If a user is removed from the policy, all email belonging to that user are set for purging. If the retention time is shortened and an email falls out of the retention period it is set for purging.
Retention Hold	Only the retention name can be edited. It does not affect the emails included in the hold.
Default	If the retention time is shortened and an email falls out of the retention period it is set for purging.

Editing a policy

To edit a retention policy:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. In the Retention Policies panel select the policy to make changes to and click **Edit**.
4. Select and apply changes to any of the following fields:
 - **Name:** Change the name of the policy.
 - **Retain mail for:** Change the number of days the email will be retained in the Data Center.
 - **Retain deleted users:** When this option is checked it sets the policy to retain mail for the normal length of the policy, even after users are deleted. It is only available when the Retention type is set to **Membership based**.
5. Click **Submit**.

Editing user

To edit the users of a policy:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.

3. Select the policy you want to edit and click **Select Users**.
4. Make the changes to the user selection using the **Add** and **Remove** buttons and click **Submit**.

Changing retention policies priorities

Retention policies should be carefully constructed and implemented to achieve organizational objectives. The order of the Retentions policies plays an important role in this.

Retention policies with a higher priority always override those of a lower priority, even when the lower priority policy has a longer duration. Ensure that policies with a longer retention period are assigned higher priority than those with a shorter period.

To re-order the retention policies:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Click **Reorder / Re-prioritize Policies**.

Type	Policy Name	Retention	Last Updated	Statistics	Actions
DRAG	Instant Message	Global IM Capture Policy	3650days	Statistic not yet computed.	
DRAG	Capture	Legal	90days	Statistic not yet computed.	
DRAG	Membership	Executive	365days	Statistic not yet computed.	
DRAG	Default	Default Retention Policy	30days	Statistic not yet computed.	

Screenshot 31: Retention Policies priority list

4. Drag and drop policies to change the order.
5. Click **Save new ordering** to keep the changes or **Revert** to go back to the original state.

Deleting Retention Policies

This is an irreversible operation. The policy deleted cannot be restored.

NOTE

Deleting a policy causes all email archived under this policy to be marked for purging unless it matches another active policy.

There is a window of time between GFI OneConnect identifying a message eligible for purging and when all records of that message are actually deleted. Eligible messages queued for purging are deleted when the next purge is performed.

To delete a retention policy:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Select the policy you want to eliminate and click **Delete**.

[Working with Retention Holds](#)

A Retention Hold is set up for a set of messages that are to be retained and prevented from being purged regardless of any other Retention Policies that may apply to it. This feature is particularly useful during a litigation process where messages must be kept for an undetermined period.

Retention Holds can be created by administrators or user that are member of a [Reviewer Group](#). To create a retention hold the user must login with an account with review group permission and under Search company archives should create a query to select the emails to be included in the Hold. For more information refer to http://go.gfi.com/?pageid=oneconnect_user_help#cshid=hold.

When a Retention hold is created, it is listed at the top of Retention Policies and is ranked higher than other membership-based or capture policies.

When a Retention Hold is deleted, messages are then available to be retained or purged based on Retention Policies applicable to each individual message.

Administrators can edit or delete Retention Holds from the GFI OneConnect Admin Console.

[Edit a Retention Hold and view a hold's change history](#)

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Identify the Retention Hold policy, and click **Edit**.
4. Only the hold's name can be changed, along with whether or not new messages matching the query are automatically retained. The scope of the hold cannot be changed.
5. Click **Submit**.

[Delete a Retention Hold](#)

Deleting a retention hold is an irreversible operation and all messages included in that hold are set for purging unless they matched another retention policy.

There is a window of time between GFI OneConnect identifying a message eligible for purging and when all records of that message are actually deleted. Eligible messages queued for purging are deleted when the next purge is performed.

To delete a Retention Hold:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.

3. Identify the Retention Hold policy to be deleted, and click **Delete**. A confirmation box appears and reminds you that this action cannot be undone.
4. Click **Delete**.

3.2.2 Using On-premise archiving

GFI OneConnect Archive uses the Journaling feature which enables the recording of email in an organization. Through the journaling feature, your mail server can send a copy of all emails sent and received to a journaling address. The journaling address channels the messages to the GFI OneConnect Data Center.

On-premise archive requires a Microsoft Exchange Server 2007 or later running within the organization premises. GFI OneConnect supports two types of journaling in Exchange:

- » **Standard journaling:** GFI OneConnect can use Microsoft® Exchange Server journaling to centralize all the emails in a single journaling address for archival.
- » **Premium journaling:** Only available with Microsoft® Exchange Enterprise client access license. It enables an administrator to setup custom journaling rules such as:

- Archive only incoming emails
- Archive only outgoing emails
- Archive emails for a particular group.

Which journaling method shall I use?

Choose standard journaling to archive all emails (inbound and outbound) for all users in your organization.

Choose premium journaling if you want more control over the emails to archive. For example, only for specific users or for inbound or outbound only.

NOTE

Premium journaling requires a Microsoft® Exchange Enterprise client access license.

Creating a journaling address

Journaling address can be configured from the GFI OneConnect web administrative console. For more information, refer to [Working with journaling address](#) (page 74).

Testing Journaling

During deployment, the recommendation is to test by configuring journaling for 1 or 2 mailboxes to ensure that journaling rules are accurate, otherwise, messages may be lost and unrecoverable. Ensure the send connector used for GFI OneConnect does not route through a spam filter or content filter, or messages may be lost. Routing to the GFI OneConnect Data Center directly is recommended.

To check the journaling status of a particular user

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. Navigate to **User Administration**.
4. Verify the **Journaling Service** column which displays each users' journaling type applied to the user.

Working with journaling address

A Journaling address is created by default by GFI OneConnect installation. If a further address needs to be created or an existing address needs to be deleted, it can be performed from the GFI OneConnect web administration page.

Create a new journaling address

To create a new journaling address:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Click **On-Premise Journaling**.

Replication Zone	Journaling Address	Last Journal	Action
testcloud.ec2.qa.gfi.com	29095e3accb141cec95644bec63b45390c7de558c9eaa7afba1134075dcaaba9@testcloud.ec2.qa.gfi.com	N/A	Delete

Screenshot 32: On-premise Journaling address created in GFI OneConnect

4. Click **Add On-Premise Journaling Address**.

5. Click **Create**.

Deleting a journaling address

A journaling address can be deleted when required. In cases when a new address is replacing an existing account, it is recommended to allow sufficient time for the existing account to finish processing all the emails before deleting it.

All journaling rules that use a deleted journaling address must be updated.

To delete a journaling address

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Click **On-Premise Journaling**.
4. Locate the address you want to eliminate and click **Delete**.
5. Click **Delete** on the message confirmation pop-up.

Enabling journaling in Microsoft® Exchange 2016

GFI OneConnect uses the journaling feature of Microsoft® Exchange Server to get a copy of every email and stored them in the Data Center.

The process of adding a new journaling address consists of two steps:

1. Locate the journaling address in GFI OneConnect.
2. Create a new contact that uses the journaling address as the main email address and configure the journaling feature of Microsoft Exchange to use the new contact.

Select the journaling type you have available on your Microsoft Exchange Server. For more information, refer to [Using On-premise archiving](#) (page 73).

Set up standard journaling

Step 1: Locate the Journaling address

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Click **On-Premise Journaling**.

Replication Zone	Journaling Address	Last Journal	Action
testcloud.ec2.qa.gfi.com	29095e3accb141cec95644bec63b45390c7de558c9eaa7afba1134075dcaaba9@testcloud.ec2.qa.gfi.com	N/A	Delete

Screenshot 33: On-premise Journaling address created in GFI OneConnect

4. Select and copy the address displayed on the **Journaling Address** column.

Step 2: Configure Journaling in the Exchange Server

1. Launch Microsoft® Exchange admin center.
2. Navigate to **recipients > contacts**.
3. Click the + sign to add a new contact. Set the journaling address of GFI OneConnect as the main email address for the contact created.
4. Navigate to **servers > databases**.
5. Select an existing Mailbox Database and click **Edit**.
6. Click **maintenance**.
7. In the **Journal recipient** field, click **browse** and select the contact created.
8. Click **save**.

Set up premium journaling

Step 1: Locate the Journaling address

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Click **On-Premise Journaling**.

The screenshot shows the GFI OneConnect web interface. In the top left, it says "GFI OneConnect". The top right has icons for Home, Manage, Settings, Help, and User. A sidebar on the left lists: Admin Console Home, Historical Mail, Retention Policies, Storage Report, Reviewer Groups, Email Recovery, and On-Premises Journaling (which is selected). The main content area is titled "On-Premises Journaling". It says "Manage on-premises replication zones and journaling addresses. You can manage cloud journaling addresses [here](#). Note: More than one journaling address may be active per journal replication zone." Below this is a table with one row:

Replication Zone	Journaling Address	Last Journal	Action
testcloud.ec2.qa.gfi.com	29095e3accb141cec95644bec63b45390c7de358c9aa7afba1134075dcaaba98@testcloud.ec2.qa.gfi.com	N/A	Delete

Screenshot 34: On-premise Journaling address created in GFI OneConnect

4. Select and copy the address displayed on the **Journaling Address** column.

Step 2: Configure Journaling in the Exchange Server

1. Launch Microsoft® Exchange admin center.
2. Navigate to **recipients > contacts**.
3. Click the + sign to add a new contact. In the main email address option paste the journaling address of GFI OneConnect.
4. Navigate to **Compliance management > Journal rules**.
5. Click the + sign to add a new rule.
6. Key in the contact created under **Send journal reports to:**
7. Under **Name** type a unique name for the rule.
8. In the field **If the message is sent or received from...** select one of the options available:

Option	Description
Apply to all messages	Select this option to have all message archived. This option is preferred when compliance is required from your organization.
A Specific user or group	Select this option to enable archiving to certain users or groups only. This option is optimal to limit storage usage. When this option is selected use the next screen to choose a user or group.

9. In the field **Journal the following messages** select the scope of the journal rule clicking the drop-down arrow. The options are **all messages, internal messages only** or **external messages only**.

10. Click **save**.

Enabling journaling in Microsoft® Exchange 2013

GFI OneConnect uses the journaling feature of Microsoft® Exchange Server to get a copy of every email and stored them in the Data Center.

The process of adding a new journaling address consists of two steps:

1. Locate the journaling address in GFI OneConnect.
2. Create a new contact that uses the journaling address as the main email address and configure the journaling feature of Microsoft Exchange to use the new contact.

Select the journaling type you have available on your Microsoft Exchange Server. For more information, refer to [Using On-premise archiving](#) (page 73).

Set up standard journaling

Step 1: Locate the Journaling address

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Click **On-Premise Journaling**.

The screenshot shows the GFI OneConnect interface with the title 'GFI OneConnect' at the top. On the left is a sidebar with icons for Admin Console Home, Historical Mail, Retention Policies, Storage Report, Reviewer Groups, Email Recovery, and On-Premises Journaling. The main content area has a header 'On-Premises Journaling' with a note about managing replication zones and journaling addresses. Below this is a section titled 'Add On-Premises Journaling Address'. A table lists a single entry:

Replication Zone	Journaling Address	Last Journal	Action
testcloud.ec2.qa.gfi.com	29095e3accb141cec95644bec63b46390c7de558c9eaa7afba1134075dcaaba9@testcloud.ec2.qa.gfi.com	N/A	Delete

Screenshot 35: On-premise Journaling address created in GFI OneConnect

4. Select and copy the address displayed on the **Journaling Address** column.

Step 2: Configure Journaling in the Exchange Server

1. Launch Microsoft® Exchange admin center.
2. Navigate to **recipients > contacts**.
3. Click the + sign to add a new contact.
4. In the main email address paste the journaling address of GFI OneConnect.
5. Navigate to **servers > databases**.
6. Select an existing Mailbox Database.
7. Click **Edit** from the toolbar.
8. Click **maintenance**.
9. Click **browse** and select the contact created in the **Journal recipient** field.
10. Click **save**.

Set up premium journaling

Step 1: Locate the Journaling address

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Click **On-Premise Journaling**.

The screenshot shows the GFI OneConnect web interface. In the top navigation bar, there are links for Home, Manage, Settings, Help, and User. On the left sidebar, there are links for Admin Console Home, Historical Mail, Retention Policies, Storage Report, Reviewer Groups, Email Recovery, and On-Premises Journaling. The main content area is titled "On-Premises Journaling" and contains a sub-section "Manage on-premises replication zones and journaling addresses. You can manage cloud journaling addresses [here](#). Note: More than one journaling address may be active per journal replication zone." Below this is a button "Add On-Premises Journaling Address". A table lists a single journaling address entry:

Replication Zone	Journaling Address	Last Journal	Action
testcloud.ec2.qa.gfi.com	29095e3accb141cec95644bec63b45390c7de358c9eaa7afba1134075dcaaba98@testcloud.ec2.qa.gfi.com	N/A	Delete

Screenshot 36: On-premise Journaling address created in GFI OneConnect

4. Select and copy the address displayed on the **Journaling Address** column.

Step 2: Configure Journaling in the Exchange Server

1. Launch Microsoft® Exchange admin center.

2. Navigate to **recipients > contacts**.

3. Click the + sign to add a new contact. Set the journaling address of GFI OneConnect as the main email address for the contact created.

4. Navigate to **Compliance management > Journal rules** and click the + sign.

5. Under **Send journal reports to:** key in the contact created previously.

6. Under **Name** type a name for the rule. The name should be unique in the organization.

7. In the field **If the message is sent or received from...** select one of the options available:

Option	Description
Apply to all messages	This option archives all email sent or received. Use this option when compliance is required from your organization.
A Specific user or group	This option enables archiving to certain users or groups only. This option is preferred when the priority is to limit storage usage. If this option is selected a new screen appears to select the user or group.

8. In the field **Journal the following messages** select the scope of the rule clicking the drop-down arrow. The options available are **all messages, internal messages only** or **external messages only**.

9. Click **save**.

Enabling Journaling in Microsoft® Exchange Server 2010

GFI OneConnect uses the journaling feature of Microsoft® Exchange Server to get a copy of every email and store them in the Data Center.

The process of adding a new journaling address consists of two steps:

1. Locate the journaling address in GFI OneConnect.

2. Create a new contact that uses the journaling address as the main email address and configure the journaling feature of Microsoft Exchange to use the new contact.

Select the journaling type you have available on your Microsoft Exchange Server. For more information, refer to [Using On-premise archiving](#) (page 73).

Set up standard journaling

Step 1: Create a new journaling address

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Click **On-Premise Journaling**.

The screenshot shows the GFI OneConnect interface with the title "GFI OneConnect". The left sidebar includes links for Admin Console Home, Historical Mail, Retention Policies, Storage Report, Reviewer Groups, Email Recovery, and On-Premises Journaling. The main content area is titled "On-Premises Journaling" and contains a note about managing on-premises replication zones and journaling addresses. It also includes a link to manage cloud journaling addresses. A table lists a single journaling address: "testcloud.ec2.qa.gfi.com" under "Replication Zone" and "29095e3accc141ce95644bec63b45390c7de258c9eaa7afba1134075dcaaba9@testcloud.ec2.qa.gfi.com" under "Journaling Address". The table has columns for "Last Journal" (N/A) and "Action" (Delete).

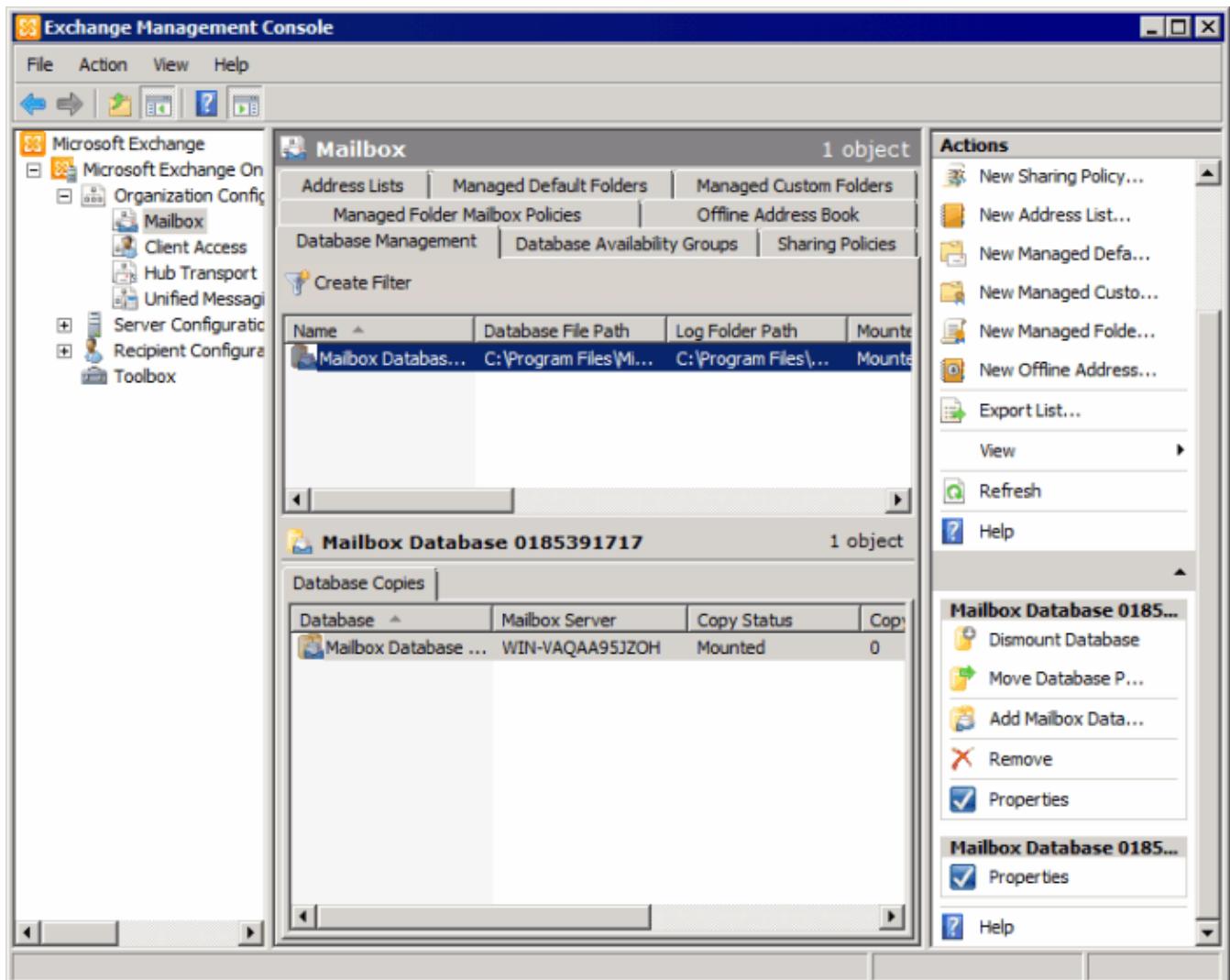
Replication Zone	Journaling Address	Last Journal	Action
testcloud.ec2.qa.gfi.com	29095e3accc141ce95644bec63b45390c7de258c9eaa7afba1134075dcaaba9@testcloud.ec2.qa.gfi.com	N/A	Delete

Screenshot 37: On-premise Journaling address created in GFI OneConnect

4. Select and copy the address displayed on the **Journaling Address** column.

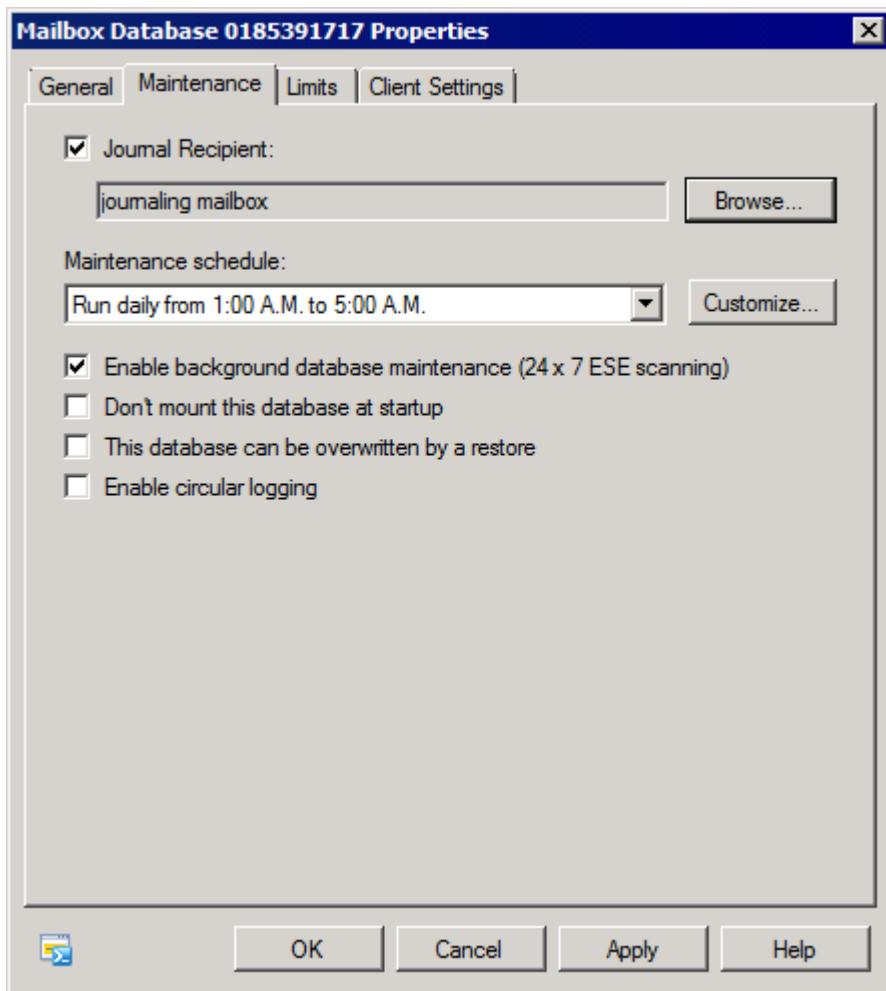
Step 2: Configure standard journaling

1. Create a **new contact** in Active Directory.
2. Set the journaling address of GFI OneConnect as the main email address for the contact.
3. Launch **Microsoft Exchange Management Console**.



Screenshot 38: Configuring a Mailbox Database

4. Expand **Microsoft Exchange > Organization Configuration > Mailbox node**. Right-click the Mailbox database and select **Properties**.



Screenshot 39: Mailbox Database properties

5. From the mailbox database properties dialog, select the **Maintenance** tab and select the **Journal Recipient** checkbox. Click **Browse**, and select the contact created in Active Directory.
6. Click **OK** to finalize setup.

Set up premium journaling

Step 1: Create a new journaling address

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Click **On-Premise Journaling**.

Replication Zone	Journaling Address	Last Journal	Action
testcloud.ec2.qa.gfi.com	29095e3accb141cec95644bec63b45390c7de358c9aa7afba1134075dcaaba98testcloud.ec2.qa.gfi.com	N/A	Delete

Screenshot 40: On-premise Journaling address created in GFI OneConnect

4. Select and copy the address displayed on the **Journaling Address** column.

Step 2: Set up premium journaling

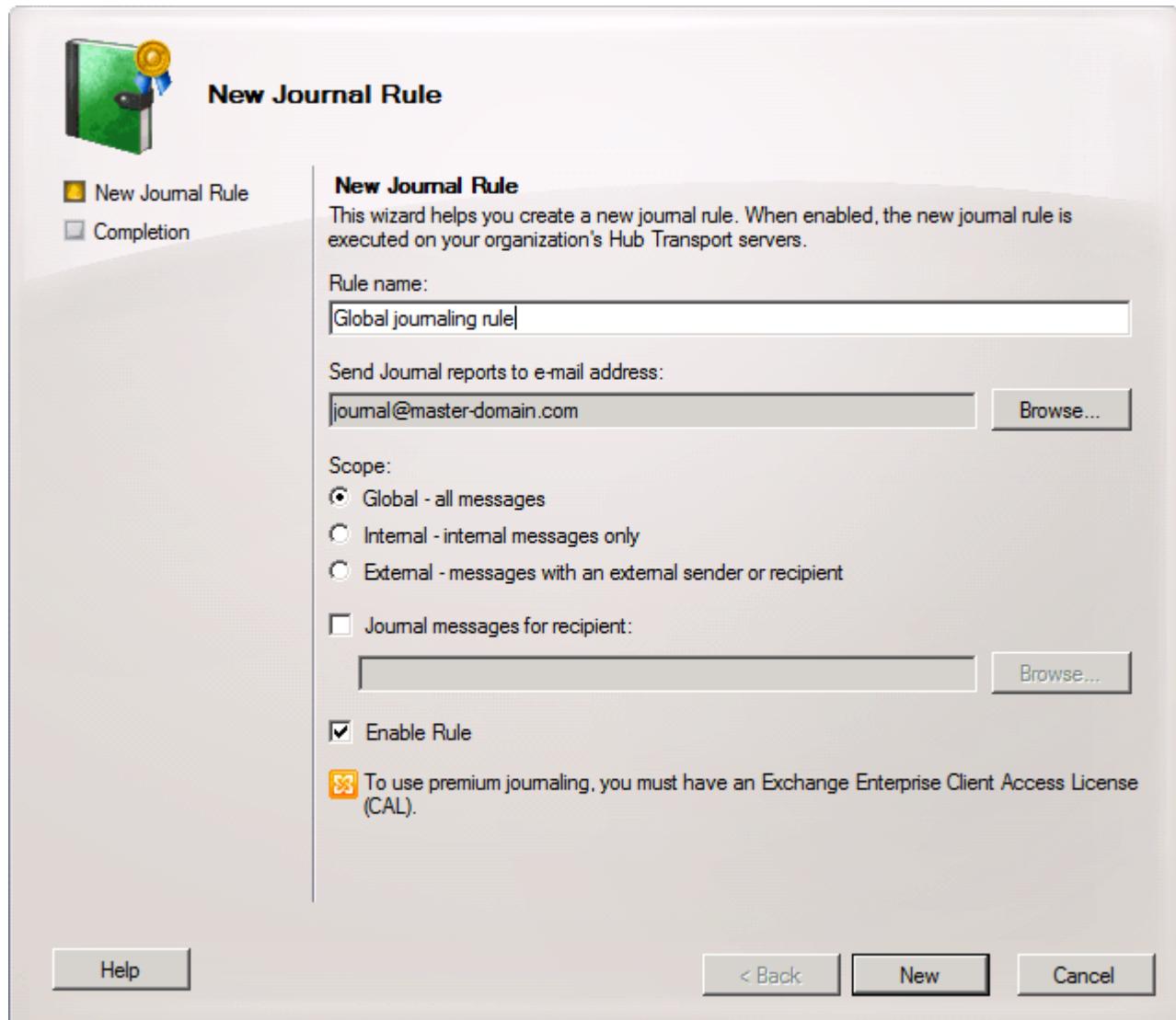
1. Create a **new contact** in Active Directory.

2. Set the journaling address of GFI OneConnect as the main email address for the contact.

3. Launch **Microsoft Exchange Management Console**.

4. Expand **Organization Configuration > Hub Transport** node and select **Journaling** tab.

5. From the **Actions** tab, click **New Journal Rule**.



Screenshot 41: Creating a new Journaling rule

6. Key in a name for the new rule

7. Click **Browse** to select the contact created in Active Directory.

8. <Optional> Configure:

- Scope - Select whether to journal all email (Global), internal or external email.
- Journal messages for recipient - Select specific recipient(s) for this journaling rule.

9. Ensure that **Enable Rule** option is enabled and click **New**.

Enabling Journaling in Microsoft® Exchange Server 2007

GFI OneConnect uses the journaling feature of Microsoft® Exchange Server to get a copy of every email and stored them in the Data Center.

The process of adding a new journaling address consists of two steps:

1. Locate the journaling address in GFI OneConnect.
2. Create a new contact that uses the journaling address as the main email address and configure the journaling feature of Microsoft Exchange to use the new contact.

Select the journaling type you have available on your Microsoft Exchange Server. For more information, refer to [Using On-premise archiving](#) (page 73).

Setting up standard journaling

Step 1: Create a new journaling address

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Click **On-Premise Journaling**.

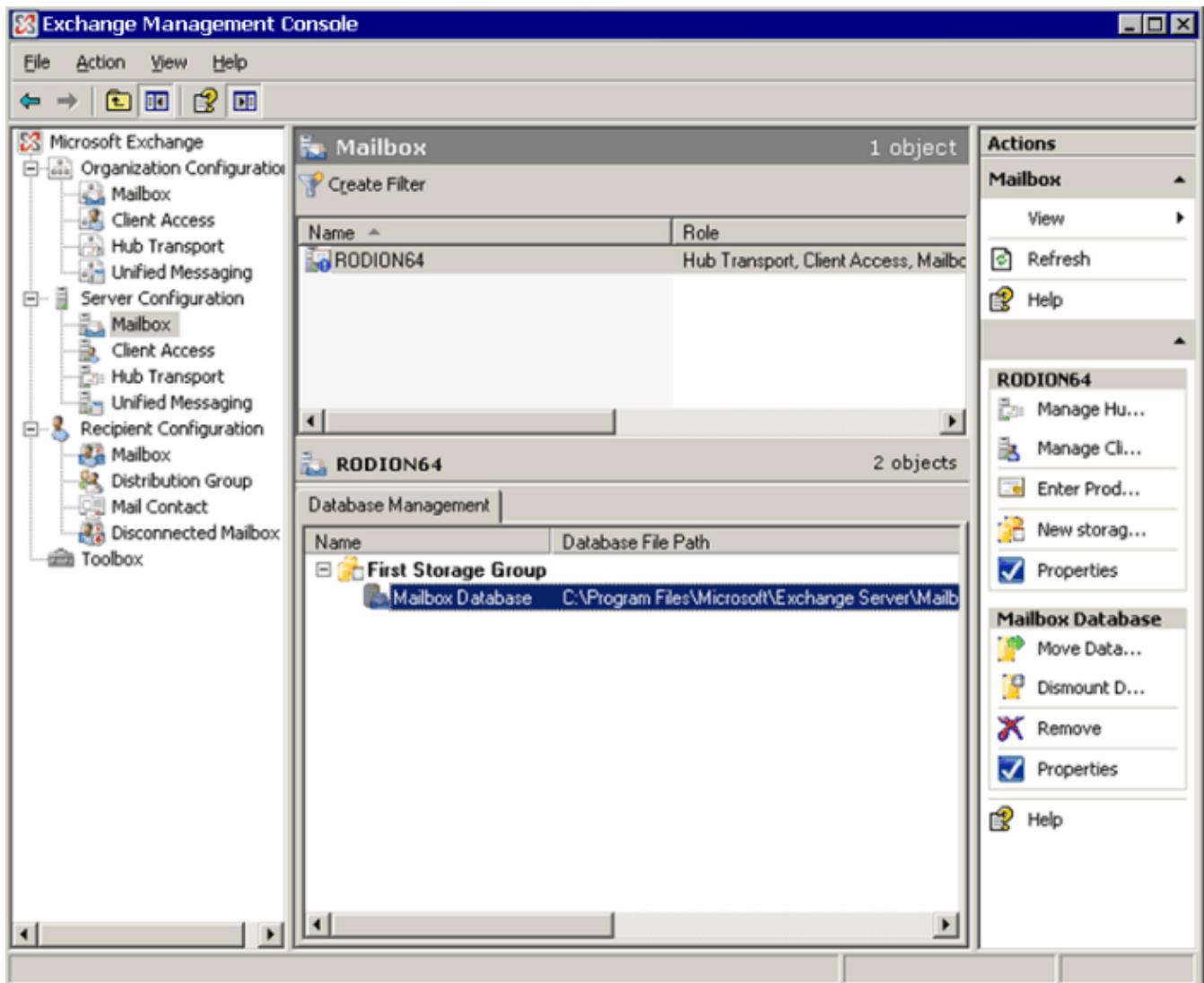
Replication Zone	Journaling Address	Last Journal	Action
testcloud.ec2.qa.gfi.com	29095e3accc141cec95644bec63b45390c7de958c9eaa7afba1134075dcaaba9@testcloud.ec2.qa.gfi.com	N/A	Delete

Screenshot 42: On-premise Journaling address created in GFI OneConnect

4. Select and copy the address displayed on the **Journaling Address** column.

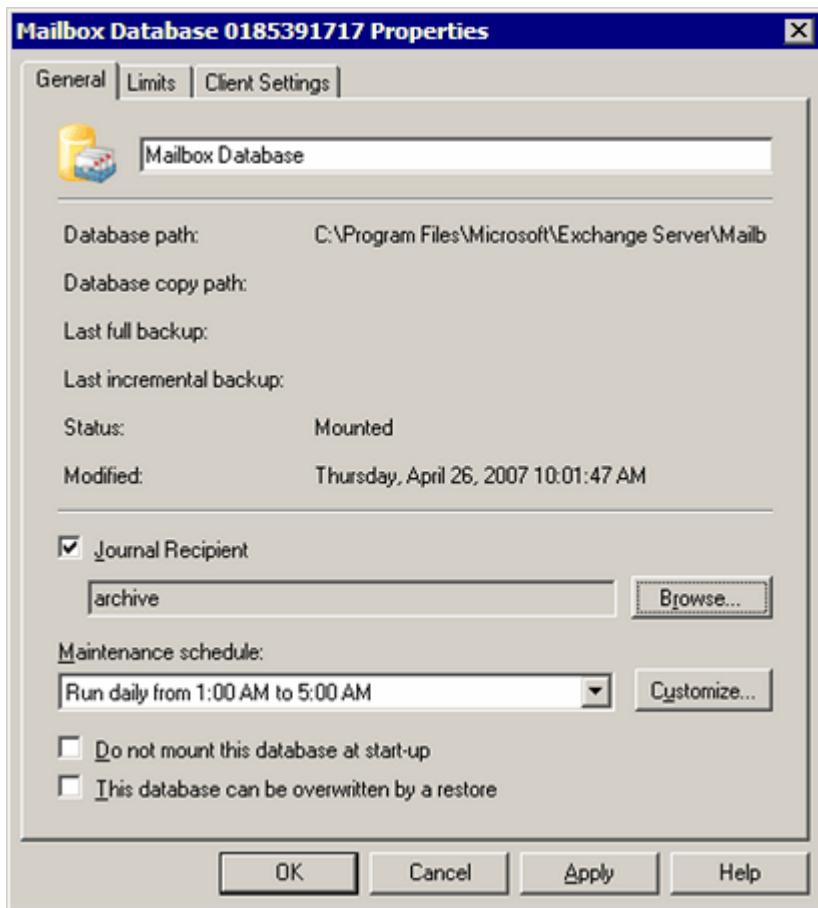
Step 2: Configure standard journaling

1. Create a **new contact** in Active Directory.
2. Set the journaling address of GFI OneConnect as the main email address for the contact.
3. Select **Start > All Programs > Microsoft Exchange Server 2007 > Microsoft Exchange Management Console**.



Screenshot 43: Configuring a Mailbox Database

4. Expand Microsoft **Exchange > Server Configuration > Mailbox node** and click **Properties** from the **Actions** pane.



Screenshot 44: Mailbox Database properties

5. Select **Journal Recipient** option, click **Browse** and select the contact created in active directory.

6. Click **OK** to finalize setup.

Setting up premium journaling

Step 1: Create a new journaling address

1. Login to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Click **On-Premise Journaling**.

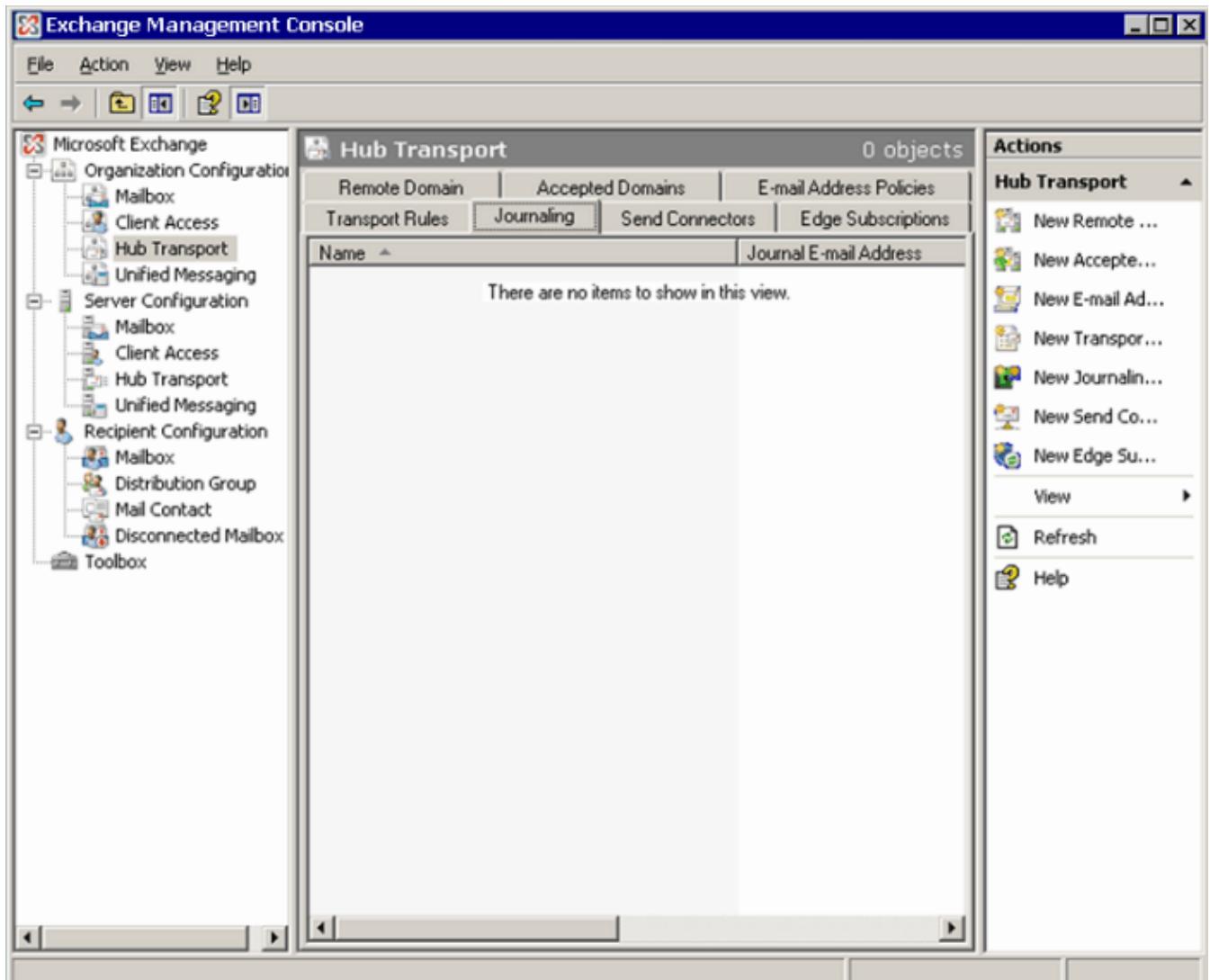
Replication Zone	Journaling Address	Last Journal	Action
testcloud.ec2.qa.gfi.com	29095e3accb141cec95644bec63b45390c7de358c9eaa7afba1134075dcaaba98@testcloud.ec2.qa.gfi.com	N/A	Delete

Screenshot 45: On-premise Journaling address created in GFI OneConnect

4. Select and copy the address displayed on the **Journaling Address** column.

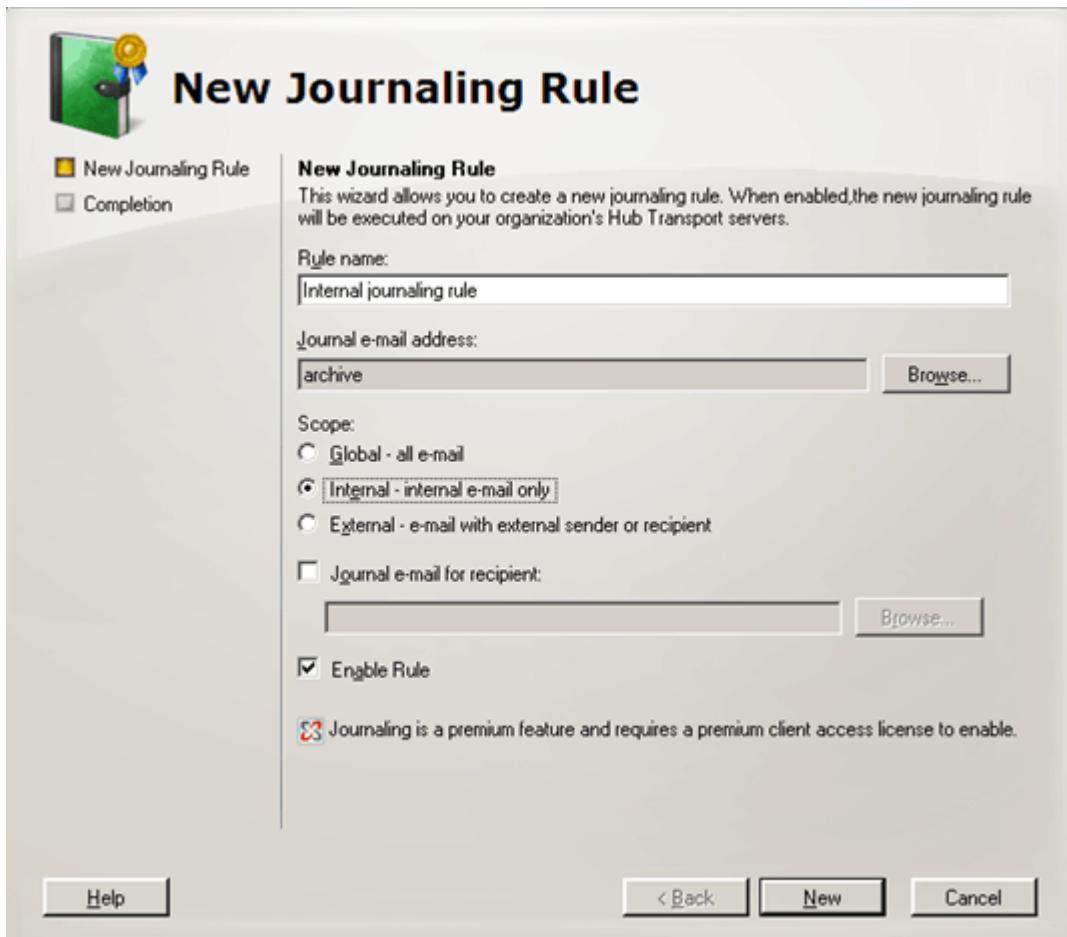
Step 2: Configure Premium journaling

1. Create a **new contact** in Active Directory.
2. Set the journaling address of GFI OneConnect as the main email address for the contact.
3. Select **Start > All Programs > Microsoft Exchange Server 2007 > Microsoft Exchange Management Console**.



Screenshot 46: Configuring Journaling rules

4. Expand **Organization Configuration > Hub Transport** node and select **Journaling** tab.
5. From the **Actions** tab and click on **New Journaling Rule**.



Screenshot 47: Creating a new Journaling rule

6. Key in a name for the new rule and click **Browse**. Select the contact created in Active Directory.

7. <Optional> Configure:

- **Scope** - Select whether to journal all email (Global), internal or external email.
- **Journal e-mail for recipient** - Select specific recipient(s) for which this journaling rule applies.

3. Ensure that the **Enable Rule** option is enabled and click **New**.

3.2.3 Archiving from Cloud services

Cloud Services is an optional GFI OneConnect Archive function that provides support for Microsoft Office 365 hybrid environments.

If users already have Office 365 mailboxes stored when GFI OneConnect is installed, the Cloud Service can be configured immediately. For more information, refer to [Configuring Cloud Services](#) (page 87).

If GFI OneConnect is already setup and you need to migrate mailboxes from a Microsoft Exchange server on-premise to Office 365, then the archiving method needs to be switched. For more information, refer to [Migrating to Microsoft Office 365](#) (page 89).

Configuring Cloud Services

The GFI OneConnect Cloud Services feature manages the journaling addresses to which all copies of journaling mail are sent. A journaling address is a Globally Unique Identifier (GUID) that is dedicated to your server. GFI OneConnect allows the creation of a journaling address that can be linked to an Office 365 account.

Cloud user's journaling address ensures that a copy of every email sent or receive by that account is forwarded to the GFI OneConnect Data Center.

Creating a new Cloud journaling address

To create a new Cloud journaling account:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Navigate to **Cloud Services**.

The screenshot shows the GFI OneConnect web interface. On the left is a sidebar with various navigation links: Admin Console Home, Historical Mail, User Administration, Cloud Services (which is selected and highlighted in grey), Mobile App Administration, Outlook Extension, Mailing Lists, Notification, Audit Reports, and System Settings. The main content area has a blue header bar with 'GFI OneConnect' on the left and icons for Home, Manage, Settings, Help, and User profile on the right. Below the header, the 'Cloud Services' section is visible, with a sub-section titled 'Cloud Services'. It says 'Manage cloud services and journaling addresses.' and includes a note: 'Note: More than one journaling address may be active per cloud service.' To the right of this note is a small blue icon of a book with a checkmark. Below this is a table titled 'Add Office 365 Journaling Address'. The table has columns for 'Cloud Service', 'Journaling Address', 'Last Journal', and 'Action'. A single row is shown for 'Office 365' with the journaling address '1ab3a017a3efd20564c7c0bf4fb1917b89345a48f27ae567aa037bbcfee814d5@testcloud.ec2.qa.gfi.com' and 'N/A' in the last two columns. There is a red 'Delete' button at the end of this row. In the center of the page is a modal dialog box titled 'Create Journaling Address'. It contains the text: 'A new [Office 365](#) journaling address will be created for the following zone: testcloud.ec2.qa.gfi.com'. Below this is another note: 'Note: Existing journaling addresses will remain active until deleted.' At the bottom of the modal are 'Cancel' and 'Create' buttons. The overall background of the interface is light grey.

Screenshot 48: Creating a new journaling address

4. Click **Add Office 365 Journaling Address** and click **Create**.
5. Select and copy the Office 365 journaling address.
6. Create a journaling rule in Microsoft Office 365 that forwards a copy of all emails to the GFI OneConnect journaling address. Detailed information on how to do this is available on http://go.gfi.com/?pageid=MAR_O365JournalingRule
7. Set the journaling address of GFI OneConnect as the address of the journaling rule in Office 365.

Deleting a journaling address

A journaling address can be deleted when required. In cases when a new address is replacing an existing account, it is recommended to allow sufficient time for the existing account to finish processing all the emails before deleting it.

All journaling rules that use a deleted journaling address must be updated.

To delete a journaling address:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.

3. Navigate to **Cloud Services**.

4. Locate the account you want to eliminate and click **Delete**.

Migrating to Microsoft Office 365

This topic describes how the GFI OneConnect Archiving setup needs to be handled when migrating a Microsoft Exchange environment to Microsoft Office 365.

Important notes to consider before migrating:

- » GFI OneConnect only supports the archiving feature for users of Microsoft Office 365. The [continuity](#) and [security](#) features are not available.
- » GFI OneConnect requires Microsoft Office 365 in hybrid mode and the Microsoft directory synchronization tool.
- » Cloud managed Microsoft Office 365 instances are not supported.
- » The Microsoft Office 365 plan must support Microsoft Exchange journaling.
- » Ensure that Continuity is in the **Ready** state before migrating any users. Important status information may be compromised when migrating users during a partial or full activation.
- » Create Retention policies that cater for the new users of the GFI OneConnect Cloud Services. A Capture Based Policy is preferred, but a Membership Policy can be used as well. For more information, refer to [Working with retention policies](#) (page 67).

When all of the above items are met, it is recommended to begin the migration process by migrating only one test mailbox. Create a journaling address and link it to the test mailbox first. Get the test mailbox working before moving on to bigger groups of users.

When the test is confirmed, you may then proceed with migration.

After migration ensure that retention polices and Microsoft Office 365 journaling policies remain in sync.

3.2.4 Reviewer Groups

Archive users who are members of a Reviewer Group have the ability to search and read emails that are within the scope of that Reviewer Group, and to create [Recovery archives](#) and [Retention Holds](#).

Any GFI OneConnect user can be designated as an Archive Reviewer. The individual does not need to have a personal email archive; that is, their personal user account does not need to be part of a retention policy.

Only Administrators can create, edit or delete Reviewer Groups. Administrators can view the Reviewer Group's Mailbox Scope and list of Reviewers.

When creating Reviewer Groups, the Mailbox Scope is a feature that restricts the emails each Reviewer Group is able to access. The Mailbox Scope can be defined in terms of Users, User Sets, Mailing Lists and Servers, and any combination thereof.

Creating a new Reviewer Group

Administrators can create Reviewer groups. Archive users who are members of a Reviewer Group have the ability to search and read emails that are within the scope of that Reviewer Group, and to create [Recovery archives](#) and [Retention Holds](#).

To create a new Reviewer Group:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.

Tabs	Description
User Sets	Predefined sets of users. Creating user sets can facilitate the administration of GFI OneConnect. It is enough to add or remove users from the group instead of editing policies and other settings. For more information, refer to Defining User Sets (page 143).
Mailing List	Users that are part of a mailing list. Mailing List membership is dynamic, so the list of users in the mailing list is based on the latest sync with the Active Directory environment. For more information, refer to Mailing Lists (page 47).
Servers	Organization servers. Selects all users that have a mailbox on the selected server or group. If using an Office 365 server, you can select Office 365 users under the cloud option.
Users	Add users that are available in GFI OneConnect, one-by-one. In the Search box, type an email address or name (using % for wildcard) and search for the results.

8. Click **Add**. Repeat until all desired users are displayed in the right-hand pane. To remove items from the selection pane, check the box beside the item and click **Remove**. Click **Next**.
9. Under the **Select Reviewer** section select users to be members of the Reviewer Group. Search the users from the **Mailing Lists** or **Users** tabs.
10. To further limit the messages available to the Archive Reviewer, such as email messages within a specific date range, or emails with a specific topic, click the **Advanced options** link. In the **Query Text** field enter a query. For more information, refer to [Advanced Query Language](#) (page 92). Click **Next**.
11. Review the summary of the Reviewer Group being created and click **Submit** to finalize.

Editing a Reviewer Group

Editing a Reviewer Group may invalidate its associated [Recovery Archives](#). Ensure that all associated Recovery Archives have been restored prior to editing the Reviewer Group.

To edit a Reviewer Group:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Navigate to **Reviewer Groups**.
4. Locate the Reviewer Group to be edited, and then click **Edit**.
5. On the **Reviewer Group Name** page, only the **Name** of the group can be changed. Click **Next**.
6. On the **Review Scope** page, add or delete users, user sets, mailing lists or servers from the scope of messages this Reviewer Group is allowed to see. Click **Next**.
7. On the **Select Reviewers** page, add or remove reviewers from the list. Click **Next**.
8. Review the changes and click **Submit** to confirm the changes.

Deleting a Reviewer Group

A Reviewer Group cannot be deleted if it is associated with any Retention Holds. Delete all the associated Retention Holds, then proceed with the Reviewer Group deletion procedure.

To delete a Reviewer Group:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Navigate to **Reviewer Group**.
4. Locate the Reviewer Group to be deleted, and then click **Delete**.
5. Click **Delete** to remove the Reviewer Group.

Query Language Search

Search is an important feature of GFI OneConnect Archive because it allows user to group email using various criteria. This feature is particularly useful when dealing with very large archive and information needs to be retrieved quickly.

Reviewer Group users can create query searches using two methods:

- » **Query Builder**. Using the web interface to define the parameters of the search.
- » **Advanced Query Language**. Using the in-built query capabilities of GFI OneConnect. This option allows building more complex search syntax with multiple conditions.

Which method should I use?

The **Query builder** uses a web interface that facilitates to build simple queries. This method is suitable for end users or simple queries. To learn more about Query Builder refer to http://go.gfi.com/?pageid=oneconnect_user_help#cshid=CompanySearch

The **Advanced Query Language** requires a deep knowledge of the search syntax. It is more suitable for administrator or complex searches that involve multiple variables.

Using Advanced Query Language

The Advanced Query Language uses the in-built query engine of GFI OneConnect to build up complex search queries.

To facilitate your query building:

- » Enclose phrases in double quotation marks.
- » Use parenthesis to group logic decisions.
- » Use a single wildcard such as a tilde, start, or exclamation point to return all results.

The Advanced Query allows administrators to create a single query with multiple conditions like:

- » Contains the subject X
- » From user Y or Z
- » Excluding mail sent in a determined date range

Example:

```
(mailsubject:"Quarterly Report" AND (senders:user@example.com OR senders:anotheruser@example.com) AND NOT emaildate:range(2017-01-31T23:00:00,2017-02-28T22:59:00) ).
```

For more information, refer to [Advanced Query Language](#) (page 92).

Search Limitations

Use Caution When Editing Generated Queries

Searches built with the **Query Builder** can be further edited clicking the **Advanced Query Language** tab. When editing a generated query, change these arguments with care, or the query may not return the expected search results.

Message Envelope Search Limitations

Message envelope searches (*envrecipients* and *recipients* query language fields) may return different results from a similar search done in Microsoft Outlook. That is due to the fact that the Advance Query Language can only search the envelope information that GFI OneConnect is able to capture.

For undisclosed recipient information (including Bcc recipients), the only addresses that will be captured are internal addresses included in a retention policy.

When searching for undisclosed recipients, the undisclosed recipient headers is not visible in the search results but the relevant messages are included in the result set.

Limitations When Formulating Long Queries

In Internet Explorer, the URL length limit of 2083 characters can cause errors when executing a long discovery query. If a query URL exceeds the character limit, Internet Explorer will display an error message and the query will not execute.

This scenario is most likely when using the Query Language or Query Builder options to build a complex query containing many search parameters. Simple searches are not likely to trigger this issue.

One workaround is to use a web browser with longer URL character limits, such as Mozilla Firefox or Chrome. Another workaround is to narrow down the search to fewer parameters.

Advanced Query Language

The Advanced Query Language allows users to create a single query with multiple conditions.

How to use the Advanced Query Language

To access the Advance Query Language tab, login to GFI OneConnect with a user that is member of a reviewer group and under **Archive** click **Search company archives**. In the Search page click **Advance Query Language**.

To start a search:

1. Type the query in the format: `field:term`, where `field` is one of the elements of an email and `term` is the value you want to find. For example, `mailsubject:"Quarterly Report"`
2. Add other conditions linking them with Boolean operators. For Example, `(mailsubject:"Quarterly Report" AND mailfrom:bob@genericcorp.com)` .

Search For Range of Dates

To search for mail using a range of dates type a query in the format `field:range (start, end)` .

Elements	Description
Field	Field that indicates the element to be searched upon. Accepted fields are <code>emaildate</code> or <code>receiveddate</code> .
Range	Defines the beginning and ending points of the search.
Start	Indicates the beginning of the search. Date can be entered as date and time format like <code>YYYY-MM-DDTHH:MM:SS</code> . If time is omitted the system uses <code>00:00:00</code> . Use <code>min</code> to indicate a search from the beginning of data stored.

Elements	Description
End	Indicates the ending of the search. Date can be entered as date and time format like YYYY-MM-DDTHH:MM:SS. If time is omitted the system uses 23:59:59. Use <code>max</code> to indicate a search till the end of data stored.

For example:

To find all messages sent between December 25, 2013 and August 1, 2015 (local time):

```
emaildate:range (2013-12-25T05:00:00, 2015-08-01T05:00:00)
```

To find messages sent before December 25, 2016 (local time):

```
emaildate:range (min, 2016-12-25T05:00:00)
```

To find messages received on or after August 2, 2016 (local time):

```
receiveddate:range (2016-08-02T05:00:00, max)
```

Boolean Operators

To combine search expressions using Boolean operators (AND, OR and NOT), use:

- » AND between terms, to indicate *both* terms must be matched.
- » OR between terms, to indicate *either* term may be matched, but at least one *must* match.
- » NOT as a prefix to a term, to find terms that do *not* match the specified criteria.

Use matched parenthesis () to group terms.

For example:

To find messages that include either the phrase `financial report` or the phrase `balance sheet` and were sent before December 25, 2013 or after August 1, 2015, but not between those dates.

```
NOT (emaildate:range (2013-12-25T05:00:00, 2015-08-01T05:00:00)) AND  
("financial report" OR "balance sheet")
```

Query Language Fields

The table below contains a detailed description of every field available together with some examples.

Field (Type)	Description	Example
altrecipients (String)	Alternative recipients listed in the To field or Cc field of the envelope journal report.	<code>altrecipients: bob_anderson@ genericorp.com</code>
attachedfiles (String)	<ul style="list-style-type: none"> » A filename (If filename contains spaces, enclose in quotes). » Filenames joined by Boolean expression (If filename contains spaces, enclose in quotes). » To match an ordered list of attachments use a semi-colon separated list of all filenames, enclosed in quotes (No need to add extra quotes to filenames with spaces). 	<ul style="list-style-type: none"> » <code>attachedfiles: picture.jpg</code> » <code>attachedfiles: picture.jpg or "second picture.jpg"</code> » <code>attachedfiles: "report.xls; report.doc; Quarterly Report.ppt"</code>
content (String)	The content of the message.	<code>content:"Q4 results"</code>
dlists (String)	Distribution lists listed in the To field or Cc field of the envelope journal report.	<code>dlists: all_employees@ genericorp.com</code>

Field (Type)	Description	Example
emaildate or receiveddate (Date)	<p><i>emaildate</i>: The date specified in the Sent Date field of the message header.</p> <p><i>receiveddate</i>: The date the message was received by the email server.</p> <p>To search by date only, use the form YYYY-MM-DD. To search by date and time, use the form YYYY-MM-DDThh:mm:ss.</p> <p>T is a required constant that identifies the following characters as times.</p> <p>Use 24-hour clock when specifying time.</p> <p>Use min and/or max to specify earliest/latest dates.</p> <p>Use < or > to specify dates before or after a certain date.</p> <p>Note: By default, emaildate is stored as UTC (GMT) time. To search using your local time zone value, use the TIME value to manually compensate for the number of hours offset from UTC. For example: T05:00:00 is midnight in the US-Central time zone.</p>	<ul style="list-style-type: none"> » To find messages received between January 1, 2008, midnight (US-Central time zone) and January 3, 2009, midnight: received-date:range (2008-01-01T05:00:00, 2009-01-03T05:00:00) » To find messages sent after Aug. 21, 2012 use: emaildate:>2012-08-21 » To find messages sent before Aug. 21, 2012, use: emaildate:<2012-08-21 » To find messages received before Aug. 21, 2012, use: receivedate:<2012-08-21
envrecipients (String)	<p>The recipient information contained in the message envelope.</p> <p><i>For non-journalized messages</i>: This field can be used to search for Bcc recipients.</p> <p>NOTE: Only email addresses found in retention policies can be found using this option. It will not find any email addresses that are external to your organization or not included in a retention policy.</p>	envrecipients: bob_anderson@genericcorp.com
envsender (String)	The sender information contained in the message envelope.	envsender: bob_anderson@genericcorp.com
filename (String)	The file name of a document or message.	filename: report.xls
isattachment (Integer)	<p>An indicator of whether the document is an email attachment or a message.</p> <p>To indicate that the document is an attachment, set isattachment:1.</p> <p>To indicate that the document is not an attachment, set isattachment:0.</p>	filename: report.xls and isattachment:1
mailbcc (String)	Recipients listed in the Bcc field of the envelope journal report.	mailbcc: bob_anderson@genericcorp.com
mailbccaltrecipient (String)	Alternative recipients listed in the Bcc field of the envelope journal report.	mailbccaltrecipient: bob_anderson@genericcorp.com
mailbccdlist (String)	Distribution lists listed in the Bcc field of the envelope journal report.	mailbccdlist: all_employees@genericcorp.com
mailcc (String)	The recipients listed in the Cc field of the message header.	mailcc: bob@genericcorp.com
mailccaltrecipient (String)	Alternative recipients listed in the Cc field of the envelope journal report.	mailccaltrecipient: bob_anderson@genericcorp.com
mailccdlist (String)	Distribution lists listed in the Cc field of the envelope journal report.	mailccdlist: all_employees@genericcorp.com

Field (Type)	Description	Example
mailfrom (String)	The sender listed in the From field of the message header.	mailfrom:bob@genericorp.com
mailsubject (String)	The subject of the message. If value contains spaces, enclose in double-quotes.	mailsubject: "Quarterly Report"
mailto (String)	The recipients listed in the To field of the message header.	mailto: bob@genericorp.com
mailtoaltrecipient (String)	Alternative recipients listed in the To field of the envelope journal report.	mailtoaltrecipient: bob_anderson@ genericorp.com
mailtotolist (String)	Distribution lists recipients listed in the To field of the envelope journal report.	mailtotolist: all_employees@ genericorp.com
recipients (String)	The recipients listed in one or more of the following: <ul style="list-style-type: none"> » The list of recipient information contained in the message envelope (see <i>enveloprecipient</i> field for details) » The To field of the message header. » The Cc field of the message header. » Distribution lists listed in the To field or Cc field of envelope journal report. » Alternative recipients listed in the To field or Cc field of envelope journal report. 	(recipients:bob@ genericorp.com OR recipients:sue@ genericorp.com)
senders (String)	The list of senders in the message envelope or the From field of the message header.	(senders:bob@ genericorp.com OR senders:sue@ genericorp.com)
undisclosedrecipient (String)	Undisclosed recipients listed in one or more of the following: <ul style="list-style-type: none"> » The list of recipients in the Bcc field of the envelope journal report. » The list of distribution lists in the Bcc field of the envelope journal report. » The list of alternative recipients in the Bcc field of the envelope journal report. 	undisclosedrecipients: bob_anderson@ genericorp.com

3.2.5 Restoring emails from Archive

This section describes the process of restoring email from the GFI OneConnect Archive back into your mail server mailboxes.

The process involves two steps:

Step 1: Create a recovery archive	GFI OneConnect Administrators and members of Reviewer Groups can create custom recovery archives, consisting of messages that are archived into GFI OneConnect, based on specific criteria. For example, create a recovery archive based on emails sent and received in a specific date range, or a particular group of users. For more information, refer to Creating Recovery Archive (page 95).
Step 2: Restore messages to mail server	Use the RecoveryManager to restore messages in the recovery archive to user mailboxes. For more information, refer to RecoveryManager (page 25).

Creating Recovery Archive

GFI OneConnect Administrators and members of Reviewer Groups can create custom Recovery Archives, consisting of messages that are archived into GFI OneConnect. The Recovery Archives can be created based on the following criteria:

Date range	<p>A Time-Based Recovery Archive consists of emails that were sent and received in a specific time period.</p> <p>Example: The mail server crashed last night, wiping out the last 12 hours of email before it could be delivered. An administrator logs into GFI OneConnect and creates a Time-Based Recovery Archive for all mail during that 12 hour period, allowing all mail to be delivered to user mailboxes the next day.</p> <p>When creating a Time-Based Recovery Archive, specify the following criteria:</p> <ul style="list-style-type: none"> » Start date and time » End date and time » Users whose emails are to be included in the archive. <p>Examples of Time-Based Recovery Archives:</p> <ul style="list-style-type: none"> » All messages for user John Jones between January 1, 2017 and September 1, 2017. » Mail for all users on the mailing list Sales between July 1, 2017 and August 1, 2017. <p>For more information, refer to Creating a Time-Based Recovery Archive (page 96).</p>
Activation-Based	<p>Create Activation-Based Recovery Archives to recover all mail sent and received during a time period prior to the beginning of a Continuity activation. Similar to a standard time-based recovery archives, the end time of an Activation-Based Archive is bound by the point at which the Continuity activation occurred.</p> <p>Example: The mail server crashed last night, and several hours later, administrators determined it will take a significant amount of time to resolve the problem. At which point, the Continuity administrator initiated an Activation to re-route users' emails for the duration of the outage. While the mail servers are being fixed, an Email Archive administrator can log into GFI OneConnect to create an Activation-Based Recovery Archive for all mail during the time period between the crash and the beginning of the activation, allowing all mail to be delivered to user mailboxes the next day.</p> <p>For more information, refer to Creating an Activation Based Recovery Archive (page 98).</p>

NOTE

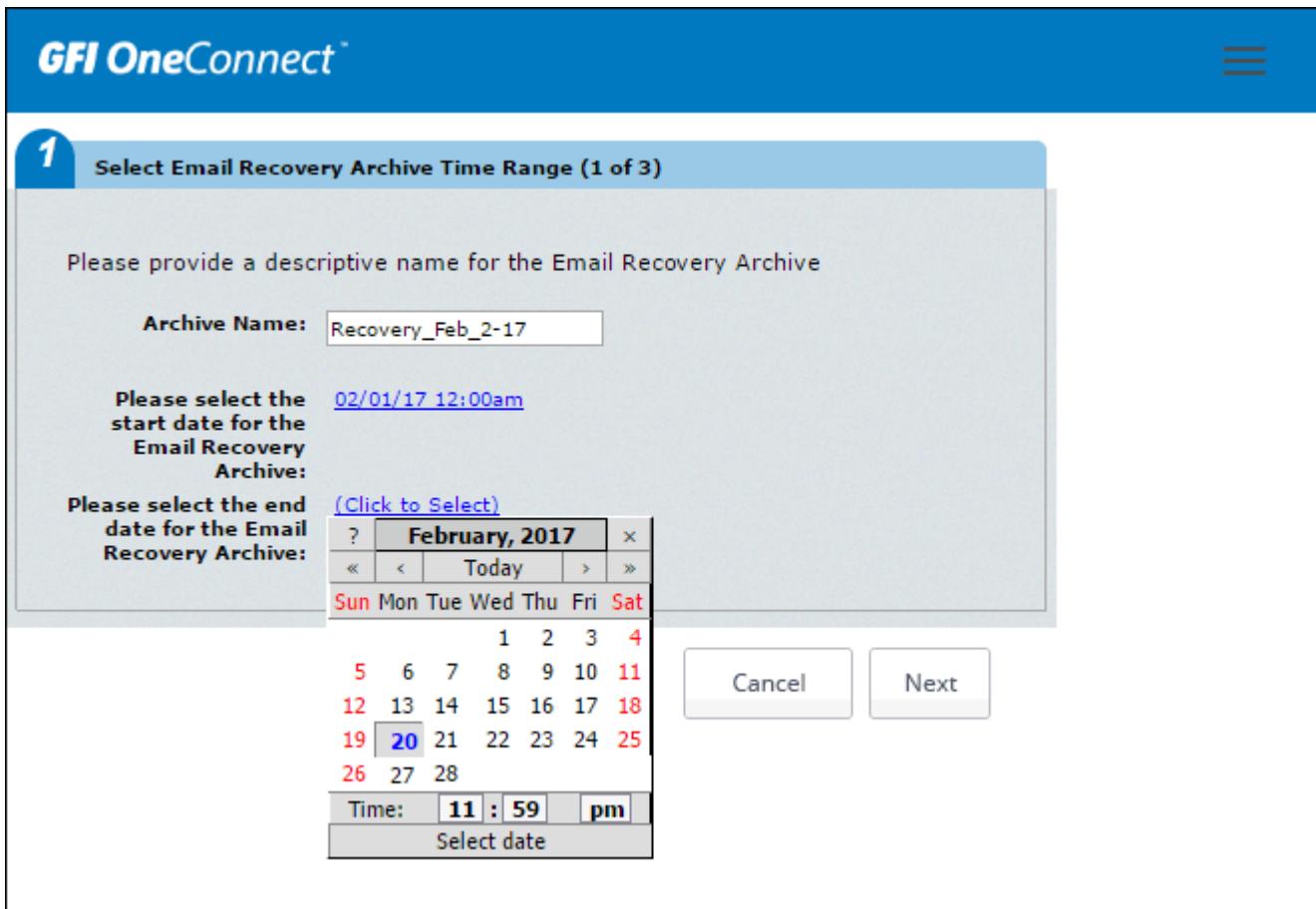
Email messages that are contained in a Recovery Archive are kept until the archive is deleted, regardless of any applicable retention policies. After the archive is deleted, control of each message's purge status reverts to the highest priority applicable retention policy.

After creating a Recovery Archive, you can use the RecoveryManager to restore the messages within the Recover Archive to end users' mailboxes, or to a designated mailbox for review. For more information, refer to [Using RecoveryManager to restore Archives](#) (page 99).

Creating a Time-Based Recovery Archive

To create a Time-Based Recovery Archive:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Navigate to **Email Recovery**.
4. Click **Create a Time Based Recovery Archive**.



Screenshot 49: Selecting the time range of a time-based Recovery Archive

5. Type a name for the archive in the **Archive Name** field. All archive names must be unique.
6. Set Start and End date for the Email Recovery Archive.
7. Click **Next**.
8. Identify the users whose messages must be collected in the archive:

Tabs	Description
User Sets	Predefined sets of users. Creating user sets can facilitate the administration of GFI OneConnect. It is enough to add or remove users from the group instead of editing policies and other settings. For more information, refer to Defining User Sets (page 143).
Mailing List	Users that are part of a mailing list. Mailing List membership is dynamic, so the list of users in the mailing list is based on the latest sync with the Active Directory environment. For more information, refer to Mailing Lists (page 47).
Servers	Organization servers. Selects all users that have a mailbox on the selected server or group. If using an Office 365 server, you can select Office 365 users under the cloud option.
Users	Add users that are available in GFI OneConnect, one-by-one. In the Search box, type an email address or name (using % for wildcard) and search for the results.

9. Click **Add**. Repeat until all desired users are listed in the right-hand pane.

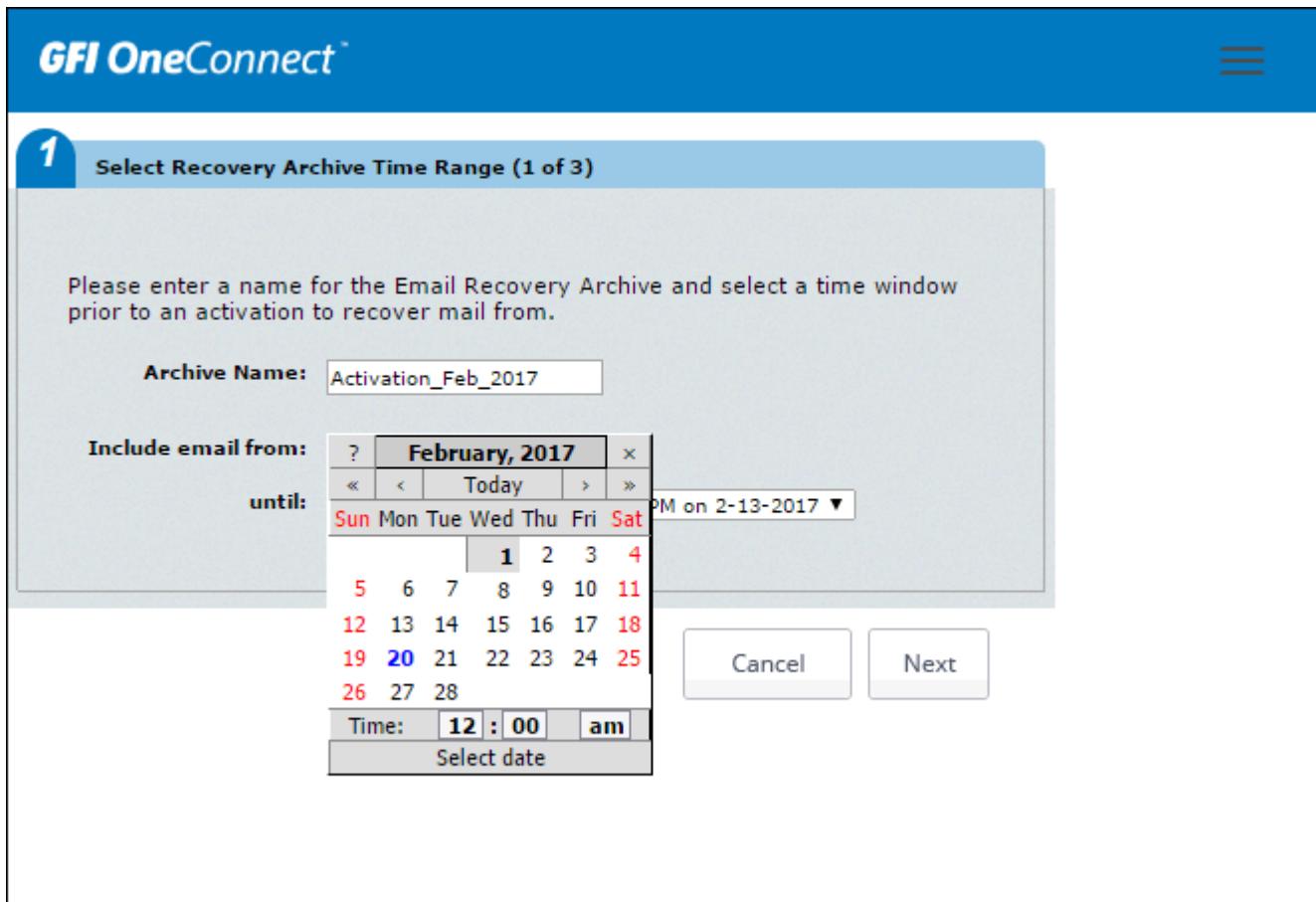
10. Click **Next** and click **OK** to complete the operation.

Next step: Recover the emails in the newly created archive to your mail system using RecoveryManager. For more information, refer to [Using RecoveryManager to restore Archives](#) (page 99).

Creating an Activation Based Recovery Archive

To create an Activation Based Recovery Archive :

1. Login to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Navigate to **Email Recovery**.
4. Click **Create Activation Based Recovery Archive**.



Screenshot 50: Selecting the time range of an Activation based Recovery Archive

5. Type a name for the archive in the **Archive Name** field. All archive names must be unique.
6. In the **Include email from** field, set the start date and time for email recovery.
7. In the **Until** dropdown, select the activation that will define the ending of this recovery archive.
8. Click **Next**.
9. Identify the users whose messages must be collected in the archive:

Tabs	Description
User Sets	Predefined sets of users. Creating user sets can facilitate the administration of GFI OneConnect. It is enough to add or remove users from the group instead of editing policies and other settings. For more information, refer to Defining User Sets (page 143).
Mailing List	Users that are part of a mailing list. Mailing List membership is dynamic, so the list of users in the mailing list is based on the latest sync with the Active Directory environment. For more information, refer to Mailing Lists (page 47).

Tabs	Description
Servers	Organization servers. Selects all users that have a mailbox on the selected server or group. If using an Office 365 server, you can select Office 365 users under the cloud option.
Users	Add users that are available in GFI OneConnect, one-by-one. In the Search box, type an email address or name (using % for wildcard) and search for the results.

10. Click **Add**. Repeat until all desired users are listed in the right-hand pane.

11. Click **Next** and click **OK** to complete the operation.

Next step: Recover the emails in the newly created archive to your mail system using RecoveryManager. For more information, refer to [Using RecoveryManager to restore Archives \(page 99\)](#).

Using RecoveryManager to restore Archives

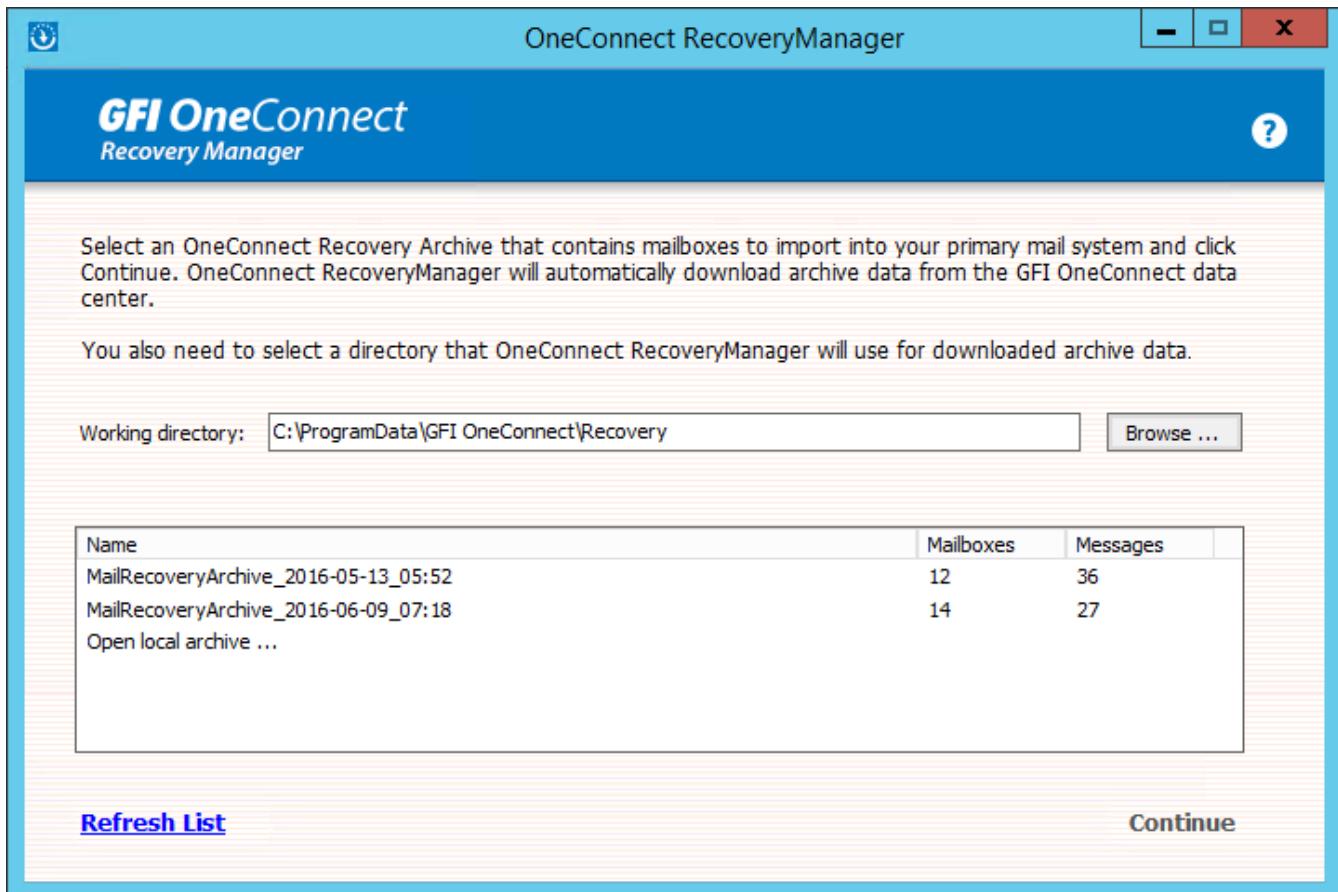
Use [RecoveryManager](#) to recover emails from [previously-created Recovery Archives](#) to user mailboxes.

1. On your GFI OneConnect server that hosts RecoveryManager, go to **Start > Programs > GFI OneConnect > RecoveryManager**.

2. Log into the RecoveryManager using a GFI OneConnect Administrator account with sufficient [permissions on the Exchange server](#).

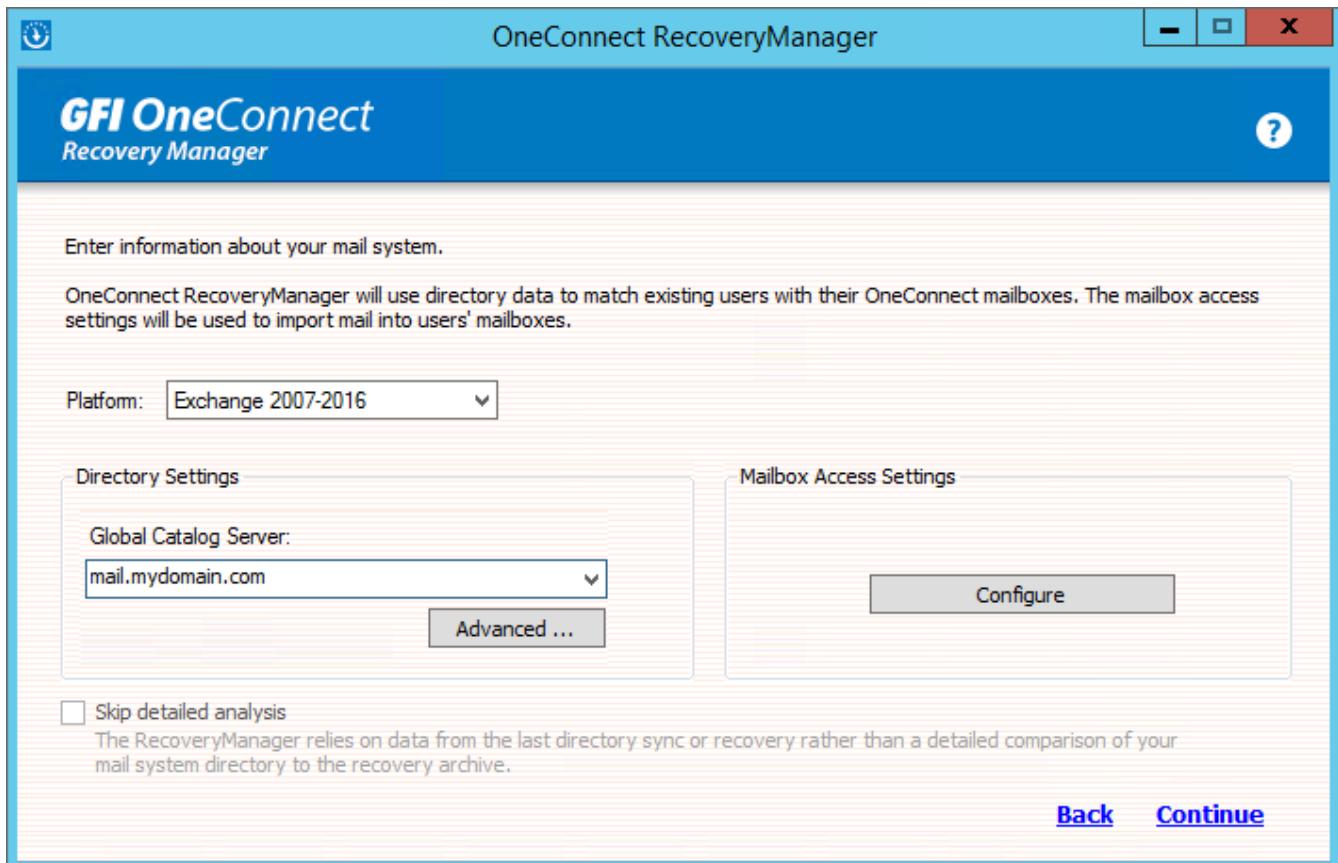
3. Click **Start Recovery**.

4. Select the **Working directory** for RecoveryManager to use as a temporary data store during the import process. Ensure that the directory chosen has sufficient disk space for all mail items. Also ensure that there is no anti-virus or backup software that may be scanning this folder, since it may block important temporary files causing errors. Refer to the anti-virus or backup software's instructions for how to exclude directories from scans. The default path is: <system drive>\ProgramData\GFI OneConnect



Screenshot 51: Choosing the mail archive to recover

5. From the list of available recovery archives, choose the Recovery Archive that was previously created. For more information, refer to [Creating Recovery Archive](#) (page 95). Click **Continue**.
6. The RecoveryManager downloads the archive metadata into the working directory. Actual mail data is downloaded for each user later in the process.



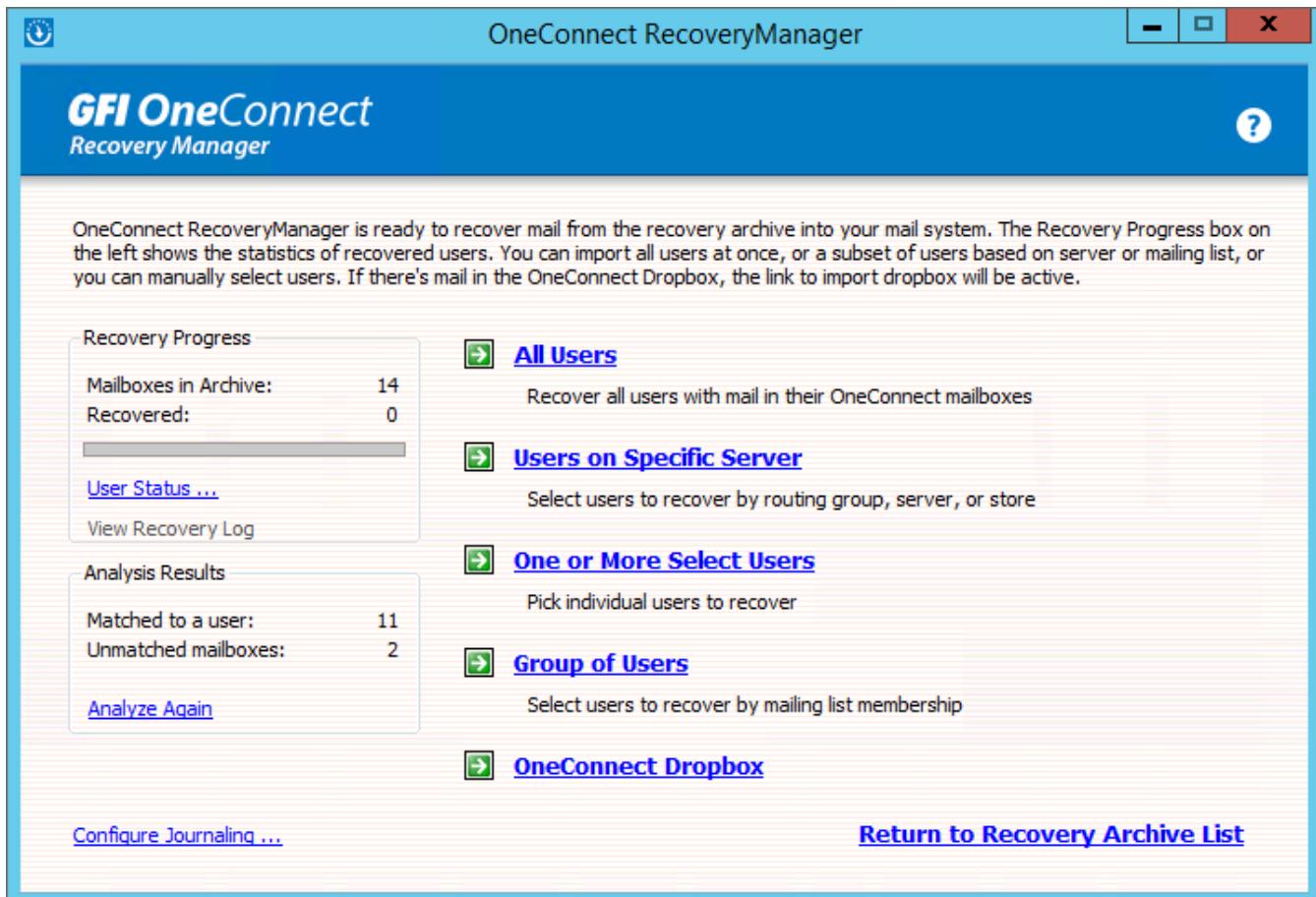
Screenshot 52: RecoveryManager global catalog settings

7. RecoveryManager uses platform information pulled from SyncManager to access the primary email system. Typically these settings are correct for recovery. If, however, there were changes applied to the mail system, such as changes to the global catalog server or EWS connection settings, click **Configure** to adjust these settings.

8. During recovery, directory information is compiled as part of the process. If SyncManager is installed, and if the most recent Directory sync was successful, RecoveryManager can use the cached results from the Directory sync for the recovery process. To use this cached data, check the **Skip detailed analysis** check box.

9. Click **Continue**.

10. RecoveryManager analyzes the archive to match up mailboxes in the archive to users' mailboxes in the primary mail system. The duration of this process depends on the number of mailboxes. Click **Continue**.



Screenshot 53: RecoveryManager mailbox and archive statistics

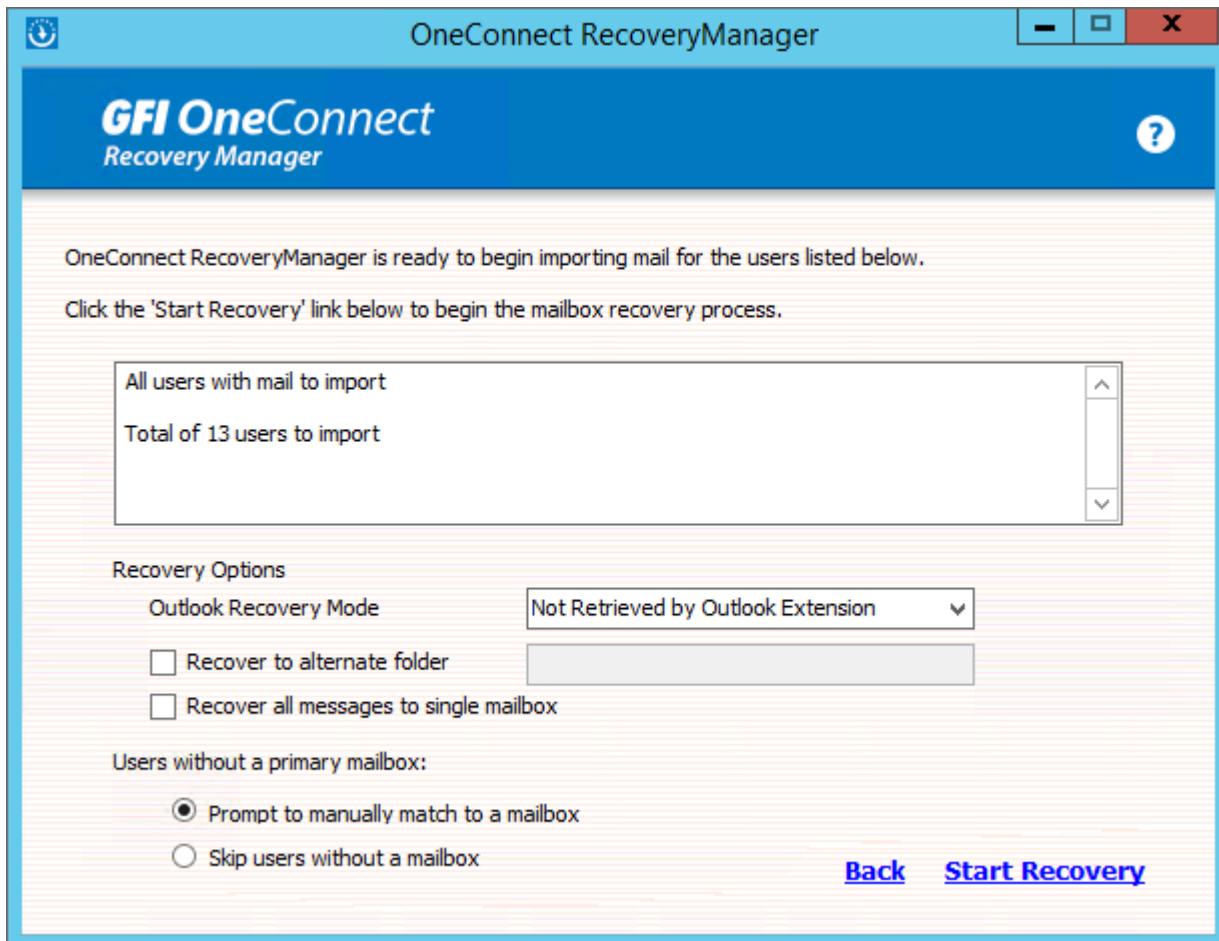
11. RecoveryManager shows mailbox and archive statistics to choose how to recover the archive:

Option	Description
Mailboxes in Archive	The total number of mailboxes in the archive.
Recovered	The number of mailboxes for which mail has been recovered.
User Status	Click to review a detailed status of each user, including usernames per server, user accounts with email data for recovery, and user accounts that cannot be matched to an account on the primary mail system.
Matched to a user	The number of user accounts that can and cannot be matched to an account on the primary mail system.
Unmatched mailboxes	The number of mailboxes that cannot be associated with a user in the primary mail system.
Analyze Again	Click to re-analyze the archive mailboxes.

Option	Description
Configure Journaling	<p>Click to specify a journaling mailbox where to store a copy of all messages transmitted during activation. This is useful for example when using a mail archiving solution such as GFI Archiver which retrieves mail from a journaling mailbox. Select the group, server or store you want to configure journaling for and click Change. Select the journaling mailbox where to copy all messages to and click OK.</p> <p>Also configure:</p> <ul style="list-style-type: none"> » BCC Journaling: Usually, the identity of a recipient in BCC is not exposed when mail is recovered to a journaling mailbox. Select this option to append the recipient's email address to the BCC field in email recovered to the journaling mailbox. If you're recovering the mail to an alternate mailbox, the alternate mailbox's address will be appended as well. Note that recipient's email address and alternate mailbox address (if applicable) are always added irrespective if original email contained recipients in BCC or not. » Save configuration for future use: Select this option to save these journaling settings for future recovery operations.

12. In the user selection area, select the users to run recovery for and click **Continue**.

User set	Description
All Users	Recover email data for all users who were activated during the outage and for which data has not yet been recovered.
Users on Specific Server	Recover email data for users on a selected message store, server, or group of servers. Check any combination of individual mail stores, servers, or server groups for recovery. (Servers without users that need recovery are grayed out.) Click Continue .
One or More Select Users	<p>Recover the mailbox of one user or the mailboxes of selected users by name. Select/Search users to recover and click Add to copy them to the user list in the right column.</p> <p>You may also override the destination of the user's restored email data. Select a user and click Properties to configure. Click Continue.</p>
Group of Users	Recover users based on distribution list membership. RecoveryManager lists all distribution lists with members who have email that needs recovery. Select groups and click Add to copy the group to the right column. Click Continue .
Dropbox	This option provides a repository for received emails sent to non-existent mailboxes or addresses not found in GFI OneConnect. If you select this option, select a server and mailbox to which all Dropbox content will be imported. Click Continue .



Screenshot 54: Recovery options

13. Choose how to restore the mail:

Option	Description
Outlook Recovery Mode	When using the Outlook Extension, emails processed during a Continuity activation are downloaded by the Outlook Extension and stored in the Microsoft Outlook OST file. When Microsoft Exchange is restored, Microsoft Outlook automatically replicates these emails with the mailbox. Choose what to do with emails processed by the Outlook Extension: <ul style="list-style-type: none"> » Not retrieved by Outlook Extension – only recovers emails that were not delivered to an Outlook Extension client. » Retrieved by Outlook Extension – only recovers emails that were delivered to an Outlook Extension client. This is useful when replication of data between Microsoft Outlook and Microsoft Exchange fails, such as when a Microsoft Outlook OST file gets corrupted. » All Messages – recovers all emails regardless of delivery method. Note that this option can create duplicates.
Recover to alternate folder	Leave this option unchecked to recover mail to the appropriate folder within a user's mailbox. To recover data to a designated folder within users' mailboxes, select this option and type a name for the folder. For example, if alternate folder name specified is <code>DisasterRecovery</code> , a new folder named <code>DisasterRecovery</code> is created in each mailbox, and all items are recovered to this folder.
Recover all messages to single mailbox	Choose this option to recover all messages from the activation to a single mailbox. Select the mailbox. For example, recover all items to an administrator mailbox for troubleshooting purposes. A folder for each user being recovered is created in the administrator mailbox.
Users without a primary mailbox	Choose how to process any unmatched mailboxes: <ul style="list-style-type: none"> » Prompt to Manually Match to a Mailbox Whenever a mailbox cannot be matched, RecoveryManager prompts to manually select the correct server and mailbox. » Skip Users: Instructs RecoveryManager to not restore data of unmatched mailboxes.

14. Click **Start Recovery** to begin importing data for selected users. RecoveryManager downloads all mail data from GFI OneConnect data center and imports it to the appropriate mailboxes and mailbox folders.

NOTE

If you click **Cancel** to stop the recovery process, RecoveryManager first completes recovery of the mailbox that is being processed before stopping.

15. Click the link **View Recovery Log** if you want to see a summary of the recovery process.

16. When the mail for all selected users has completed recovery, click **Continue**. If you need to recover additional mail, click **Select another archive to recover** to return to the RecoveryManager main screen. If not, select **Exit RecoveryManager**.

NOTE

Recovery does not import mail in user mailboxes more than once. Even if users or mailboxes belong to more than one group, their data is only imported once. The RecoveryManager skips already recovered user accounts, even if they are members of other distribution lists or groups.

3.2.6 Import Manager

Import Manager is an installable component of GFI OneConnect that the administrator can use to import mail messages from local information stores into the GFI OneConnect data center.

Messages imported into the data center using Import Manager are associated with the specified owner, are subject to retention policies and are searchable through the user's archive.

Import Manager supports the following information stores:

- » PST files
- » EML files
- » Microsoft Exchange mailboxes
- » Microsoft Office 365 mailboxes

Important notes before using Import Manager

- » Ensure that the owner of the imported messages have at least one retention policy applied. Otherwise the message cannot be retained in the data center. For more information, refer to [Working with retention policies](#) (page 67).
- » It is advisable to gather PST and EML files together in a local directory to simplify the import process and improve performance.
- » Emails inside a PST file are associated to the archive of the owner assigned during the import job, regardless of who the sender or recipients are. You need to run multiple import jobs to add the emails to other owners.
- » Import Manager cannot process files that are locked. Ensure that Microsoft Outlook or other email clients are not using PST or EML files that are about to be imported.

Import Manager installation

This topic describes how to install the GFI OneConnect Import Manager on a machine within your network infrastructure.

This same procedure applies to both a fresh installation or an upgrade from a previous version.

IMPORTANT

Import Manager CANNOT be installed on the same server that has the other GFI OneConnect components. Install it on a different machine.

Unlike the other GFI OneConnect components, Import Manager can be installed on a Microsoft Exchange Server.

Important notes before installation

- » Ensure that the GFI Account used is licensed for GFI OneConnect archiving.
- » Log in to the machine using an account with domain administrative privileges.
- » It is advisable to temporarily disable any anti-virus on the machine.
- » During installation you will need to choose an installation mode:

Mode	Description
Complete (recommended)	Install all the components required by Import Manager. This mode requires more disk space but enables you to use all features. Proceed with the installation steps below.
Custom	Install only selected components. This option allows users to choose which program features to install and where to install them. For more information, refer to Custom Installation of Import Manager (page 108).

System Requirement

Install GFI OneConnect Import Manager on a machined that meets or exceeds the following requirements:

Hardware requirements

Component	Minimum Required
Processor	2GHz or better multi-core (x64 processor)
Memory	Minimum: 8 Gb Recommended: 16Gb
Disk Space	Minimum: Two independent hard drives capable of simultaneous read/write. Recommended: RAID 0 or better, NAS or SAN.
Network	Minimum: 100Mb/s full duplex network interface. Recommended: 1GB/s full duplex network interface.

Software requirements

The GFI OneConnect server must use one of the operating systems:

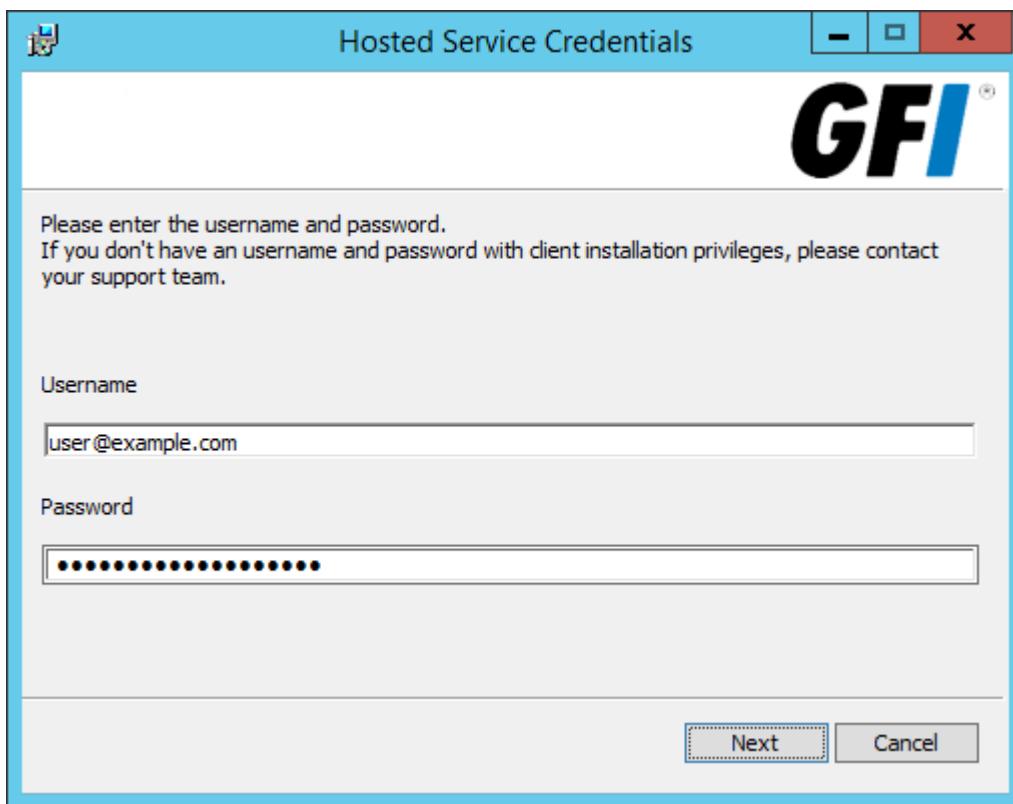
Operating System	Supported editions and notes
Windows Server 2016	Standard or Datacenter
Windows Server 2012 R2	Standard or Datacenter
Windows Server 2012	Standard or Datacenter
Windows Server 2008 R2	Standard or Enterprise

Other required software

Software	Notes
.NET Framework	.NET Framework 4.5
Microsoft Outlook	Microsoft Outlook 2010 or higher is required to Import emails from Microsoft Exchange or Microsoft Office 365 mailboxes unless Import Manager is installed directly on the Microsoft Exchange Server.

Installation procedure

1. Download the installer from the GFI OneConnect administration console. For more information, refer to [Downloads page](#) (page 165).
2. Right-click the GFI OneConnect installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.
3. Launch the installation wizard.



Screenshot 55: Credentials pages on the installation wizard

4. In the **Username** and **Password** fields, enter your [GFI Accounts](#) area credentials or the account used when signing up to GFI OneConnect.
5. Click **Next** in the welcome screen.
6. If you agree with the License Agreement, select **I accept the terms in the License Agreement** and click **Next**.
7. Select the **Complete** installation mode. If you would like to exclude certain components from getting installed, select **Custom**. For more information, refer to [Custom Installation of Import Manager](#) (page 108).
8. The **Fully Qualified Domain Name** and the **Friendly Name** are automatically populated. This information refers to the machine where you are installing Import Manager. Double-check that they are correct and click **Next**.

9. Under services credentials enter the **Domain**, **Username** and **Password** fields with the credentials of a domain admin account to run the service and click **Next**.

10. Click **Install** to start the installation process.

11. Click **Finish**.

Custom Installation of Import Manager

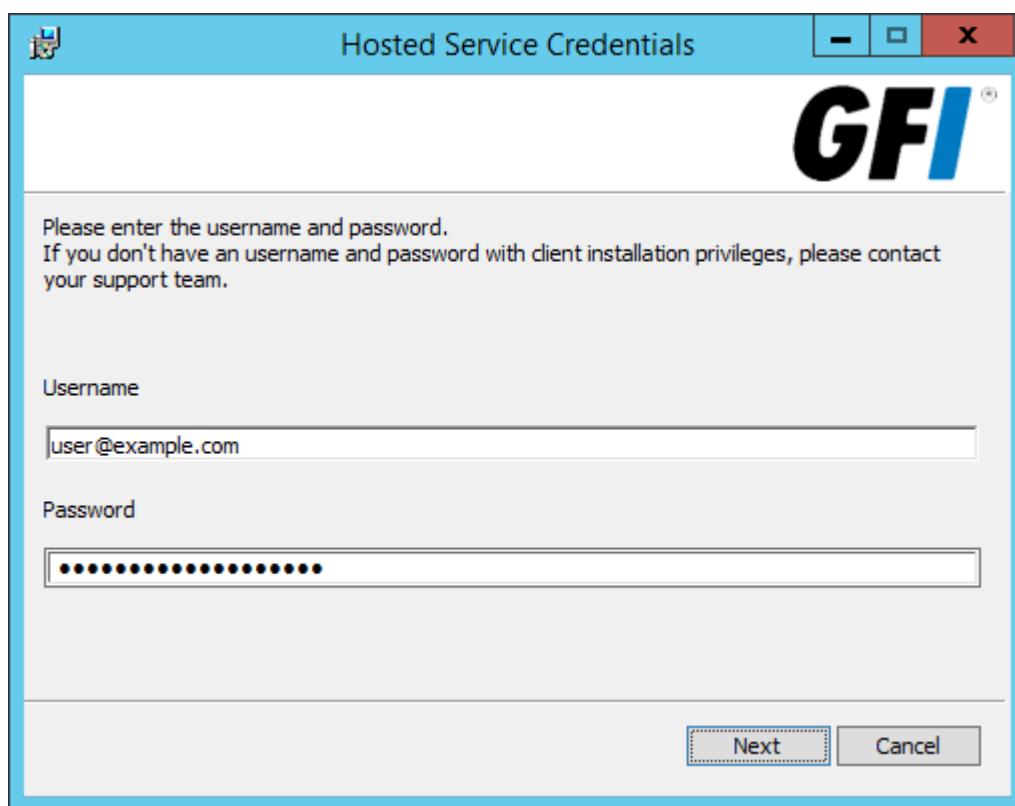
During installation you can select the Custom mode instead of the Complete mode. This option installs only the selected components. Custom mode allows users to choose which program features to install and where to install them. It is recommended for advanced users.

Doing a custom installation also allows you to select a different install directory for Import Manager components. Typically you would only need to do this if you have a large amount of import data and at least one additional physical disk to place the compression directory on for system performance purposes.

1. Download the installer from the GFI OneConnect administration console. For more information, refer to [Downloads page](#) (page 165).

2. Right-click the GFI OneConnect installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.

3. Launch the installation wizard.



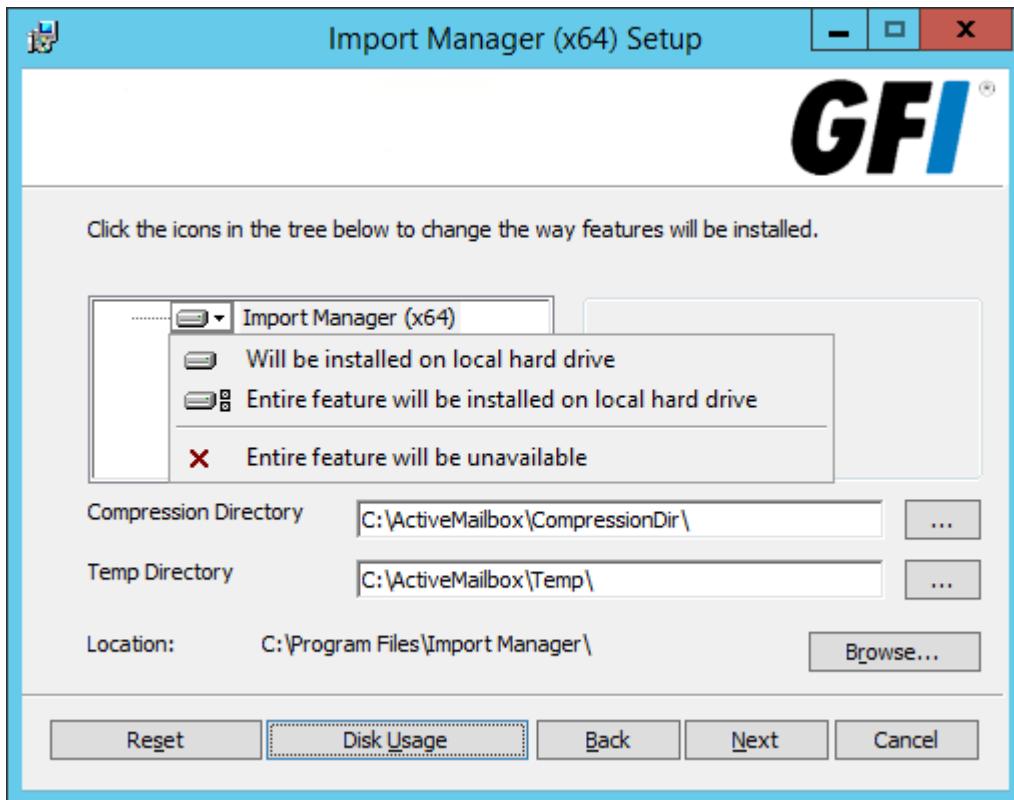
Screenshot 56: Credentials pages on the installation wizard

4. In the **Username** and **Password** fields, enter your [GFI Accounts](#) area credentials or the account used when signing up to GFI OneConnect.

5. Click **Next** in the welcome screen.

6. If you agree with the License Agreement, select **I accept the terms in the License Agreement** and click **Next**.

7. Select the **Custom** installation mode.



Screenshot 57:Custom install options

The following options are available:

Option	Description
Compression Directory	Click ... to change the location of the Compression Directory.
Temp Directory	Click ... to change the location of the Temp Directory.
Location	Click Browse to install Import Manager in a different location.

8. Click **Next**.

9. The **Fully Qualified Domain Name** and the **Friendly Name** are automatically populated. This information refers to the machine where you are installing Import Manager. Double-check that they are correct and click **Next**.

10. Under the services credentials fill the **Domain**, **Username** and **Password** fields with the credentials of a domain admin account to run the service and click **Next**.

11. Click **Install** to start the installation process.

12. Click **Finish**.

Configuring Import Manager

Manage, review and configure import jobs from the GFI OneConnect Import Manager.

Launch Import Manager from **Start > Programs > Import Manager**.

The screenshot shows the GFI OneConnect Import Manager application window. At the top, there's a toolbar with a refresh button, a gear icon for settings, and a question mark icon for help. Below the toolbar is a header titled "Job List". On the left, there's a "New Import" button. The main area contains two sections: "Job List" and "Job Details".

Job List: This section displays a table of completed import jobs. The columns are "Task Name", "Start Time", "End Time", and "Status". Each row has a green checkmark icon in the status column. The table includes the following data:

Task Name	Start Time	End Time	Status
Exchange-12/6/2017-11-24-41...	12/6/2017 11:25 AM	12/6/2017 11:25 AM	Completed
Exchange-11/29/2017-2-31-48...	11/29/2017 2:32 AM	11/29/2017 2:32 AM	Completed
Exchange-11/29/2017-2-31-48...	11/29/2017 2:32 AM	11/29/2017 2:32 AM	Completed
Exchange-11/29/2017-2-30-37...	11/29/2017 2:31 AM	11/29/2017 2:31 AM	Completed
Exchange-11/29/2017-2-30-37...	11/29/2017 2:31 AM	11/29/2017 2:31 AM	Completed
Exchange-11/29/2017-2-29-21...	11/29/2017 2:29 AM	11/29/2017 2:29 AM	Completed
Exchange-11/29/2017-2-29-21...	11/29/2017 2:29 AM	11/29/2017 2:29 AM	Completed
Exchange-11/29/2017-2-27-46...	11/29/2017 2:28 AM	11/29/2017 2:28 AM	Completed

Job Details: This section shows job statistics. It includes tabs for "Statistics", "Task", and "Logs". The "Statistics" tab displays the following data:

```

Num-Total: 5
Num-Processed: 5
Num-Success: 5
Num-Error: 0

```

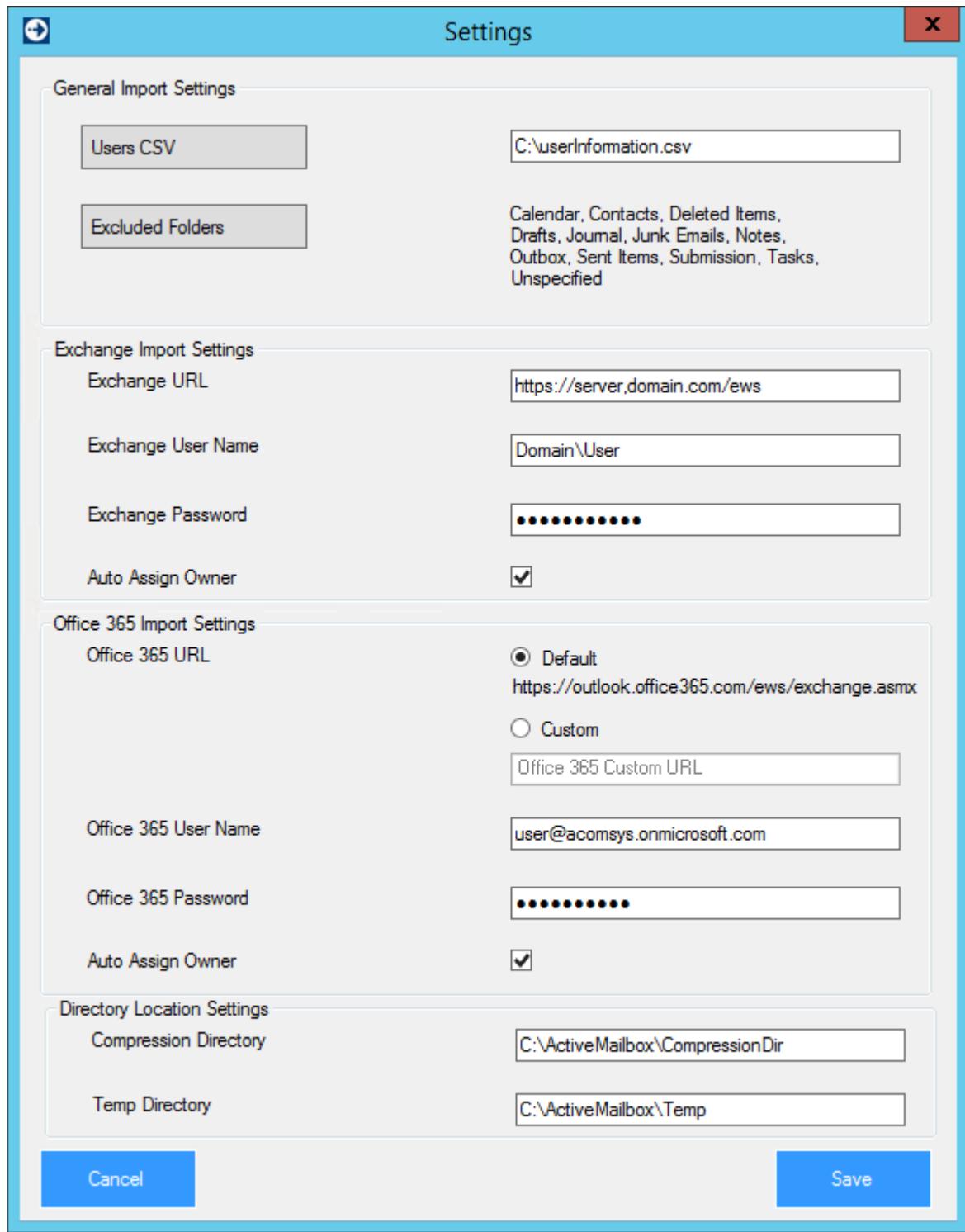
Screenshot 58: Import Manager interface

The Import Manager home screen features two main areas :

- » **Jobs List** - Displays the list of import jobs completed, divided into four tabs according to the job type: **Exchange**, **Office 365**, **PST** and **EML**.
- » **Job Details** - Shows the statistics, task details, and log details of a job.

From the home page it is also possible to configure the general settings of the Import Manager. To edit the Settings click





Screenshot 59: Import Manager settings

These are the options available:

Option	Description
Users CSV	Click to select the CSV file containing the list of GFI OneConnect users. For more information, refer to Import Manager User List (page 112).
Exclude Folders	Define the folders to exclude from being imported. This defines the default exclude behavior. You can further customize the exclusion list while performing a specific job. The exclude is applicable for PST, Exchange and Office 365 imports.

Option	Description
Exchange URL	Configure the connection to your Microsoft Exchange environment when triggering Microsoft Exchange mailbox import jobs.
Exchange User Name/Exchange Password	Microsoft Exchange credential entry fields. Note that it is requested to use an Admin Account with access to all mailboxes.
Auto Assign Owner	Check this option to allow the Import manager to automatically assign owners. When this option is checked GFI OneConnect tries to match the sender or recipient of the emails to a GFI OneConnect user.
Office 365 URL	Configure the connection to Microsoft Office 365 when triggering Office 365 mailbox import jobs. You can either use the default URL or specify a custom URL.
Office 365 User Name	Enter the username of a Microsoft Office 365 account with sufficient permissions to access all mailboxes
Office 365 Pass-word	Enter the password that corresponds to the account above.
Auto Assign Owner	When this option is checked GFI OneConnect automatically assigns an owner to the email matching the Office mailbox 365 owner to a user in GFI OneConnect.
Compression Directory	Default location for the Compression Directory used to store files during the import process. The folder may use a significant amount of disk space. Type in a different path to move the folder to another disk.
Temp Directory	Default location for the Temporary Directory used to store temporary files during the import process. The folder may use a significant amount of disk space. Type in a different path to move the folder to another disk.

Import Manager User List

Messages imported into the data center using Import Manager are:

- » associated with the specified owner.
- » subject to retention policies.
- » searchable through the user's archive.

You can export a list of user from GFI OneConnect main interface and export it to the Import Manager tool, making a list of users available when starting an import job.

Step 1: Export user information from GFI OneConnect

To export the user list from GFI OneConnect:

1. Login to GFI OneConnect configuration page.
2. Go To **Admin Console Home > User Administration > Export**.
3. Click **Export**.

Step 2: Import user information in Import Manager

1. Login to the machine where Import Manager is installed.
2. Save the file downloaded in Step 1 into a directory of your choice.
3. Launch Import Manager from **Start > Programs > Import Manager**.
4. Click the  icon on the home page.

5. Click **Users CSV**. Locate the directory that holds the users list csv file and select it. Click **Open**.

6. Click **Save**.

Importing from a Microsoft Exchange mailbox

GFI OneConnect Import Manager allows administrators to import the entire content of a Microsoft Exchange mailbox to the GFI OneConnect Archive.

Conditions for a successful Exchange import job:

- » The GFI Account for GFI OneConnect needs to be licensed for archiving.
- » A retention policy must exist in GFI OneConnect Retention Policies for each user to whom you need to archive emails. For more information, refer to [Working with retention policies](#) (page 67).
- » Double-check the Import Manager settings before proceeding. For more information, refer to [Configuring Import Manager](#) (page 109).
- » The account that connects to Microsoft Exchange mailbox needs to have sufficient permissions to access the mailboxes included in the job.
- » For large Exchange imports, you may need to increase the values of the field for the Exchange Server Application. For more information refer to <http://support.microsoft.com/kb/830836>

Starting an Exchange import job

To import from a Microsoft Exchange mailbox:

1. Launch the application from **Start > Programs > Import Manager**.

2. In the home page click **New Import**.

3. Select **Exchange Import**.

4. Under **Job Name**, a default name is automatically created using date and time of the job. Change the name as needed. The name is listed under the completed tasks for Exchange imports.

5. Click **Select Owner** to see a list of detected users. Select one owner and click **OK** Alternatively, you can type a full email address in the text box. This option is grayed out if you selected **Auto Assign Owner** option in the settings. For more information, refer to [Configuring Import Manager](#) (page 109).

6. Select the **Range**. The options are:

Range	Description
All	Check this option to import all the emails in the mailbox.
Selected Emails	Select this option to choose a start and end date to limit the import job. Click the calendar icon to select the date. Date format is MM/DD/YYYY.

7. Click **Exclude Folders** to select which folder to exclude from the import. The list of excluded folder is displayed next to it.

8. Click **Select Mailboxes** to select the mailboxes to be imported.

9. Click **Start**.

Imported emails show under the user's archive. Administrators can use the company search to verify that emails were archived properly. To know more about company search access, refer to http://go.gfi.com/?pageid=oneconnect_user_help#cshid=CompanySearch

Importing from a Microsoft Office 365 mailbox

GFI OneConnect Import Manager allows administrators to import the entire content of a Microsoft Office 365 mailbox to the GFI OneConnect Archive.

Conditions for a successful Microsoft Office 365 import job:

- » The GFI Account for GFI OneConnect needs to be licensed for archiving.
- » A retention policy must exist in GFI OneConnect Retention Policies for each user to whom you need to archive emails. For more information, refer to [Working with retention policies](#) (page 67).
- » Double-check the Import Manager settings before proceeding. For more information, refer to [Configuring Import Manager](#) (page 109).
- » The account to connect to Microsoft Office 365 mailbox needs to have the necessary permission to access the mailboxes included in the job.

Starting a Microsoft Office 365 import job

To import from a Microsoft Office 365 mailbox:

1. Launch the application from **Start > Programs > Import Manager**.
2. In the home page click **New Import**.
3. Select **Office 365 Import**.
4. Under **Job Name**, a default name is automatically created using date and time of the job. Change the name as needed. The name is listed under the completed tasks for Microsoft Office 365 imports.
5. Click **Select Owner** to see a list of detected users. Select one owner and click **OK**. Alternatively, you can type a full email address in the text box. This option is grayed out if you selected **Auto Assign Owner** option in the settings. For more information, refer to [Configuring Import Manager](#) (page 109).
6. Select the **Range**. The options are:

Range	Description
All	Check this option to import all the emails in the mailbox.
Selected Emails	Select this option to choose a start and end date to limit the import job. Click the calendar icon to select the date. Date format is MM/DD/YYYY.

7. Click **Exclude Folders** to select which folder to exclude from the import. The list of excluded folder is displayed next to it.
8. Click **Select Mailboxes** to select the mailboxes to be imported.
9. Click **Start**.

Imported emails show under the user's archive. Administrators can use the company search to verify that emails were archived properly. To know more about company search access, refer to http://go.gfi.com/?pageid=oneconnect_user_help#cshid=CompanySearch

Importing from a PST file

GFI OneConnect Import Manager allows administrators to import the entire content of a PST file to the GFI OneConnect Archive.

Conditions for a successful import job:

- » The GFI Account for GFI OneConnect needs to be licensed for archiving.
- » A retention policy must exist in GFI OneConnect Retention Policies for each user to whom you need to archive emails. For more information, refer to [Working with retention policies](#) (page 67).
- » Double-check the Import Manager settings before proceeding. For more information, refer to [Configuring Import Manager](#) (page 109).
- » It is advisable to gather PST files together in a local directory to simplify the import process and improve performance.
- » The user logged on the machine should have full permissions on the directory that holds the PST files.

Starting a PST import job

To import PST files:

1. Launch the application from **Start > Programs > Import Manager**.
2. In the home page click **New Import**.
3. Select **PST Import**.
4. Under **Job Name**, a default name is automatically created using date and time of the job. Change the name as needed. The name is listed under the completed task for PST imports.
5. Click **Select Owner** to see a list of detected users. Select one owner and click **OK**. Alternatively, you can type a full email address in the text box.
6. Select the **Range**. The options are:

Range	Description
All	Check this option to import all the emails in the file.
Selected Emails	Select this option to choose a start and end date to limit the import job. Click the calendar icon to select the date. Date format is MM/DD/YYYY.

7. Click **Choose PST**. Navigate to the directory that holds the files, select one or more files and click **Open**.
8. Click **Exclude Folders** to select which folder to exclude from the import. The list of excluded folder is displayed next to it.
9. Click **Start**.

Imported emails show under the user's archive. Administrators can use the company search to verify that emails were archived properly. To know more about company search access, refer to http://go.gfi.com/?pageid=oneconnect_user_help#cshid=CompanySearch

Importing from an EML file

GFI OneConnect Import Manager allows administrators to import EML files to the GFI OneConnect Archive.

Conditions for a successful EML import job:

- » The GFI Account for GFI OneConnect needs to be licensed for archiving.
- » A retention policy must exist in GFI OneConnect Retention Policies for each user to whom you need to archive emails. For more information, refer to [Working with retention policies](#) (page 67).

- » Double-check the Import Manager settings before proceeding. For more information, refer to [Configuring Import Manager](#) (page 109).
- » It is advisable to gather EML files together in a local directory to simplify the import process and improve performance.
- » The logged on user should have full permissions on the directory that holds the EML files.

Starting an EML import job

To import EML files:

1. Launch the application from **Start > Programs > Import Manager**.
2. In the home page click **New Import**.
3. Select **EML Import**.
4. Under **Job Name**, a default name is automatically created using date and time of the job. Change the name as needed. The name is listed under the completed tasks for EML imports.
5. Click **Select Owner** to see a list of detected users. Select one owner and click **OK**. Alternatively, you can type a full email address in the text box.
6. Select the **Range**. The options are:

Range	Description
All	Check this option to import all emails.
Selected Emails	Select this option to choose a start and end date to limit the import job. Click the calendar icon to select the date. Date format is MM/DD/YYYY.

7. Click **Choose Source**. Navigate to the directory that holds the files, select one or more files and click **Open**.

8. Click **Start**.

Imported emails show under the user's archive. Administrators can use the company search to verify that emails were archived properly. To know more about company search access, refer to http://go.gfi.com/?pageid=oneconnect_user_help#cshid=CompanySearch

3.2.7 Retention Policy Storage Report

The Storage Report provides a high-level overview report for data retained by each retention policy.

Notes to consider about Storage reports:

- » All storage reports are updated daily, so statistics may not take into account changes made since the last calculations.
- » Since a message or attachment can be subject to multiple retention policies, there may be a discrepancy between the Storage Usage Data total of all the policy data and the aggregate storage data. In these situations, the **Aggregate Statistics** entry reflects the correct value.
- » The default policy causes a number of additional messages that are not held for an explicit policy to be visible in the totals. This occurs when users are deleted or removed from a membership-based policy.

To view storage reports:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Archiving**.
3. Navigate to **Storage Report**.

GFI OneConnect™

Home Manage Settings ?

Admin Console Home Historical Mail Retention Policies Storage Report Reviewer Groups Email Recovery On-Premises Journaling User Administration Cloud Services Mobile App Administration Outlook Extension Mailing Lists Notification Audit Reports System Settings	<h3>Storage Report</h3> <p>Report of all messages stored by OneConnect policies. Note: Multiple policies can apply to a message, so a message may be counted in the totals for several different policies.</p> <p>The total storage calculated across all Retention and Storage Management will count each message only once.</p> <h4>Policy Types</h4> <p>Membership (Membership-Based Policy): Retention rules apply to users currently in the policy.</p> <p>Capture (Capture-Based Policy): Retention rules apply to messages to or from users in the policy at the time the message was captured.</p> <p>Retention Hold (Query-Based Retention Hold): An Archive Reviewer identifies specific messages (found by a query) to be retained indefinitely.</p> <p>User Classification (User Classification Policy): Allows designated users to determine which messages are retained under the policy.</p> <p>Instant Message (Instant Message-Based Policy): Retention rules apply to instant messages as per customer specification.</p> <h4>Retention Policy Statistics</h4> <table border="1"> <thead> <tr> <th>#</th> <th>Type</th> <th>Policy Name</th> <th>Retention</th> <th>Statistics</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>User Classification</td> <td>Manual 1camaro</td> <td>3650 days</td> <td>Users: 0 Messages: 0 Total size: 0 bytes</td> </tr> <tr> <td>2</td> <td>Instant Message</td> <td>Global IM Capture Policy</td> <td>3650 days</td> <td>Users: 0 Messages: 0 Total size: 0 bytes</td> </tr> <tr> <td>3</td> <td>Membership</td> <td>HR</td> <td>365 days</td> <td>Users: 25 Messages: 2456 Total size: 43.6 Mb</td> </tr> <tr> <td>4</td> <td>Membership</td> <td>Accounts</td> <td>365 days</td> <td>Users: 32 Messages: 4321 Total size: 65.7</td> </tr> <tr> <td>5</td> <td></td> <td>Default Retention Policy</td> <td>1825 days</td> <td>Users: 0 Messages: 0 Total size: 0 bytes</td> </tr> </tbody> </table> <h4>Aggregate Statistics</h4> <table border="1"> <thead> <tr> <th>Statistics</th> </tr> </thead> <tbody> <tr> <td>Users: 57 Messages: 6777 Total size: 109.3 MB</td> </tr> </tbody> </table>	#	Type	Policy Name	Retention	Statistics	1	User Classification	Manual 1camaro	3650 days	Users: 0 Messages: 0 Total size: 0 bytes	2	Instant Message	Global IM Capture Policy	3650 days	Users: 0 Messages: 0 Total size: 0 bytes	3	Membership	HR	365 days	Users: 25 Messages: 2456 Total size: 43.6 Mb	4	Membership	Accounts	365 days	Users: 32 Messages: 4321 Total size: 65.7	5		Default Retention Policy	1825 days	Users: 0 Messages: 0 Total size: 0 bytes	Statistics	Users: 57 Messages: 6777 Total size: 109.3 MB
#	Type	Policy Name	Retention	Statistics																													
1	User Classification	Manual 1camaro	3650 days	Users: 0 Messages: 0 Total size: 0 bytes																													
2	Instant Message	Global IM Capture Policy	3650 days	Users: 0 Messages: 0 Total size: 0 bytes																													
3	Membership	HR	365 days	Users: 25 Messages: 2456 Total size: 43.6 Mb																													
4	Membership	Accounts	365 days	Users: 32 Messages: 4321 Total size: 65.7																													
5		Default Retention Policy	1825 days	Users: 0 Messages: 0 Total size: 0 bytes																													
Statistics																																	
Users: 57 Messages: 6777 Total size: 109.3 MB																																	

Screenshot 60: Storage Report overview

The **Retention Policy Statistics** report lists each retention policy in priority order, along with the policy's type, name, duration, number of users and messages affected by the policy, and the total storage size of each policy.

Column title	Description
#	Priority of the retention policy. The higher priority (smaller number) policy controls the retention duration of messages included in multiple retention policies.
Type	Category of retention policy. <ul style="list-style-type: none"> » Capture: A Capture Based Policy where retention rules apply to messages to or from users in the policy at the time the message was captured. » Membership: A Membership Based Policy where retention rules apply to users currently in the policy. » Retention Hold: A Query-Based Retention Hold where a GFI OneConnect Reviewer uses a query to identifies specific messages to be retained indefinitely.
Policy Name	The name of the retention policy.
Retention	The length of days to keep a message governed by the policy.
Statistics (Daily Snapshot)	The number of: <ul style="list-style-type: none"> » Users » Messages » Total size <p>Note that these totals reflect only the current state. No historical information is maintained.</p>

The **Aggregate Statistics Report** area shows the total number of users and messages, and total amount of storage consumed for all policies.



Screenshot 61: Aggregate Statistics Report

Field	Description
Users	Total number of users affected by all policies, with each user counted only once. This count includes only current policy membership. No historical information is maintained as users are added to or removed from policies.
Messages	Total number of messages stored by all policies, with each message counted only once.
Total size	Total amount of storage space consumed by the messages stored under all policies.

3.3 GFI OneConnect Security

The GFI OneConnect Security service protects your inbound email from viruses, filters out spam and provides mail monitoring features.

This section guides you through the process of configuring the Security service of GFI OneConnect.

To access the Security configuration console, [log in](#) to GFI OneConnect using an Administrator account. Navigate to **Manage > Security**. Key in your Administrator credentials in the Security login screen.

When login is completed, the service provides three roles. Choose the role depending on the feature to configure or monitor:

Role	Description
User	Options related to your user's mailbox: <ul style="list-style-type: none">» Configure your user's personal Blacklist & Whitelist» Manage the list of quarantined emails sent to your address.» Personal quarantine report settings
Domain Administrator	Manage your organization's security service options: <ul style="list-style-type: none">» Configure Blacklist & Whitelist entries for the organization» Manage organization's quarantine» Generate mail usage reports at organization-level
Domain Group Administrator	Manage your organization's security service options: <ul style="list-style-type: none">» Configure mail filtering options for protected domains» Configure Blacklist & Whitelist entries for the organization» Custom mail filtering policies for individual users» Manage organization's quarantine» Generate mail usage reports at organization-level

To switch the role, click the **Role** field in the top right corner and select the new role.

Logged In: [Joe.Doe@mydomain.com](#) | [Dashboard](#) | [Logout](#)
Role: Domain Group Administrator | Domain Group: [GFI-P-852](#)
Version: 6.13 | License: STE-3-0000-151736

Screenshot 62: The top-right corner section where to change role and domain

Topics in this section:

3.3.1 Security Dashboard	119
3.3.2 Domain Policies	120
3.3.3 User Policies	124
3.3.4 Domain Whitelist & Blacklist	127
3.3.5 Quarantine	128
3.3.6 Security Reports	130

3.3.1 Security Dashboard

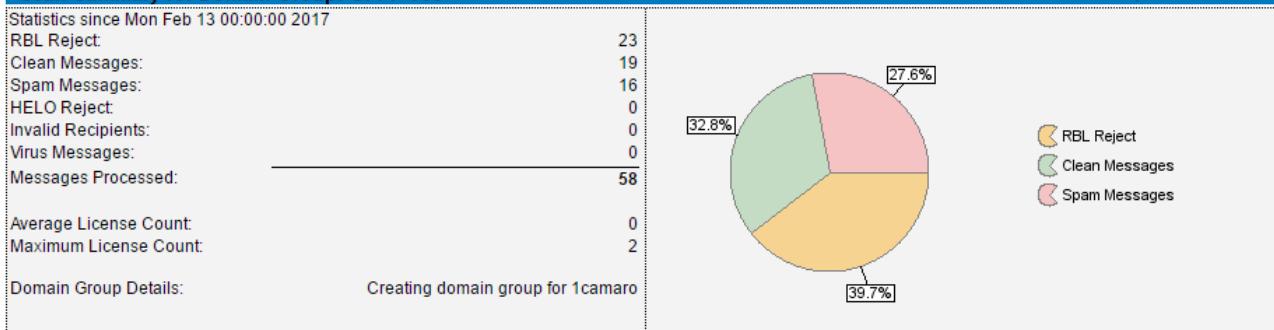
The Security Dashboard provides a summary and statistics of the service status.

To access the Security Dashboard:

1. [Login](#) to GFI OneConnect using an Administrator account and navigate to **Manage > Security**.
2. Key in your Administrator account credentials in the Security login screen.
3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.
4. Click **Dashboard** from the top-right corner.

Scan Summary for Domain Group: GFI-P-935

14:33:31 Thu, Mar 02 2017



Last 7 Days

[Table](#) [Chart](#)

Date	Total	Spam	Clean	Invalid rcpts	Viruses	RBL Hits	HeLo Reject	License Count
2017-03-01	1	0	0	0	0	1	0	0
2017-02-28	2	0	0	0	0	2	0	0
2017-02-27	2	0	0	0	0	2	0	0
2017-02-26	2	1	0	0	0	1	0	0
2017-02-25	2	0	0	0	0	2	0	0
2017-02-24	3	2	0	0	0	1	0	0

©2006-2016 Copperfasten Technologies

Screenshot 63: The Security Dashboard

The **Scan Summary** section shows various metrics related to processed and blocked emails.

The **Last 7 days** section shows trends and counts of blocked emails during the previous seven days. Choose tab:

- » **Table:** Counts of emails processed and blocked per day.
- » **Chart:** A line chart of emails processed and blocked during the last seven days.

3.3.2 Domain Policies

Use the Security Domains Policy settings to apply anti-virus, anti-spam, and other filtering mechanisms on emails processed on a per-domain basis.

The screenshot shows the 'Domain Policy Management' page. At the top, there are tabs for 'Anti-Spam Engine', 'Quarantine', and 'Reporting'. Below that, a sub-menu has 'Domain Policies' and 'User Policies' options. The main area is titled 'Domain Policy Management' with a search bar for 'Filter Domain'. It displays two rows of policy settings for 'mydomain1.com' and 'mydomain2.com'. The columns are: Policy (checkbox), Spam, Virus, Banned, Digest, Archive, and Options (with edit icons). Both domains have 'On [5:Quarantine]' selected across all categories. An 'Edit...' button is located at the bottom right.

Policy	Spam	Virus	Banned	Digest	Archive	Options
mydomain1.com	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Off	Off	
mydomain2.com	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Daily	Off	

Screenshot 64: Domain Policies page

To access the Domain Policies screen:

1. [Login](#) to GFI OneConnect using an Administrator account and navigate to **Manage > Security**.
2. Key in your Administrator account credentials in the Security login screen.
3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.
4. Navigate to **Anti-Spam Engine > Domains Policies**.
5. Choose a domain and click the icon to configure the domain's filtering options. These domain settings are inherited by all users in those domains.

Edit Domain Policy: mydomain1.com

Spam Filtering: **ON** [Disable](#)

Consider mail spam when score is greater than:

Spam should be: [Quarantined](#)

Discard Spam scoring above:

Add X-Spam headers to non-spam mails: **ON** [Disable](#)

Virus Filtering: **ON** [Disable](#)

Viruses should be: [Quarantined](#)

Attachment Type Filtering: **ON** [Disable](#)

Banned Attachments should be: [Quarantined](#)

Archive Clean Email: **OFF** [Enable](#)

Quarantine Report: **OFF** [Enable](#)

Reset settings to default: [Reset](#)

[Apply](#) [Cancel](#)

Screenshot 65: Edit Domain Policy dialog

Configure the following options:

Option	Description	Default value
Spam Filtering	Specifies whether spam filtering is enabled for the selected domain. Toggle Enable / Disable to switch this option on or off.	ON
Consider mail spam when score is greater than	When scanning messages for spam, GFI OneConnect Security applies various checks to determine an overall spam score for each message. Emails scoring above this threshold are considered as spam. Emails scoring below the threshold will be considered legitimate and passed onto the recipient(s) If you find this setting too aggressive or not aggressive enough, then you can change the threshold.	5

Option	Description	Default value
Spam should be	Action to perform when a message is classified as spam: <ul style="list-style-type: none"> » Quarantined: The message is moved to the GFI OneConnect Security Quarantine. It appears in the recipient's Quarantine Report and may be later released from the quarantine if it is deemed by the user to be a false positive. » Passed (Tagged): Spam emails will be passed onto the end recipients, but headers are added to the message so that it will be possible to filter messages on the backend mail server and/or on the end-recipients mail client. » Rejected: The message will be rejected. The message are dropped before they are received by the mail server. Those messages cannot be recovered. 	Quarantined
Discard Spam scoring above	Messages scoring above the specified score will be automatically discarded. This option is only available when the action is set to Quarantined .	999 (no messages will be discarded)
Spam Modifies Subject	Enable this option to prepend text to the Subject header, indicating that the message has been identified as spam. Specify an appropriate Spam Subject Tag to be added to the subject. This option is only available when the action is set to Passed (Tagged) .	OFF
Add X-Spam headers to non-spam mails	Specifies if additional headers are added to inbound messages, indicating the result of the spam analysis. The headers added are: <ul style="list-style-type: none"> » X-Spam-Status: This will show if the message exceeded the spam threshold and the score that it achieved. It will also list what rules were fired by the anti-spam engine. » X-Spam-Score: Lists the spam score achieved. <p>Toggle Enable / Disable to switch this option on or off.</p>	ON
Virus Filtering	Specifies whether virus filtering is enabled for the selected domain. Toggle Enable / Disable to switch this option on or off.	ON
Viruses should be	The action to perform when a message is identified as containing a virus. Refer to the actions documented in the anti-spam section above.	Quarantined
Attachment Type Filtering	Specifies whether the default GFI OneConnect message attachment policy is applied to messages received by recipients in the selected domain. Toggle Enable / Disable to switch this option on or off. The blocked attachment types are: .vbs, .scr, .pif, .js, .flv, .exe, .dll, .com, .cmd, and .bat.	ON
Banned Attachments should be	The action to perform when a message is blocked by Attachment Type Filtering: <ul style="list-style-type: none"> » Quarantined: The message is moved to the GFI OneConnect Security Quarantine. It appears in the recipient's Quarantine Report and may be later released from the quarantine if it is deemed by the user to be a false positive. » Passed (Tagged): Spam emails will be passed onto the end recipients, but headers are added to the message so that it will be possible to filter messages on the backend mail server and/or on the end-recipients mail client. » Rejected: The message will be rejected. The message are dropped before they are received by the mail server. Those messages cannot be recovered. 	Quarantined
Archive Clean Email	Enable this setting to store all clean messages received by this domain in the history. (Go to Reporting > History to view clean emails.) Toggle Enable / Disable to switch this option on or off.	OFF
Quarantine Report	This field specifies whether quarantine reports should be generated for recipients in this domain. A quarantine report will be generated for each recipient who has at least one email quarantined. Toggle Enable / Disable to switch this option on or off.	OFF

Option	Description	Default value
Language	If enabling quarantine reports, select the default report language. Recipients may change the language of their report by logging into GFI OneConnect Security and changing their preferences.	English
Email report every	If enabling quarantine reports, select the frequency of the reports. Reports may be generated every day, every weekday (Monday to Friday), every Friday, or every month. Recipients may change the frequency of their reports by logging into GFI OneConnect Security and changing their preferences.	Day
Report contains	If enabling quarantine reports, choose the items to show in the report. Recipients may change this option of their report by logging into GFI OneConnect Security and changing their preferences. The report may include: <ul style="list-style-type: none">» All quarantined items» New items since last report only» All quarantined msgs (except viruses)» New items since last report (except viruses)	New items since last report only
Exclude spam mails scoring above	Usually, users are only interested in messages that fall just above the spam threshold to look for false positives. Spam messages scoring above a certain threshold can be unequivocally deemed as spam. If users get a significant amount of spam, then to keep the report size manageable you can exclude spam messages above, for example 30. This setting is set to 999 by default, meaning that no messages will be excluded (as a message cannot score that high).	999 (no messages will be excluded)
Reset settings to default	Reset the policy to default values.	

6. Click **Apply** to save settings.

3.3.3 User Policies

By default, each recipient email address inherits the policy as set for that [domain](#). GFI OneConnect Security enables administrators to apply custom email filtering policies to individual users, that override the domain policies. User policies have a higher priority than domain policies. When an email is received for a user who does not have a user policy, then GFI OneConnect uses the domain policy. If a user policy associated with the email address exists, then GFI OneConnect uses the user policy.

GFI OneConnect also enables end-users to customize their quarantine report preferences. The User policies screen shows these customizations, enabling administrators to track the changes applied.

User policies are created when:

- » A user logs into the GFI OneConnect Security UI the first time.
- » A user whitelists a sender from their quarantine report.
- » An *existing* user (who has already sent or received email) requests their password using the **Forgot Password** link on the GFI OneConnect Security login page.
- » An administrator manually creates a user policy rule as documented below.

Anti-Spam Engine Quarantine Reporting

Domain Policies User Policies

User Policy Management

Page: 1 Entries per page: 15 Email: Filter Email Domain: Filter Domain Showing 1 - 4 of 4 users

Email Account	User Role	Spam	Virus	Banned	Digest	Locked	Archive	Actions
ian@mydomain.com	User	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Off		Off	
jane@mydomain.com	User	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Weekly		Off	
john@mydomain.com	User	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Monthly		Off	
tom@mydomain.com	User	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Daily		Off	

Edit... Delete Add...

Screenshot 66: User Policies page

To access the User Policies screen:

1. [Login](#) to GFI OneConnect using an Administrator account and navigate to **Manage > Security**.
2. Key in your Administrator account credentials in the Security login screen.
3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.
4. Navigate to **Anti-Spam Engine > User Policies**.
5. To create new user policies click **Add...**. To edit an existing user policy, click the icon in the options column.
6. Configure the following options:

Option	Description
Email Addresses	Specify one or more email addresses to create user policies for. Specify multiple email addresses in separate lines.
User Role	Choose User .
Spam Filtering	Specifies whether spam filtering is enabled for the selected user. Toggle Enable / Disable to switch this option on or off.
Consider mail spam when score is greater than	This is the anti-spam engine scoring threshold above which mail is considered to be spam.
Spam should be	Action to perform when a message is classified as spam: <ul style="list-style-type: none"> » Quarantined: The message is moved to the GFI OneConnect Security Quarantine. It appears in the recipient's Quarantine Report and may be later released from the quarantine if it is deemed by the user to be a false positive. » Passed (Tagged): Spam emails will be passed onto the end recipients, but headers are added to the message so that it will be possible to filter messages on the backend mail server and/or on the end-recipients mail client. » Rejected: The message will be rejected. The message are dropped before they are received by the mail server. Those messages cannot be recovered.
Discard Spam scoring above	Messages scoring above the specified score will be automatically discarded. This option is only available when the action is set to Quarantined .

Option	Description
Spam Modifies Subject	Enable this option to prepend text to the Subject header, indicating that the message has been identified as spam. Specify an appropriate Spam Subject Tag to be added to the subject. This option is only available when the action is set to Passed (Tagged) .
Add X-Spam headers to non-spam mails	Specifies if additional headers are added to inbound messages, indicating the result of the spam analysis. The headers added are: <ul style="list-style-type: none"> » X-Spam-Status: This will show if the message exceeded the spam threshold and the score that it achieved. It will also list what rules were fired by the anti-spam engine. » X-Spam-Score: Lists the spam score achieved. <p>Toggle Enable / Disable to switch this option on or off.</p>
Virus Filtering	Specifies whether virus filtering is enabled for the selected domain. Toggle Enable / Disable to switch this option on or off.
Viruses should be	The action to perform when a message is identified as containing a virus. Refer to the actions documented in the anti-spam section above.
Attachment Type Filtering	Specifies whether the default GFI OneConnect message attachment policy is applied to messages received by this recipient. Toggle Enable / Disable to switch this option on or off. The default file types blocked are .bat, .cmd, .com, .dll, .exe, .flv, .js, .piv, .scr and .vbs.
Banned Attachments should be	The action to perform when a message is blocked by Attachment Type Filtering. The options are: <ul style="list-style-type: none"> » Quarantined: The message is moved to the GFI OneConnect Security Quarantine. It appears in the recipient's Quarantine Report and may be later released from the quarantine if it is deemed by the user to be a false positive. » Passed (Tagged): Spam emails will be passed onto the end recipients, but headers are added to the message so that it will be possible to filter messages on the backend mail server and/or on the end-recipients mail client. » Rejected: The message will be rejected. The message are dropped before they are received by the mail server. Those messages cannot be recovered.
Archive Clean Email	Enable this setting to store all clean messages received by this domain in the history. (Go to Reporting > History to view clean emails.) Toggle Enable / Disable to switch this option on or off.
Lock Policy	When enabled, any changes applied to the parent domain policy will not affect the user policy. For example, if the domain policy for example.com changes the spam score to 1, any user policy under example.com will also see that change appears on their policy unless it has been locked.
Quarantine Report	This field specifies whether quarantine reports should be generated for recipients in this domain. A quarantine report will be generated for each recipient who has at least one email quarantined. Toggle Enable / Disable to switch this option on or off.
Language	If enabling quarantine reports, select the default report language.
Email report every	If enabling quarantine reports, select the frequency of the reports. Reports may be generated every day, every weekday (Monday to Friday), every Friday, or every month.
Report contains	If enabling quarantine reports, choose the items to show in the report. The report may include: <ul style="list-style-type: none"> » All quarantined items » New items since last report only » All quarantined msgs (except viruses) » New items since last report (except viruses)
Exclude spam mails scoring above	If enabling quarantine reports, users are usually only interested in messages that fall just above the spam threshold to look for false positives. Spam messages scoring above a certain threshold can be unequivocally deemed as spam. If users get a significant amount of spam, then to keep the report size manageable you can exclude spam messages above, for example 30. This setting is set to 999 by default, meaning that no messages will be excluded (as a message cannot score that high).

7. Click **Add** to save settings.

To impersonate a user, click on the  icon in the options column. This automatically log you into that user interface with the same permissions as they would have.

3.3.4 Domain Whitelist & Blacklist

The Whitelist contains a list of sender email addresses and domains. Emails received from whitelisted addresses, are always classified as not spam, even if the message is detected as spam. Note however that GFI OneConnect Security still scans emails received from whitelisted senders for viruses and malware.

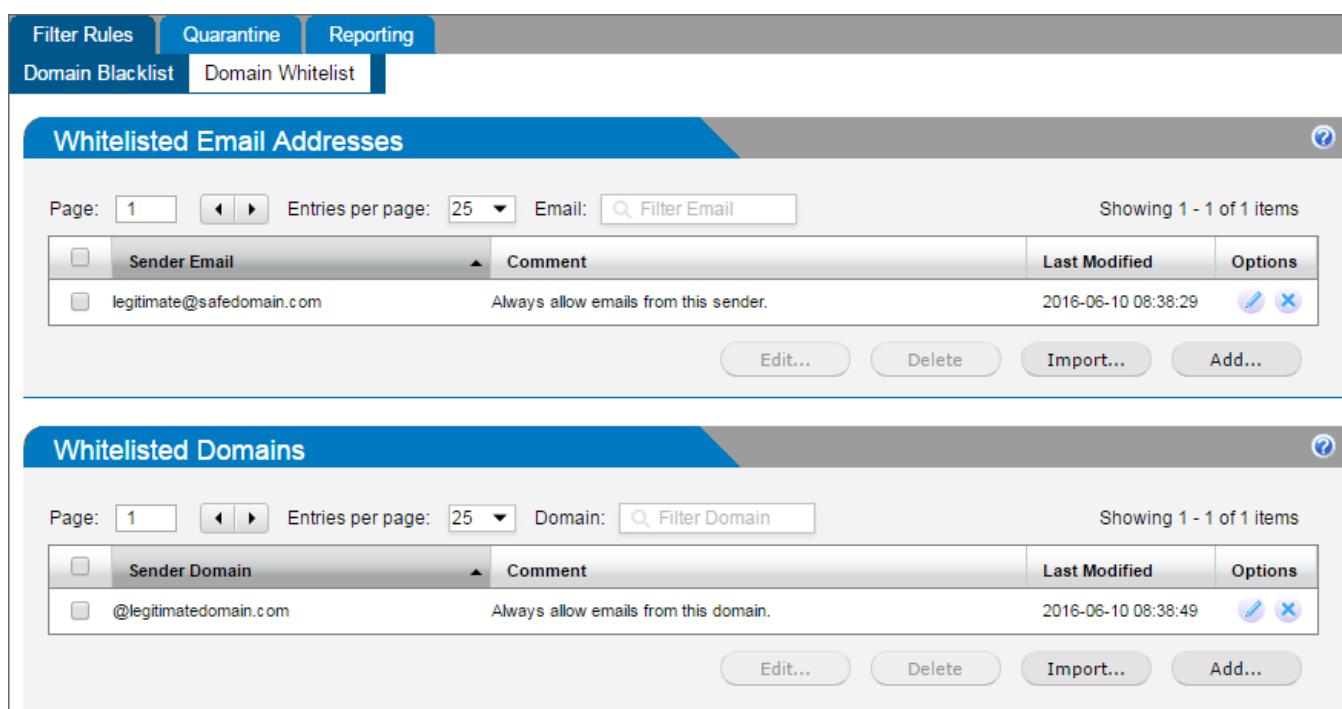
On the contrary, emails received from email addresses or domains added to the Blacklist are always blocked and classified as spam, even if the message is not detected as spam by the scanning engine. Add to the Blacklist the senders from which you never want to receive emails.

Blacklist & Whitelist can be configured at domain level or at user level. GFI OneConnect Security administrators can manage domain lists, applicable to emails received by the organization. End-users can manage their own lists for emails received by them only.

This topic describes how to configure domain-level Whitelist & Blacklist. For information on how end-users can manage User Blacklist/Whitelist, refer to http://go.gfi.com/?pageid=oneconnect_user_help#cshid=userfilterrules.

To access the Domain Whitelist & Blacklist filter rules:

1. Login to GFI OneConnect using an Administrator account and navigate to **Manage > Security**.
2. Key in your Administrator account credentials in the Security login screen.
3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.
4. Navigate to the **Filter Rules** tab.
5. Select the list to access: **Domain Whitelist** or **Domain Blacklist**.



Whitelisted Email Addresses

Sender Email	Comment	Last Modified	Options
legitimate@safedomain.com	Always allow emails from this sender.	2016-06-10 08:38:29	 

Whitelisted Domains

Sender Domain	Comment	Last Modified	Options
@legitimatedomain.com	Always allow emails from this domain.	2016-06-10 08:38:49	 

Screenshot 67: The Domain Whitelist screen

Adding entries manually

1. Click **Add** in the **Email Addresses** or **Domain sections**.
2. Key in the domain or email address to add:
 - Email Address must be entered in the form *user@example.com*.
 - Domain entries must be in the form *example.com*.

3. (Optional) Add a comment. It may be helpful to remember why the item was added on that list.
4. Click **Save**.

Importing a list

1. Create a text file containing all the entries to whitelist or blacklist. Write one entry per line:

- Email addresses must be in the form *user@example.com*.
- Domain entries must be in the form *@example.com*.
- The text file may contain a mixed list of both email addresses and domains.

2. Click **Import...** in the **Email Addresses** or **Domain** sections.

3. Select the file to be imported and click **Open**.

Editing entries

1. Select the entry to modify and click **Edit...**.
2. Make the changes and click **Save**.

Deleting entries

1. Access the list you want to edit.
2. Select the entry and click **Delete**.

NOTES

- » A sender may not be added to both the Whitelist and the Blacklist at the same time.
- » Whitelist and Blacklist entries specified by end-users at User level, overrule the domain level settings.

3.3.5 Quarantine

The GFI OneConnect Security Quarantine provides a central store where all emails detected as spam or malware are retained. This ensures that users do not receive unwanted messages in their mailbox and processing on the mail server is reduced.

Administrators and end-users can review quarantined emails by accessing the quarantine interface from a web browser. GFI OneConnect Security can also send regular quarantine email reports to end-users to review their blocked emails.

This chapter describes the quarantine management system, and how the administrator manages the organization's quarantined messages. End-users can also review their personal quarantine. For more information refer to http://go.gfi.com/?pageid=oneconnect_user_help#cshid=userquarantine

Note that emails get quarantined only when GFI OneConnect Security is configured to quarantine blocked emails. The action taken can be customized by the Administrator from the **Domain Policies** and from **User Policies**.

Using the quarantine

The Quarantine is accessible by logging in to GFI OneConnect. From the Quarantine, administrators can review blocked emails and apply various actions, for example, release a false positive, whitelist the sender or permanently delete emails.

To access the organization's Quarantine:

1. Login to GFI OneConnect using an Administrator account and navigate to **Manage > Security**.
2. Key in your Administrator account credentials in the Security login screen.
3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.
4. Go to **Quarantine > Manage Quarantine**.

The screenshot shows the 'Manage Quarantine' page. At the top, there are tabs for Anti-Spam Engine, Filter Rules, Quarantine (which is selected), and Reporting. Below the tabs is a 'Manage Quarantine' link. The main area is titled 'Search Quarantine' with sections for 'SEARCH FILTERS' and 'DISPLAY SETTINGS'. A date range is set to 'Yesterday'. The table lists one item: a message from 'spammer@spam.com' to 'info@example.com' with subject 'Legal Support to obtain European Citizenship.' and score '17.375'. Action buttons for Release, Whitelist, and Delete are shown for this message. A note at the bottom says 'Showing 1 - 1 of about 1 items'.

Screenshot 68: Manage Quarantine page

The **Manage Quarantine** page shows the emails in quarantine.

Use the **Search Filters** tab to filter through the list of quarantined emails on a number of different criteria including message type, email address, score, subject and message flow direction.

The following actions may be performed on messages in the Quarantine:

Action	Description
View Message	To safely view a message that is in the quarantine click the From, To, or Subject of a particular quarantined message from the list. This opens the message in a separate window. Note that images are blocked from this preview to prevent possible inappropriate content. If a message is subsequently released and delivered, then the original images will be present.
Release Message	Messages in the quarantine that are misidentified as spam (False positives) can be released for delivery to their intended recipients. Click Release to perform this action.
Delete Message	Users can choose to permanently delete messages one at a time, or in bulk by checking the check boxes of messages to delete. Note that if a message is deleted from the quarantine then that message will not appear in the quarantine report.
NOTE Deleted messages are permanently purged and are not recoverable.	
Whitelist Sender	Adds the sender of the selected message(s) to the whitelist so that all future emails from this sender bypass the GFI OneConnect Security anti-spam engine. Selecting this option will also automatically release the message from the quarantine. Note that the sender email address that is added to the Whitelist is the envelope email address. This is sometimes different from the address that appears in the From header of the message. Check Reporting > History to see the envelope sender email address.

NOTE

Quarantined items are automatically deleted from the quarantine store after 21 days. Deleted items are not recoverable.

Enabling Quarantine reports for the users

Administrators can enable quarantine reports to be sent to users on a daily basis. A quarantine report is generated for each recipient who has at least one email quarantined.

The report contains a list of items in quarantine and a link for the users to access their personal quarantine.

To enable quarantine reports for the users:

1. [Login](#) to GFI OneConnect using an Administrator account and navigate to **Manage > Security**.
2. Key in your Administrator account credentials in the Security login screen.
3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.
4. Navigate to **Anti-Spam Engine > Domains Policies**.
5. Choose a domain and click the  icon to configure the domain's filtering options.
6. On the **Quarantine Report** option click **Enable**.

3.3.6 Security Reports

GFI OneConnect Security enables administrators and end-users to create reports based on emails processed and blocked by the service.

The GFI OneConnect Administrator can access and generate reports for the whole organization or specific domains. End-users can generate reports for emails addressed to them.

To access the GFI OneConnect Security Reports:

1. [Login](#) to GFI OneConnect using an Administrator account and navigate to **Manage > Security**.
2. Key in your Administrator account credentials in the Security login screen.
3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.
4. Go to the **Reporting** tab and choose the required action:
 - » [Review mail transactions \(history\)](#)
 - » [Generate a report](#)
 - » [Scheduled reports](#)
 - » [Archived reports](#)

Activity Log & History

The **Reporting > History** page enables you to monitor all processed emails and review all mail transactions that have passed through GFI OneConnect Security.

Screenshot 69: History page

The Mail History table

The **Mail History** table shows a row for each processed email and its attributes.

By default, the table does not show all the columns documented here. Use the **Display Settings** tab to add more columns as required. For more information, refer to [Display Settings](#) (page 133).

The **Export to CSV** link allows you to download all transactions for the given search criteria to a Microsoft Excel spreadsheet.

Click the **Refresh** link to refresh the history view. Since the entire history is not shown on one page, use the links at the bottom of the page to jump to other pages.

The following table describes each of the columns that are displayed in the Mail History table.

Column	Description
Date	Specifies the time and date that the message was processed.
Msg Id	The internal message identifier that GFI OneConnect Security has assigned to the message. Click the Message ID to view extended details in a pop-up window.
Client Address	The source IP address of the host that sent the message to GFI OneConnect. Note that if all your mail is relayed through an upstream mail relay before arriving at GFI OneConnect, then this column will only contain the address of the upstream mail relay.
Type	The message type as classified by GFI OneConnect Security during scanning.
From	The envelope sender address.
To	The envelope recipient address.
Size	The size of the message
Subject	If enabled in Display Settings , this column shows the subject header of the received message.
Flow	If enabled in Display Settings , this column shows the direction of the message <ul style="list-style-type: none"> » Inbound » Outbound » Internal

Column	Description
TLS	If enabled in Display Settings , this column indicates if TLS was applied to the message. The value may be one of the following: <ul style="list-style-type: none"> »  Received over encrypted TLS channel »  Sent out over encrypted TLS channel »  Received and sent out over encrypted TLS channel
Delivery	If enabled in Display Settings , this column indicates the delivery status of the message. The delivery status may be one of the following: <ul style="list-style-type: none"> » Any » Sent » Deferred » Bounced » Expired <p>Note that rejected or quarantined emails have no delivery status as they have not been delivered.</p>
Delivery Response	If enabled in Display Settings , this column shows the SMTP response from the destination server. This can be useful to indicate, for instance, why a remote server rejected a message.

Mail Filters

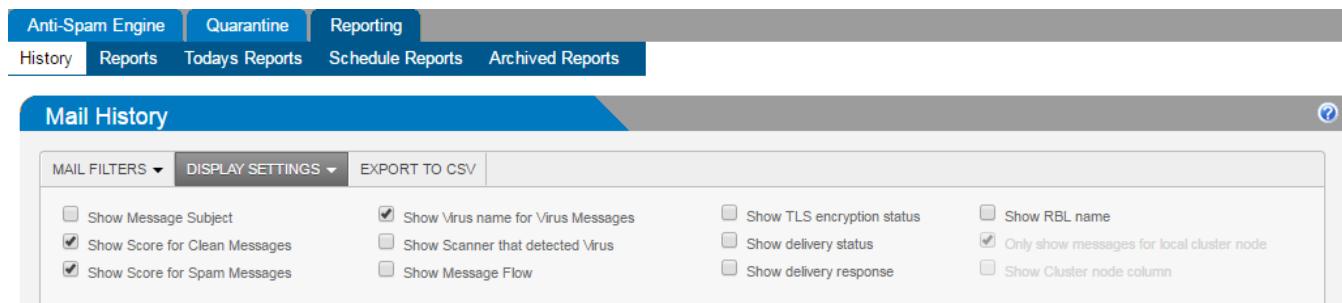
Various filters can be applied to narrow the number of logs in the Mail History table. The following table describes the various mail filters that can be employed. Multiple filters can be applied together to narrow the search further.

Filter	Description
Message Flow	Indicates the message flow direction: Inbound or Outbound
Message Type	Filter messages based on how they were classified by GFI OneConnect Security. Select Choose types and select the scan result types to show.
Recipient email address	Filter results using the recipient email address. Use * as a wildcard character. For example, to filter all messages sent to domain example.com enter *@example.com
Sender email address	Filter results using the sender email address. Use * as a wildcard character. For example, to filter all messages from the .co.uk domain enter *@*.co.uk
Source IP address	Filter results based on the connecting client IP address.
Security ID	The internal GFI OneConnect Security ID which is assigned to every message.
Score	The GFI OneConnect Security spam score assigned to a message. Note that messages which are not analyzed for spam will have no score (e.g. rejected messages)
Delivery Status	The delivery status may be one of the following: <ul style="list-style-type: none"> » Any » Sent » Deferred » Bounced » Expired <p>Note that rejected or quarantined emails have no delivery status as they have not been delivered.</p>
Subject	Filter based on message subject. Use * for wildcards.

Press the **Apply** button after selecting your search filters to refresh the display.

Display Settings

The options in the **Display Settings** tab allow you to control what columns and information are displayed in the mail history table.

A screenshot of the GFI OneConnect web interface showing the 'Mail History' section. At the top, there's a navigation bar with tabs for 'Anti-Spam Engine', 'Quarantine', and 'Reporting'. Under 'Reporting', there are sub-tabs: 'History' (which is selected), 'Reports', 'Todays Reports', 'Schedule Reports', and 'Archived Reports'. Below the navigation is a header bar with 'MAIL FILTERS ▾', 'DISPLAY SETTINGS ▾' (which is currently selected), and 'EXPORT TO CSV'. The main area contains a grid of checkboxes for various display settings. Some checkboxes are checked (e.g., 'Show Score for Clean Messages', 'Show Virus name for Virus Messages') while others are unchecked (e.g., 'Show Message Subject', 'Show TLS encryption status').

Setting	Description
Show Message Subject	Shows the subject of the message.
Show Score for Clean Messages	Shows the score assigned by GFI OneConnect Security for messages classified as Clean in the Type column.
Show Score for Spam Messages	Shows the score assigned by GFI OneConnect Security for messages classified as Spam in the Type column.
Show Virus name for Virus Messages	Shows the virus name that the scanner detected in the Type column for virus messages. Note that GFI OneConnect uses multiple virus scanners. If the virus scanners have different names for the virus, the name of the virus as identified by the virus scanner which identified the virus first will be used.
Show Scanner that detected Virus	Shows the name(s) of the virus scanner(s) that detected the virus in the Type column for virus messages.
Show Message Flow	Shows the direction of the email.
Show TLS encryption status	Shows the status of the Transport Layer Security (TLS).
Show delivery status	Shows the delivery status.
Show delivery response	Shows the SMTP response from the destination server.
Show RBL name	Shows the name of the Real-time Blackhole List (RBL) that blocked the message.

Screenshot 70: Configuring History Display settings

The following table describes the various Display Settings:

Display Setting	Description
Show Message Subject	Displays the subject of the message
Show Score for Clean Messages	Shows the score assigned by GFI OneConnect Security for messages classified as Clean in the Type column.
Show Score for Spam Messages	Displays the score assigned by GFI OneConnect Security for messages classified as Spam in the Type column .
Show Virus name for Virus Messages	Shows the virus name that the scanner detected in the Type column for virus messages. Note that GFI OneConnect uses multiple virus scanners. If the virus scanners have different names for the virus, the name of the virus as identified by the virus scanner which identified the virus first will be used.
Show Scanner that detected Virus	Displays the name(s) of the virus scanner(s) that detected the virus in the Type column for virus messages.
Show Message Flow	Shows the direction of the email.
Show TLS encryption status	Shows the status of the Transport Layer Security (TLS)
Show delivery status	Shows the delivery status.
Show delivery response	Shows the SMTP response from the destination server.
Show RBL name	Shows the name of the Real-time Blackhole List (RBL) that blocked the message.

Generating reports

The **Reporting > Reports** page allows you to generate a number of on-demand reports.

The screenshot shows the 'Generate Reports' section of the GFI OneConnect reporting interface. It includes a 'GENERATE REPORT ▾' dropdown, a 'Domain Group' field set to 'GFI-P-935', a 'Type' dropdown set to 'Domain Group Summary Report', a 'Period' dropdown set to 'Just for Today', a 'From' dropdown set to 'Local node only', a 'Report size' input field containing '10', and a 'Run' button.

Screenshot 71: Generating reports

The following table describes the options available when generating on-demand reports:

Field	Description
Type	Select the type of report to generate. The report types groups the information that includes overview of mail usage, top spam and viruses recipients..
Period	Choose the period for which the report will be generated. Options available are: <ul style="list-style-type: none"> » Just for Today » From Yesterday » Last 7 Days » All Note that a report period of All will generate a report based on all the records in the database. As records can be automatically purged, this may not include all records since subscribing to GFI OneConnect.
From	Choose the option that matches the scope of report. The options are: Local node only: Restricted to the server from where the report is been generated. Cluster: Include the entire cluster.
Report Size	Indicates the number of items to include in the report. This value is only relevant for top-ten type reports. Note that the pie chart is limited to a maximum of 25 items.

Click **Run** to start generating the report.

Go to **Reporting > Today's Report** to access all the on-demand reports that were requested today. The latest report is displayed on top. Click **View** to see the report data.

The following actions can be performed on generated reports:

Option	Description
View	Click to view your generated report. The displayed information depends on the type of report selected. Some reports display in the form of a table and some display as a pie chart.
Generate PDF Report	Generate and download a PDF version of the report.

Option	Description
Download to Spreadsheet	Generate and download a Microsoft Excel spreadsheet version of the report.
Delete	Delete the selected report. Note that deleted reports are not recoverable.
Archive	Generated reports are automatically purged on a daily basis. To save the report for longer, then you can archive it by clicking Archive. The Archive is accessible from Reporting > Archived Reports tab. For more information, refer to Archived Reports (page 136).

Scheduled Reports

GFI OneConnect Security reports enable you to generate reports on a pre-defined schedule to automate the generation of reports that are required on a regular basis. Scheduled reports are sent via email to a custom list of email addresses at a particular frequency.

The screenshot shows the 'Add report' dialog box with the following settings:

- Type:** Domain Group Summary Report
- From:** Cluster
- Frequency:** Daily Report
- Format:** PDF
- Max. items:** 10
- Archive:** Yes
- Email:** user@example.com
- Subject:** GFI OneConnect Security Report

At the bottom are 'Save' and 'Cancel' buttons.

Screenshot 72: Scheduled Reports options

Access the **Reporting > Schedule Reports** and configure the following report parameters:

Option	Description
Type	Select the type of report to generate. The reports available may vary depending on the role. The Domain Group Administrator role has access to organizational reports, and the data will include metrics for all domains. The Domain Administrator role can generate reports for the selected domain only. Change the role and the domain from the top-right corner of the screen.
From	Choose the option that matches the scope of report. The options are: <ul style="list-style-type: none"> » Local node only: Restricted to the server from where the report is been generated. » Cluster: Include the entire cluster.

Option	Description
Frequency	Choose how frequent you need to receive the report: » Daily : a report for the previous day's activity. » Weekly : run report every Monday covering the previous Monday-Sunday period. » Monthly : run report on the 1st day of every month covering the data for the previous month.
Format	Reports can be generated in a PDF document, a text file, a Microsoft Excel spreadsheet or all three.
Max Items	The maximum number of items to display in the report.
Archive	Specifies if the report should be saved in the Archive .
Email Address	Enter the addresses where to send the reports. Separate multiple emails addresses with spaces.
Subject	The subject to use for emailed reports.

Click **Save** to save the scheduled report.

Archived Reports

Generated on-demand reports are by default stored only temporarily, unless users opt to store a copy of the report in the Archive. The Archive page also stores copies of scheduled reports that are configured to be archived.

The **Reporting > Archived Reports** page lists all the reports that have been archived on GFI OneConnect Security.

From this page you can download reports in Text, Microsoft Excel or PDF formats or permanently delete the archived report.

Use the **Type**, **Frequency** and **Domain** settings to filter the list of displayed reports.

Date	Subject	Type	Frequency	Node	Download	Options	
2017-03-07 07:47:27	GFI OneConnect Security Report: [GFI-P-935]	Domain Group Summary Report	All	mx2.onemail.gfi.com	Text	Excel	PDF

Screenshot 73: Archived Reports

4 System settings

The topics in this section describe how to customize and configure GFI OneConnect system settings.

4.1 User Administration	137
4.2 Authenticating to GFI OneConnect	149
4.3 Email domains	157
4.4 Downloads page	165
4.5 Uninstalling the components	166

4.1 User Administration

Your organization's users are automatically imported to GFI OneConnect by the SyncManager component. Any changes applied to your organization's user directory are automatically synchronized by the SyncManager so that you do not have to maintain users in GFI OneConnect.

To access the list of GFI OneConnect users:

1. [Login](#) to GFI OneConnect using an administrator account.
2. From the top-right menu, navigate to **Settings > Users**.

The screenshot shows the GFI OneConnect web application. At the top, there is a blue header bar with the GFI OneConnect logo and several icons: Home, Sync, Settings, Help, and User. Below the header is a navigation bar with four tabs: 'Users' (which is selected and highlighted in blue), 'Authentication', 'Domains', and 'Downloads'. The main content area is titled 'Users' and contains a table of user information. The table has columns: a checkbox column, 'NAME', 'EMAIL', 'TYPE', 'LAST LOGIN', and 'ACTIONS'. There are five rows in the table, each representing a user: 'Administrator' (email: administrator@example.com, type: User), 'Bob B. Smith' (email: bob@example.com, type: User), 'Tim T. Smith' (email: tim@example.com, type: User), and 'Ann Smith' (email: ann@example.com, type: User). Each row has 'Edit' and 'Change Password' buttons in the 'ACTIONS' column. At the bottom right of the table, there is a button labeled 'Show 20 Results ▾'.

<input type="checkbox"/>	NAME	EMAIL	TYPE	LAST LOGIN	ACTIONS
<input type="checkbox"/>	Administrator	administrator@example.com	User		Edit Change Password
<input type="checkbox"/>	Bob B. Smith	bob@example.com	User		Edit Change Password
<input type="checkbox"/>	Tim T. Smith	tim@example.com	User		Edit Change Password
<input type="checkbox"/>	Ann Smith	ann@example.com	User		Edit Change Password

Screenshot 74: The list of GFI OneConnect users

The users table shows the users which are synchronized in GFI OneConnect. Use the **Search** and the **Filter** features to find particular users and narrow the list of users. Click a user's name or click **Edit** to show more user information.

This section describes features and functions that can be performed on GFI OneConnect users:

4.1.1 Promoting users to GFI OneConnect administrators	138
--	-----

4.1.2 Reviewing a user's contact information	138
4.1.3 Reset User Passwords	139
4.1.4 Creating Aliases	142
4.1.5 Defining User Sets	143
4.1.6 Export users information	144
4.1.7 Exclude Users or Mailboxes	146
4.1.8 Resolve User ID Conflicts	148

4.1.1 Promoting users to GFI OneConnect administrators

GFI OneConnect administrators can manage and configure GFI OneConnect. They can perform the actions and functions documented in this help, for both the Security and Continuity services.

NOTE

Assign administrative privileges only to trusted and knowledgeable users, since administrators have total control over the configuration and functionality of GFI OneConnect.

To promote a GFI OneConnect user to an administrator:

1. [Login](#) to GFI OneConnect using an administrator account.
2. From the top-right menu, navigate to **Settings > Users**.
3. Select one or more users to assign administrative privileges.
4. Click the **Set as** drop-down which is located above the users table and choose **Administrator**.
5. Click **OK** to confirm.

Removing administrative privileges

To revoke the administrative rights from an administrator account and demote the account to a regular user:

1. [Login](#) to GFI OneConnect using an administrator account.
2. From the top-right menu, navigate to **Settings > Users**.
3. Select one or more administrators to change to regular users.
4. Click the **Set as** drop-down which is located above the users table and choose **User**.
5. Click **OK** to confirm.

4.1.2 Reviewing a user's contact information

Users are normally requested to enter personal emergency contact information after logging in to GFI OneConnect the first time. This information is useful to enable you to get in touch with the user in the event of an email outage. GFI OneConnect also uses this information to send notification emails or SMS to users when there is a Continuity activation.

A GFI OneConnect administrator can review and edit another user's information when needed.

To load a user's contact information:

1. [Login](#) to GFI OneConnect using an administrator account.
2. From the top-right menu, navigate to **Settings > Users**.
3. The users table shows the users which are synchronized in GFI OneConnect. Use the **Search** and the **Filter** features to find particular users and narrow the list of users. Click a user's name or click **Edit** to show more user information.

The screenshot shows the 'Contact Details' tab of a user profile for 'Joe Doe'. At the top, there is a placeholder user icon, the name 'Joe Doe' with the title 'Administrator', and an email address 'jdoe@mydomain.com'. To the right, there are status indicators: 'Continuity' (Recovery), 'Server' (SERV801), 'Mailbox Store' (Mailbox Database), and 'Last Login' (14-Nov-2016 09:16 AM). Below this, there are tabs for 'Contact Details', 'Aliases', and 'Login History', with 'Contact Details' being active. The main area contains several input fields: 'Street Address 1' and 'Street Address 2' (both empty), 'State/Province' and 'City' (both empty), 'Zipcode' and 'Country' (both empty), and a 'Home Phone Number' field (empty). To the right, there is a section for 'Alternate Email Addresses' containing a single entry 'joe.doe@example.com' with a delete button. Below that is a dropdown for 'Cell Phone Carrier/Provider' set to 'Select'. Underneath is a 'Cell or SMS Number' field (empty) and a group of radio buttons for notification preferences: 'Do not use cellphone for automatic notifications' (selected) and 'Use cellphone for automatic text notifications via SMS'.

Screenshot 75: A user's contact details

4. The **Contact Details** window displays the list of contact fields.
5. Review or update any information as necessary.
6. Click **Save**.

4.1.3 Reset User Passwords

By default, users can log in to GFI OneConnect via Windows Authentication. For more information, refer to [Authenticating to GFI OneConnect](#) (page 149). If, however, the organization prefers to use a custom authentication system, then passwords need to be managed from the console.

GFI OneConnect automatically generates initial passwords for users when you send the [Welcome](#) message. There are two methods for resetting a user's password:

- » [Reset an Individual User's Password](#)
- » [Reset Multiple Passwords by CSV Import](#)

NOTE

If a user's password is changed when Continuity is in Ready or Recovery states, and the user's notification setting is set to receive text notifications via SMS, the user will **not** receive a password change confirmation SMS message. The password change notification is sent to the user's primary email address only. However, if the user's password is changed when Continuity is in the Active state, and the user's notification setting is to receive text notifications via SMS, the user receives a password change confirmation SMS message.

[Reset an Individual User's Password](#)

NOTE

This feature applies only when using Custom authentication, and not when using Windows Authentication.

To reset a user's password:

1. [Login](#) to GFI OneConnect using an administrator account.
2. From the top-right menu, navigate to **Settings > Users**.
3. Search for the appropriate user account and locate it in the users table. On the same line as the user account listing, click **Change Password**.
4. In the **New Password** box, type a new password.
5. In the **Confirm Password** box, retype the new password.
6. Click **OK**

[Reset Multiple Passwords by CSV Import](#)

You change user passwords in bulk using a CSV (comma separated values) file with UTF-8 encoding.

NOTE

This feature applies only when using Custom authentication, and not when using Windows Authentication.

[Step 1: Create a password import CSV file](#)

To create a password import CSV file, two reference files are provided for you to help create your CSV file. To locate them:

1. [Login](#) to GFI OneConnect using an administrator account.
2. From the top-right menu, navigate to **Settings > Users**.
3. Click **Upload Passwords**.
4. To download a CSV template file that you can use to start your own CSV file, click **Download Template**.

Row number	A	B	C	D
1	Primary Email	Password	Welcomed	Notification
2	user1@example.com	user1-p4ssw0rd	Y	

Row number	A	B	C	D
3	user2@example.com	user2-p4ssw0rd	N	user2@other.com
4	user3@example.com	user3-p4ssw0rd		user3@other.com
5	user4@example.com	user4-p4ssw0rd	Y	

The first row must contain the import file header typed exactly as it appears below:

- » First column: Primary Email
- » Second column: Password
- » Third column: Welcomed
- » Fourth column: Notification

Each additional row must contain the following information for exactly one user:

Column	Required	Description
Primary Email	Required	This address must match the user's existing email address in the system. If your file contains an unrecognized email address, the reset fails.
Password	Optional	The password to import for the user. During the import step, you can choose to enforce your organization's password policy when importing these passwords or to ignore it. To leave a user's existing password as it is, leave this column blank.
Welcomed	Optional	A flag indicating whether the user has already been welcomed to the system. <ul style="list-style-type: none"> » To leave the user's existing flag as it is, leave this column blank. » To indicate that the user has already been welcomed, set to Y. » To indicate that the user must be welcomed the next time they log in, set to N.
Notification	Optional	An optional notification address for the user. <ul style="list-style-type: none"> » To set the notification address to the same value as the user's primary address, set this column to Y. » To set an alternate address, type the email address in this column. » To leave the user's existing notification address, leave this field blank.

Save your import file as a CSV file with UTF-8 encoding.

NOTE

The CSV file you use for importing passwords must use UTF-8 encoding. Otherwise, passwords containing non-ASCII characters will be imported incorrectly, and users will be unable to log in.

Step 2: Import passwords by CSV file

To import passwords by CSV file:

1. [Login](#) to GFI OneConnect using an administrator account.
2. From the top-right menu, navigate to **Settings > Users**.
3. Click **Upload Passwords**.
4. In **Select Import File**, click **Browse** to locate the CSV file you want to import. Locate the file, then click **Open**.

NOTE

The CSV file you import must be correctly formatted. The CSV file must be located on your local machine or in a network-accessible location.

5. Under **Import Options**, select the options to apply to this import:

Option	Description
Overwrite passwords that were already created	Overrides any existing permanent passwords with those specified in the upload file. Leave this box blank (unchecked) to leave any existing permanent passwords.
Passwords must be at least 6 characters long and not the same as the user's primary email address or user ID.	Check this box to validate the passwords you are uploading against the criteria listed. If this box is checked, all passwords in the file must meet the listed criteria, or the import fails. Uncheck this box to upload all passwords in the file without applying any validation criteria.
Require users to change these passwords at next login.	Check this box to upload the passwords as temporary passwords that users must change immediately when they next log in. Uncheck this box to set the passwords as permanent , that can be used until they meet any expiration criteria defined by your organization.

6. Click **Next**.

7. The **Validation Results** page displays the total number of users found in the file, the number of users that will be imported or skipped, and any other important information. Click **Download Validation Results** to download a CSV file that shows any users that are skipped or whose information contains errors. You can use the information in this file to revise your import file, if necessary. Commented (informational) rows in the file begin with the # character. To find users whose information contains errors, look for rows that do not begin with the # character

8. If no validation errors are found, you can proceed with the bulk reset by clicking **Import**.

4.1.4 Creating Aliases

GFI OneConnect automatically creates an account for each mailbox in the primary mail system, whether the mailbox is associated with an individual person (end user) or is a collection box for certain types of email (such as status notices that are sent to a designated address). Administrators can manually create aliases that map incoming email messages to existing mailboxes. Any emails received by these aliases are treated as emails belonging to the associated mailbox.

Aliases of users and mailing lists imported from your primary mail system must adhere to the following requirements:

- » Usernames and distribution list names must not start with the pound character (#). GFI OneConnect ignores any mailing list or username that begins with the pound character.
- » Aliases must be in the form of email addresses (such as user@genericcorp.com) and contain a maximum of 64 characters, including the @ symbol and the full domain name.

To create an alias:

1. [Login](#) to GFI OneConnect using an administrator account.
2. From the top-right menu, navigate to **Settings > Users**.
3. The users table shows the users which are synchronized in GFI OneConnect. Use the **Search** and the **Filter** features to find particular users and narrow the list of users. Click a user's name or click **Edit** to show more user information.
4. Click the **Aliases** tab.

The screenshot shows the 'Aliases' tab selected for the user 'Jane Doe'. The top right corner has a close button (X). On the left, there's a user icon, the name 'Jane Doe', title 'User', email 'jdoe@example.com', and a summary table with fields: Continuity (Recovery), Server (SERV801), Mailbox Store (Mailbox Database), and Last Login (N/A). Below the summary table are three tabs: 'Contact Details', 'Aliases' (which is active and highlighted in blue), and 'Login History'. The main content area is titled 'Add Aliases to this user'. It contains three informational paragraphs: 1) A note about alias routing to the user's mailbox. 2) A note about quarantined inbound emails being routed to a mailox and continuity activation. 3) A note about alias address requirements. To the right, a modal window titled 'Added aliases:' lists three entries: 'jane.doe@example.com' (with a red X), 'jane@example.com' (with a red X), and 'doe@example.com' (without a red X). Below the list is a text input field 'Enter alias address here' and a blue 'Add' button with a plus sign.

Screenshot 76: User aliases screen

5. Key in an alias email address for the selected user and click **Add**.
6. Repeat the previous step to add more aliases or close the user window to return to the Users screen.

NOTE

To remove an alias, click **X** next to the alias address.

4.1.5 Defining User Sets

Administrators can define groups of mailboxes called **user sets**. User sets allow you to activate Continuity or apply other GFI OneConnect features to a designated group of users. For example, if you anticipate certain groups of users are likely to be activated separately (such as system administrators for tests), you can define a user set for them. Defining user sets specifically for testing allows for performance of regular system tests without activating all users and without taking down primary services.

NOTE

Activating Continuity for a subset of users or user sets requires the use of [Partial Activation via Redirectors](#).

To create a Continuity user set:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. From the Continuity Admin Console, go to **User Administration > User Sets**.
4. Click **Create User Set**.
5. In the **Name** box, type the name for the user set.
6. To build the user set manually, click the appropriate tab to select users for inclusion in the set by Servers, Mailing List, or individually by User.
 - If you select the **Mailing List** or **User** tab, in the **Search** box type an email address or name and search for the results. Then click the listed mailing list or user to select.
 - If you select the **Server** tab, click a server to select it.
 - Repeat until all desired servers, mailing lists, or users display in the **Users in the Set** listing.
7. To upload a CSV file containing user sets, click the **Chosen File** button, browse to the file location, select the upload file, and click **Open**. The CSV import file must be structured as follows:
 - a. The first row must contain the import file header **Email Address**.
 - b. Each additional row must contain the email address for exactly one user.
8. When all the users are selected, or the upload file is listed, click **Add**.
9. Click **Submit**.

4.1.6 Export users information

User data can be exported to a CSV file.

To generate a CSV spreadsheet of emergency contact data for all users:

1. [Login](#) to GFI OneConnect.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. From the Continuity Admin Console, go to **User Administration > Export**.
4. In the **Export User Information** screen click **Export** to download a CSV file containing the current data for all users.

Export files contain data that is available in the system as described in the table below.

Category	Data
User Account	Primary Email
	Display Name
	Journaling Service
	System ID
	Last Login
	Welcome Message Sent status
	Excluded (status)
	Has permanent password (status)
	Opted Out of Notifications (status)

Category	Data
Contact Information This field requires manual entry by end user into their GFI OneConnect profile.	Street Line 1 Street Line 2 City State/Province Zip/Postal Code Country Home Number Work Number Cell Number Email Address 1 Email Address 2 Email Address 3 Full Name 1 Relationship 1 Email Address 1 Phone Number 1 Full Name 2 Relationship 2 Email Address 2 Phone Number 2 Full Name 3 Relationship 3 Email Address 3 Phone Number 3
Notification Email Addresses Fields used by automated GFI OneConnect Alerting systems.	
End User's Emergency Contacts This field requires manual entry by end user into their GFI OneConnect profile.	

Category	Data
Additional data	Country/Region
Fields that are automatically synchronized from your organization's Active Directory. This consists of custom user attributes synchronized from Active Directory, so that the entries will be different for each organization.	Comment
	Company
	Department
	Fax
	First Name
	Home Phone
	Address-Home
	City
	Cell Phone
	Phone-Mobile-Other
	Pager
	Office
	Street Address
	Zip Code
	Last Name
	State
	Street-Address
	Street Address
	Phone Number
	Title

4.1.7 Exclude Users or Mailboxes

You can exclude certain mailboxes from receiving email notifications, from the welcome process and login status reports. You can exclude users by user sets, mailing lists, servers, and individual users.

This is typically useful to exclude resource mailboxes or other mailboxes that are not associated with a specific user, but which would still require the Security and Continuity services provided by GFI OneConnect.

To exclude a user:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. From the Continuity Admin Console, go to **User Administration > Excluded Users**

Excluded Users

An excluded user is not included in the notification reports, login status reports, or welcome process. This may be used for a resource mailbox, or any other mailbox not associated with a specific user who would be activated on OneConnect. By default no users are excluded.



You may use one of the links below to add/remove multiple users from the exclude list in one operation. You may also selectively remove users from the exclude list by clicking the remove button next to a user in the table below.

Excluded users are synced, and may be activated.

Exclude users ...

Add users to the excluded list.

Remove users from the excluded list ...

Remove users from the excluded list.

Search for users by name or email address.

Search For Users :

By Email By Name

*To remove users from the excluded list, click the Remove button next to the user's name.

[Export to file]

Name	Email Address	Action
John Doe	jdoe@mydomain.com	<input type="button" value="Remove"/>
Tim T. Smith	tim@mydomain.com	<input type="button" value="Remove"/>

Prev | Next

Screenshot 77: Excluded Users screen

4. Click **Exclude users**.

5. Identify users (mailboxes) to exclude. Click the appropriate tab to identify users by Server, Mailing List, or individually by User. If you select the **Mailing List** or **User** tab, in the **Search** box type an email address or name and search for the results. Then click the listed mailing list or user to select. If you select the **Servers** tab, click a server to select it.

6. Click **Add**. Repeat until all users to be excluded appear in the right list.

7. Click **Next**. The **Confirm** screen appears. To see the list of excluded users, click **Show Affected Users**.

8. Click **Submit**.

To remove individual users from the Exclude list (reinstate them in the system), click the **Remove** button next to the user's name in the **Excluded Users** table.

To remove multiple users from the **Excluded Users** list (reinstate them in the system):

1. Click **Remove Users from the excluded list...**

2. Identify users (mailboxes) to remove from exclude list. Click the appropriate tab to identify users by Server, Mailing List, or individually by User. If you select the **Mailing List** or **User** tab, in the **Search** box type an email address or name and search for the results. Then click the listed mailing list or user to select. If you select the **Servers** tab, click a server to select it.

3. Click **Add**. Repeat until all users to exclude are listed in the right list.

4. Click **Next**. The **Confirm** screen appears. To see the list of reinstated users, click **Show Affected Users**.

5. Click **Submit**.

4.1.8 Resolve User ID Conflicts

The system uses the Microsoft Exchange LegacyDN as a unique user identifier when processing mail. When moving users between Administrative Groups or Exchange Organizations, the Exchange LegacyDN may change. To ensure that retained mail remains associated with a user as the LegacyDN changes, the SyncManager checks for multiple instances of the same primary email address on each directory sync.

When SyncManager encounters more than one instance of a primary email address, GFI OneConnect sends out a notification to persons to the fault notifications recipients.

In most cases, the instances of the primary email address refer to the same, single end user, and by resolving the conflict, you ensure that mail collected for the first instance is associated with the second instance.

NOTE

When the same primary email address belongs to two different users, you must assign a new primary email address to either one of the users. For example: user Joe Smith (jsmith@organization.org) left the organization, but his mail was still subject to retention policies. A year later, you hired Jill Smith, and assigned the email address jsmith@organization.org. SyncManager would detect the conflict, but you would not want to resolve it using the methods described here, as that would associate Joe's retained mail with Jill's new mail. Instead, you must assign a new primary email address to either Joe or Jill.

User ID conflicts can be resolved automatically or manually. To configure the method to use for resolving user ID conflicts:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. From the Continuity Admin Console, go to **System Settings > User ID Resolution**.
4. In the **User Resolution Type** drop-down, select the resolution method.

Method	Description
Manual	Each User ID conflict must be addressed manually by an administrator through the Continuity Admin Console. This is the default setting. For more information, refer to Resolve User ID Conflicts Manually (page 148).
Primary Email	All multiple instances of a primary email address are presumed to be the same end user, and all mail is associated with that user automatically without administrator intervention.
All Aliases	If all aliases in the mailbox of the first instance of the primary email address are present in the second, the primary email addresses are presumed to be the same user, and the conflict is resolved automatically. The second may have additional aliases as well, but each of the primary aliases must appear. If only some or most of the primary ones are present, the action fails and an administrator must address the conflict manually in the Continuity Admin Console.
Active Directory Attribute	Choose a custom or default attribute from the ones synced from Active Directory. If the attribute values match, the primary email addresses are presumed to be the same user, and the conflict is resolved automatically. Some examples might be Employee Number, User ID or phone number.

5. Click **Submit**.

Resolve User ID Conflicts Manually

GFI OneConnect Administrators can resolve user ID conflicts manually using the processes described in this section.

Reset user ID conflicts manually using CSV

If you are doing a planned migration of users, and anticipate many user ID conflicts, you can prepare a spreadsheet identifying the users and upload it to the system. When the CSV is uploaded, the conflicts are resolved after the next Directory sync.

Prepare a CSV file in the format displayed in the table below.

First column:	Second column:
The Primary Email Address	New Exchange Legacy DN
suzy@lab104.organization.org	/o=E2K7-Lab104/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=suzy

To resolve multiple user ID conflicts using a CSV file:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. From the Continuity Admin Console, go to **User Administration > User Conflicts**.
4. In the **Upload user resolution information** section, click **Browse**, then select the CSV file.
5. Click **Submit**.

NOTE

Changes uploaded by CSV go into effect after the next directory sync. You may want to perform a manual sync to have the changes take place as soon as possible.

Resolve user ID conflicts individually

Each instance of duplicate primary address information encountered by the SyncManager is provided in the Continuity Admin Console. For each instance in the list, you can determine whether the email address belongs to the same user, and if so, resolve it.

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Manage > Continuity**.
3. From the Continuity Admin Console, go to **User Administration > User Conflicts**.
4. In the **Resolving User ID Conflicts Individually** section, identify a user and, in the **Resolve User** column, click **Details**. Both instances of the primary email address are provided, along with the Exchange Legacy DN value.
5. For the user, select one of the following:
 - I am unsure whether these are the same user. Keep these addresses in a conflict state until I find more information.
 - These addresses belong to the same user. Resolve the conflict, and store all mail together for this user in the system.
 - These addresses belong to different users. The first instance will be deleted, and only mail for the second instance will be retained as of the next directory sync.
 - These addresses belong to different users. I must create a new primary email address for one of the users. Remove this conflict from the list, but do not create new directory information until the next sync.
6. Click **Submit**.

7. If you chose to resolve the conflict, the user appears in the **Users Resolved** section. To delete the user from the list, click **Remove**.

4.2 Authenticating to GFI OneConnect

The authentication method defines the method that will enable your organization users and administrators to login to GFI OneConnect.

GFI OneConnect offers two methods of authentication. It is recommended to evaluate the best authentication mechanism for your organization and then decide on the preferred method.

The email address (username) and the set password is used to authenticate for all GFI OneConnect features, including logging in to the web interface, accessing WebMail during an email outage and accessing the security quarantine.

Authentication method	Description
Windows Authentication (default)	This authentication method allows your users to log into GFI OneConnect using their existing Windows passwords, as configured in your Active Directory forest. Although this is the easier authentication mechanism for end users as they do not need to manually set or remember a different password it requires the installation of multiple Authentication Manager components in your environment that facilitate verification of credentials with Active Directory. If no Authentication Manager is available, your users will not be able to log in to GFI OneConnect. For more information, refer to Windows Authentication (page 150).
Custom Authentication	An alternative login system dedicated to GFI OneConnect. This provides a password management system where a password policy can be implemented together with the facilities to reset and manage passwords. This method requires your users to login to GFI OneConnect to set a custom password which they can use exclusively for GFI OneConnect. For more information, refer to Custom Authentication (page 152).

4.2.1 Windows Authentication

This authentication method allows your users to log into GFI OneConnect using their existing Windows passwords, as configured in your Active Directory forest.

How it works

When a user tries to login, GFI OneConnect validates with Windows Authentication Manager component installed in your environment whether the credentials supplied are valid. Windows Authentication Manager, in turn, queries Active Directory to verify the credentials. The Active Directory reply (confirm or deny the validity of credentials supplied) gets sent back to the data center to allow or block access to GFI OneConnect.

IMPORTANT

User passwords are NOT stored on the GFI OneConnect data center. Authentication Manager validates credentials against the local Windows subsystem when users attempt to login. If the data center does not have access to at least one Windows Authentication Manager instance, users will not be able to login using their Windows credentials.

Windows Authentication prerequisites and important notes

The following are required to use Windows Authentication:

- » Ideally multiple Authentication Managers are installed, each in a different geographic region. More Authentication Managers provide redundancy and shorter login times. For more information, refer to [Installing Windows Authentication Manager](#) (page 151).
- » Any machine housing an Authentication Manager must be able to access a Domain Controller capable of authenticating a given user.
- » Sites housing Authentication Managers must have dedicated internet connections to provide redundancy in case of a site failure.
- » Disabled and/or Locked Active Directory accounts cannot log in.
- » Windows NT login IDs cannot be used; there is no way to ensure that an NT ID is globally unique. The SMTP address is a unique identifier.

Support for Exchange Resource Forests varies depending on the type of trust between the Exchange and security forests.

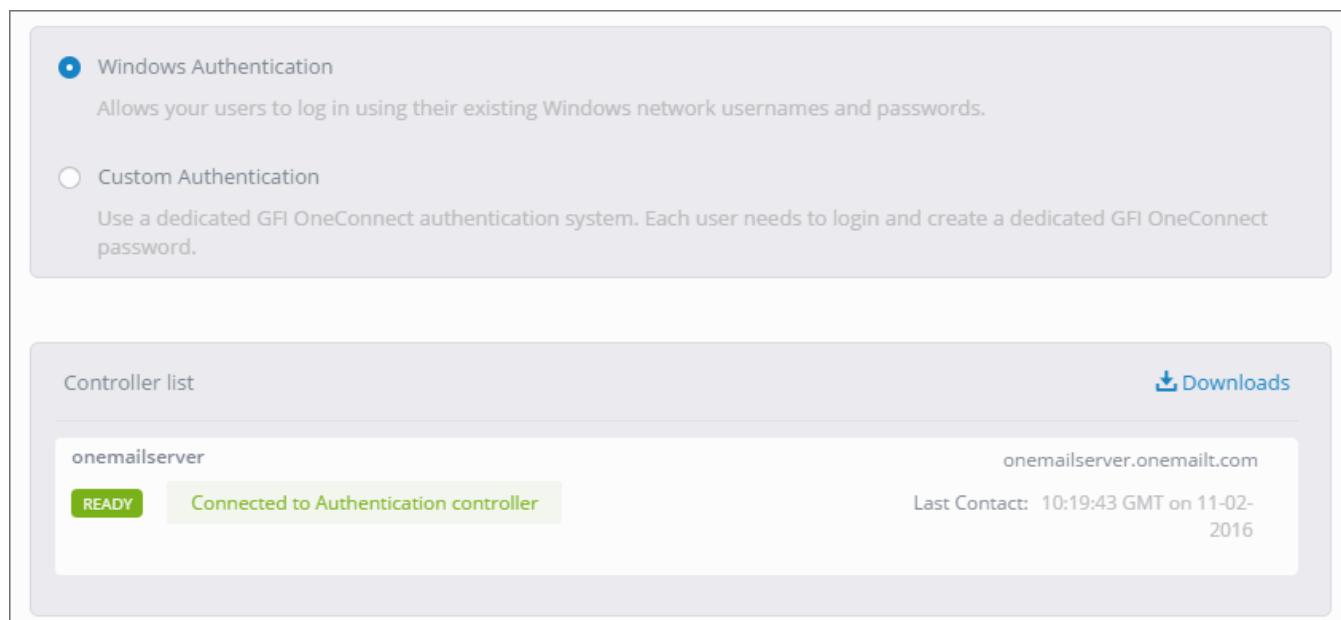
- » Two-way trust: No changes beyond the normal requirements for deploying authentication controllers (redundancy, distributed, etc) should be required.
- » One-way trust: Treat one-way trusts as distributed environments, and be sure to deploy a sufficient number of authentication controllers for redundancy purposes.

Enabling Windows Authentication

Windows Authentication is the default authentication method and usually, no further configuration is required from the GFI OneConnect web configuration.

In the event that authentication was switched to Custom Authentication, it can be reverted to Windows Authentication as follows:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Settings > Authentication**.
3. Select **Windows Authentication**.
4. Click **Save** to confirm the change.



Screenshot 78: Windows Authentication method selected

The **Controller list** area interface displays a list of Windows Authentication Managers available when this method is selected. Ensure that all controllers are Ready and that more than one controller is present for redundancy purposes. For more information, refer to [Windows Authentication](#) (page 150).

Installing Windows Authentication Manager

When installing the GFI OneConnect components, the Windows Authentication Manager is automatically installed. For more information, refer to [Installing the service components](#) (page 15).

To install other Authentication Manager instances on other servers, re-run the installation on other servers. When the wizard detects another instance of GFI OneConnect components, choose **Secondary** and click **Next**. In the next screen, select **Windows Authentication** and unselect the other features. Click **Next** and proceed with the wizard.

IMPORTANT

If Windows Authentication is not selected as the authentication mechanism used by your organization, Windows Authentication Manager cannot be installed. For more information, refer to [Enabling Windows Authentication](#) (page 151).

4.2.2 Custom Authentication

An alternative login system dedicated to GFI OneConnect. This provides a password management system where a password policy can be implemented together with the facilities to reset and manage passwords.

This method requires GFI OneConnect administrators to ensure that users set an account password, so that they can login. This is done by following a user welcome process, whereby users are notified about the service via email and invited to login at least once using a temporary password. On first login, users will be required to create a password and then to configure notification information.

The welcome process is important because it introduces users to the service before an emergency, helping them understand that system usage is a shared responsibility. It also allows the system to notifying users about the email outage and how to continue using email on their alternate email addresses, minimizing calls to your IT Helpdesk.

Next steps:

- » [Enabling Custom Authentication](#)
- » [Sending a welcome email to users](#)
- » [Welcoming new users automatically](#)
- » [Sending welcome process reminders](#)
- » [Custom password settings](#)

[Enabling Custom Authentication](#)

The default authentication mechanism in GFI OneConnect is Windows Authentication. To switch your authentication mechanism to Custom Authentication:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Settings > Authentication**.
3. Select **Custom Authentication**.
4. Click **Save** to confirm.

Windows Authentication
Allows your users to log in using their existing Windows network usernames and passwords.

Custom Authentication
Use a dedicated GFI OneConnect authentication system. Each user needs to login and create a dedicated GFI OneConnect password.

User Notifications Advanced Settings

Count	Description	Action
7	User who did not receive the introductory email from GFI OneConnect	View
2	Did not respond to the introductory email	View
9	Did not set a permanent password	View
11	Did not provide notification information	View
0	Set an account password and provided notification information	

Screenshot 79:Custom Authentication method selected

The web interface shows a list of users and their password setup status. Run the Welcome process to invite users to set an account password and configure their notification settings. For more information, refer to [Sending a welcome email to users](#) (page 153).

[Sending a welcome email to users](#)

The Welcome process enables GFI OneConnect administrators to facilitate the introduction of the system to the organization's users.

The process consist of three basic steps:

1. The administrator sends a welcome email to organization users, inviting them to login to GFI OneConnect using a temporary password.
2. The users login in to the system the first time using the temporary password and then set a custom permanent password.
3. The users enter notification details, including alternate email addresses where the system can reach them in the case of an outage.

The welcome process is important because it introduces users to the service before an emergency, helping them understand that system usage is a shared responsibility. It also allows the system to notifying users about the email outage and how to continue using email on their alternate email addresses, minimizing calls to your IT Helpdesk.

To send a welcome email to your organization's users when using Custom Authentication:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Settings > Authentication**.
3. Click the row **User who did not receive the introductory email from GFI OneConnect**. This category includes all users who have not yet been sent the welcome email.
4. Choose the users to whom to send the welcome email and click **Send Notification**.
5. Enter the notification details:

Message field	Description
From	Key in an email address that the message will be sent from. It is highly recommended to enter an alias within your organization so that any users who reply with questions are directed to an email administrator.
Subject	Type the message subject or use the default text.
Message Text	Type the message body text or use the default text. The service provides default text for the welcome message. You can also use the following variables in your message: <ul style="list-style-type: none">» %__username% — the recipient's GFI OneConnect username.» %__tempPassword% — temporary password generated by GFI OneConnect for the recipient.» %__autologinUrl% — the URL to access GFI OneConnect (with the username and password embedded).

1. Click **Send Now** to send the welcome email.

Sending welcome process reminders

Some users will undoubtedly ignore the GFI OneConnect welcome email and do not set a permanent password. GFI OneConnect provides tools to monitor the users who have not yet set a password and the facilities to send them reminders.

To send reminders to users who have either not set a permanent password or who have not specified any notification information:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Settings > Authentication**.
3. From the **User Notification** area, click the row for the particular user status that you would like to send a reminder to:

Statuses	Description
User who did not receive the introductory email from GFI OneConnect	Users who have never received a welcome message.
Did not respond to the introductory email	Users who were sent a welcome email but did not set an account password and did not provide notification information.
Did not set a permanent password	Users who have not set a permanent password.
Did not provide notification information	Users who have not yet provided an alternative e-mail address or mobile number for communication in case of an email outage. Notification information, such as alternative email addresses, is important to reach users when the primary email is down. It also allows users to take advantage of the Forgot Password link if they ever need it.

Statuses	Description
Set an account password and provided notification information	Users who completed the welcome user process by setting both an account password and notification information. IMPORTANT: You should aim to have all users within this category.

4. Select the users to receive the reminder. By default all users that match the group condition are selected.

5. Click **Send Notification**.

6. Enter the notification details:

Message field	Description
From	Key in an email address that the message will be sent from. It is highly recommended to enter an alias within your organization so that any users who reply with questions are directed to an email administrator.
Subject	Type the message subject or use the default text.
Message Text	Type the message body text or use the default text. The service provides default text for the welcome message. You can also use the following variables in your message: <ul style="list-style-type: none"> » %__username% — the recipient's GFI OneConnect username. » %__tempPassword% — temporary password generated by GFI OneConnect for the recipient. » %__autologinUrl% — the URL to access GFI OneConnect (with the username and password embedded).

7. Click **Send Now**.

Welcoming new users automatically

When new mailboxes and Active Directory users are added into your organization, SyncManager adds these new users to GFI OneConnect. These new users will also be required to set up a permanent password and provide notification information. GFI OneConnect offers the option to automatically send a welcome email to new users when these are added to GFI OneConnect by SyncManager.

NOTE

This feature works only when new users are detected, and existing users need to be notified manually.

To send a welcome message to new users as soon as they are added to GFI OneConnect:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Settings > Authentication**.
3. From the **User Notification** area, click **Advanced Settings**.
4. Select **Automatically send message to new users** and click **Configure Message**.
5. Enter the message details:

Message field	Description
From	Key in an email address that the message will be sent from. It is highly recommended to enter an alias within your organization so that any users who reply with questions are directed to an email administrator.
Subject	Type the message subject or use the default text.

Message field	Description
Message Text	Type the message body text or use the default text. The service provides default text for the welcome message. You can also use the following variables in your message: ➤ %__username__% — the recipient's GFI OneConnect username. ➤ %__tempPassword__% — temporary password generated by GFI OneConnect for the recipient. ➤ %__autologinUrl__% — the URL to access GFI OneConnect (with the username and password embedded).

6. Click **Save**.

New users will now be sent this email as soon as they are added to GFI OneConnect. It is recommended that periodically you login to ensure that new users have set a permanent password and provided notification information. Send reminders to those who do not. For more information, refer to [Sending welcome process reminders](#) (page 154).

Custom password settings

When using Custom Authentication GFI OneConnect, you can apply certain restrictions and limitations on the password set by users.

To configure Custom Authentication password settings:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Settings > Authentication**.
3. From the **User Notification** area, click **Advanced Settings**.
4. Configure the following options:

Password Constraints	Description
Minimum password length	Set the minimum number of characters that a password should be.
Password unique within (months)	Set the number of months for which the password should be unique. This prevents users from reusing old passwords within a period of time.
Password unique within (changes)	Set the number of changes for which the password should be unique. This prevents users from reusing old passwords within the specified iterations.
Allow password to match username	If enabled; users can set their password to be equal to their username.
Require strong passwords	If enabled; passwords must contain upper and lowercase letters, numbers and punctuation.
Notify users when their password is changed	Send an email notification to users when their password is modified.

The changes are automatically saved.

4.2.3 Lockout settings

The lockout policy settings specify the number of failed login attempts permitted and lockout period duration. These settings apply to both Windows and Custom authentication.

To Access the Lockout settings:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Settings > Authentication**.

3. Scroll down to the Lockout policy section.

4. Configure the following lockout settings:

Lock Out Policy	Description
Maximum Attempts	Define how many failed login attempts are allowed until a user is locked out.
Reset Attempts After	The number of failed attempts is automatically reset to zero after the specified number of minutes.
Lockout Period	How long the system will lock a user out after they have exceeded the number of failed Maximum Attempts .

The changes done are automatically saved.

4.3 Email domains

GFI OneConnect requires the list of your domains to identify emails belonging to your organization. When GFI OneConnect receives an email addressed to one of your domains, it first scans it through the Security service according to your organization's configuration. If the email is legitimate, GFI OneConnect redirects the email to your mail server.

There are some important considerations to be made when adding domains to GFI OneConnect:

- » The top priority MX Records of protected domains must be configured to point to GFI OneConnect so that inbound emails are first received by GFI OneConnect. For more information, refer to [Email routing](#) (page 11).
- » After GFI OneConnect processes an email, it must redirect it to your mail server. Make sure that your firewall and your mail servers accept inbound SMTP traffic (port 25) from GFI OneConnect. For more information, refer to [Email routing](#) (page 11).
- » After applying changes to domain configuration in GFI OneConnect, allow up to 10 minutes for the changes to take effect.
- » Incorrect or invalid domain settings can result in delayed, bounced or lost messages.

While setting up GFI OneConnect the first time you will be required to add a domain. Other domains can be added at a later stage from the GFI OneConnect Admin Console. To access and configure your account's email domains:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Settings > Domains**.

Refer to these topics for more information:

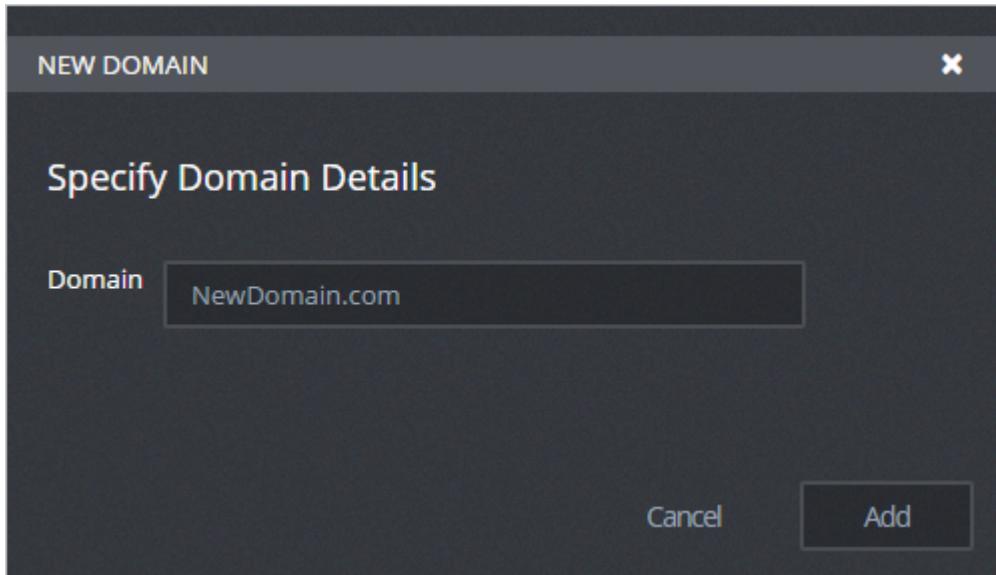
4.3.1 Adding a new domain	157
4.3.2 Editing a domain	158
4.3.3 Recipient Verification	160
4.3.4 Enabling Recipient Verification in Microsoft Exchange	162
4.3.5 Deleting a domain	164

4.3.1 Adding a new domain

While setting up GFI OneConnect the first time you will be required to add a domain. Other domains can be added at a later stage from the GFI OneConnect Admin Console.

To add a new domain:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Settings > Domains**.
3. Click **Add +** from the top-right corner.



Screenshot 80: Adding a new domain to GFI OneConnect

4. Key in the domain name and click **Add**.
5. Under the **Inbound routing** tab enter the following:

Option	Description
Inbound destination server	<p>Enter the public FQDN (preferred) or IP address of a mail server where GFI OneConnect redirects emails addressed to this domain. Click Add to add the address to the list. Repeat to add all the required destination servers. Mail servers can also be deleted by clicking X next to the domain to remove.</p> <p>IMPORTANT</p> <p>GFI OneConnect delivers inbound email to these servers in failover mode. If the first server is down or unavailable, it attempts delivery to the next server.</p> <p>The servers configured here must not send mail back to GFI OneConnect as a fail-over. Improper configuration can result in bounced or undelivered mail.</p>
Send test email	<p>Enter an email address in this field to send a test email to verify the domain configuration. Click Send. Ensure that you receive the test email to confirm that the Inbound destination server addresses specified are valid.</p>

6. Click **Save**.

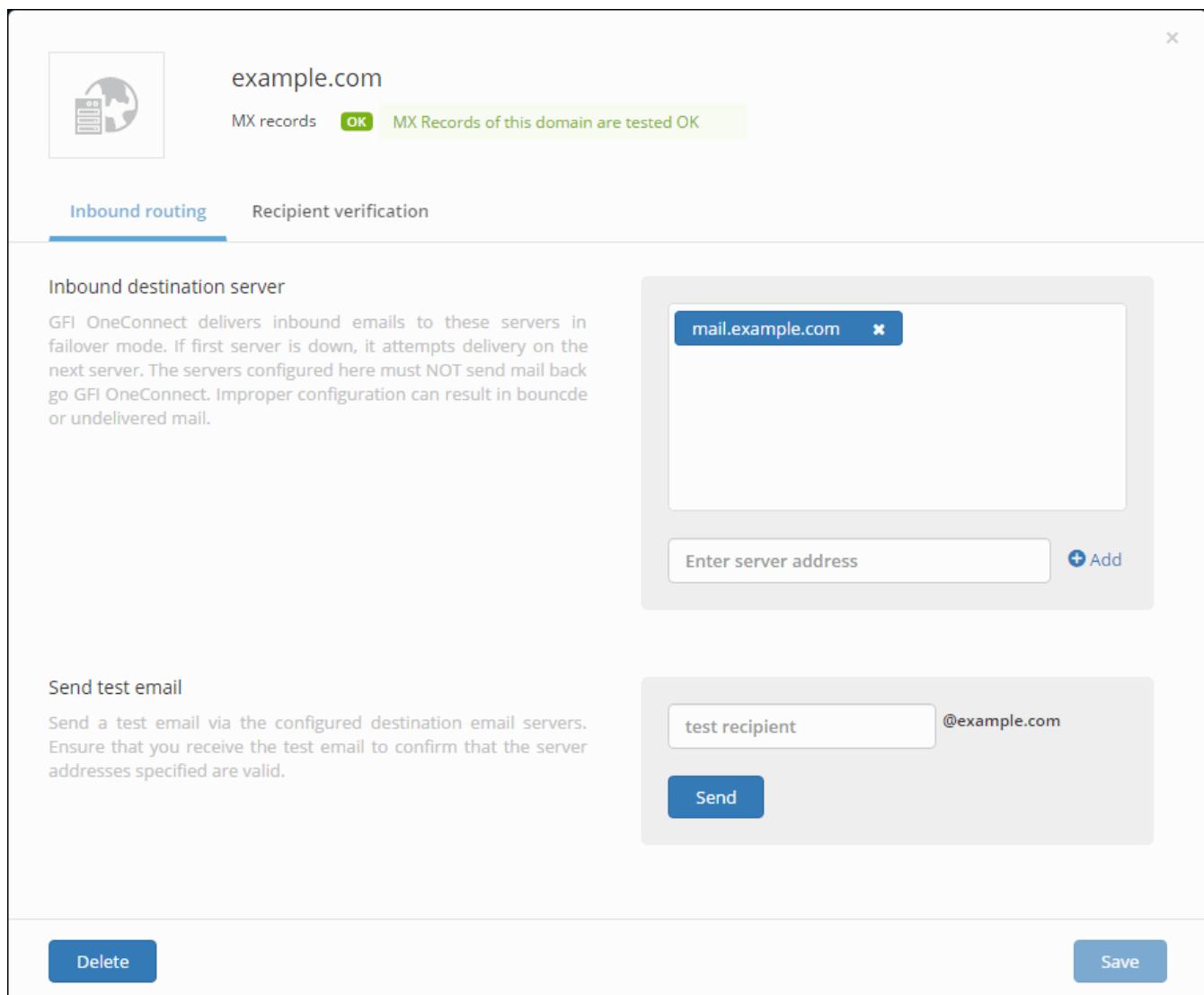
Under the **Recipient verification** tab, you can also turn on recipient verification for this domain. For more information, refer to [Recipient Verification](#) (page 160).

4.3.2 Editing a domain

Domains can be edited to reflect changes in the email infrastructure.

To edit a GFI OneConnect domain:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Settings > Domains**.
3. Click  from the right-top corner of the domain box.



example.com

MX records  MX Records of this domain are tested OK

Inbound routing Recipient verification

Inbound destination server

GFI OneConnect delivers inbound emails to these servers in failover mode. If first server is down, it attempts delivery on the next server. The servers configured here must NOT send mail back to GFI OneConnect. Improper configuration can result in bounces or undelivered mail.

mail.example.com 

Enter server address 

Send test email

test recipient @example.com

Send

Delete 

Screenshot 81: Email domain properties

4. Edit the properties as needed.

Option	Description
Inbound destination server	<p>Enter the public FQDN (preferred) or IP address of a mail server where GFI OneConnect redirects emails addressed to this domain. Click Add to add the address to the list. Repeat to add all the required destination servers. Mail servers can also be deleted by clicking X next to the domain to remove.</p> <p>IMPORTANT</p> <p>GFI OneConnect delivers inbound email to these servers in failover mode. If the first server is down or unavailable, it attempts delivery to the next server.</p> <p>The servers configured here must not send mail back to GFI OneConnect as a fail-over. Improper configuration can result in bounced or undelivered mail.</p>

Option	Description
Send test email	Enter an email address in this field to send a test email to verify the domain configuration. Click Send . Ensure that you receive the test email to confirm that the Inbound destination server addresses specified are valid.

5. Click **Save**.

You can also edit the recipient verification settings from the **Recipient verification** tab. For more information, refer to [Recipient Verification](#) (page 160).

4.3.3 Recipient Verification

The Recipient Verification check in the Security service prevents directory harvesting attacks.

Directory harvesting attacks occur when spammers try to guess email addresses by attaching well-known usernames to your domain. The majority of the email addresses are non-existent. Spammers send emails to randomly generated email addresses and while some email addresses may match real users, the majority of these messages are invalid.

Directory harvesting attacks can affect negatively the performance of the mail server during such attacks. It can also increase the volume of spam sent to the server if it finds legitimate email address to be used in future scamming campaigns.

Recipient Verification can stop these attacks by blocking emails addressed to users not in the email server or in the GFI OneConnect user list.

To enable Recipient Verification in GFI OneConnect:

1. [Login](#) to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Settings > Domains**.
3. Click  from the right-top corner of the domain box.

example.com

MX records OK MX Records of this domain are tested OK

Inbound routing Recipient verification

Recipient verification

Checks if the email recipients of inbound emails exist to protect against Directory Attacks. Emails to addresses that do not exist are rejected.

[Read More](#)

Enable Recipient Verification

Choose how to retrieve the recipient list:

GFI OneConnect users
Use the list of GFI OneConnect users as retrieved by SyncManager

Dynamic recipient verification
Verify recipients with your mail server. Your mail server must be configured to reject emails addressed to invalid addresses. Enter the mail server public address

[Read More](#)

Mail Server

mailserver.domain.com

Delete Save

Screenshot 82: Recipient Verification settings

4. Go to the **Recipient Verification** tab.
5. Switch Recipient Verification on or off from the **Enable Recipient Verification** option.
6. If enabled, choose how to retrieve the list of recipients:

Option	Description
GFI OneConnect users	<p>Use the list of GFI OneConnect users as retrieved by SyncManager. Use this option only in case that your mail server does not have the recipient verification option enabled.</p> <p>Ensure that new users are retrieved immediately by the GFI OneConnect SyncManager. Failure to do so may cause emails to be deleted before being processed by the mail server. For more information, refer to Setting up the SyncManager (page 21).</p>
Dynamic recipient verification (recommended)	<p>Verify recipients with your mail server. This option requires that your mail server supports recipient verification. For more information, refer to Enabling Recipient Verification in Microsoft Exchange (page 162).</p> <p>Under MailServer enter the public FQDN or the public IP address of the mail server.</p> <p>NOTE If using Microsoft Exchange 2013 or 2016 add port 2525 at the end of the mail server entry. For example <code>mailserver.domain.com:2525</code></p>

7. Click **Save**.

4.3.4 Enabling Recipient Verification in Microsoft Exchange

The dynamic recipient verification feature of GFI OneConnect relies on the capacity of the mail server to be able to detect which users belong to the domain and automatically reject users that did not exist.

Depending on the version of your Microsoft Exchange Server different methods can be used to enable recipient verification.

Follow the recommendations below to enable this feature on your mail server:

- » Microsoft Office 365
- » Microsoft Exchange 2013/2016
- » Microsoft Exchange 2007/2010

Microsoft Office 365

To enable Recipient Verification in Office 365 you need:

- » To have Exchange Online Protection enabled
- » To use a Global Admin or an Exchange Company Administrator account.
- » Enable Directory Based Edge Blocking (DBEB) feature from Office 365 to reject messages for nonexistent recipients.

For more information see <https://technet.microsoft.com/en-us/library/dn600322%28v=exchg.150%29.aspx>

Microsoft Exchange 2013/2016

In Exchange 2013 Microsoft recipient checking is done after DATA reception. This means even if the recipient validation is enabled on the mail server, any recipient check gets a "250 OK" response for invalid recipients.

To work around this problem you need to enable "Anonymous Users" on the Default Hub Transport connector and access the server on port 2525. In this way, invalid recipients are rejected after they are specified using the RCPT TO command.

To enable Recipient verification in Microsoft Exchange 2013/2016:

Step1: Check if the Exchange Anti-Spam Agents are installed and enabled

1. Login to the Microsoft Exchange Server with administrative credentials.
2. Open the Exchange Management Shell.
3. Run the following command: `Get-TransportAgent`
4. Ensure that the Recipient Filter Agent is installed and enabled.
5. If Recipient Filter Agent is not installed, run the following command:

```
& $env:ExchangeInstallPath\Scripts\Install-AntiSpamAgents.ps1
```

6. If Recipient Filter Agent is installed but not enabled, run the following command:

```
Enable-TransportAgent "Recipient Filter Agent"
```

7. Restart the Exchange Transport service after changes in the Recipient Filter.

Step 2: Ensure AddressBook is enabled

1. Run the following command in the Exchange Management Shell:

```
Get-AcceptedDomain | Format-List Name,AddressBookEnabled
```

2. Then ensure the Address Book is enabled.

3. If the AddressBook is disabled, use the following command replacing *example.com* with your domain:

```
Set-AcceptedDomain example.com -AddressBookEnabled $true
```

4. Restart the Exchange Transport service.

Step 3: Ensure Recipient Validation is enabled

1. Run the following command in the Exchange Management Shell:

```
Get-RecipientFilterConfig | FL Enabled,RecipientValidationEnabled
```

2. If Recipient Validation is disabled use the following command:

```
Set-RecipientFilterConfig -RecipientValidationEnabled $true
```

3. Restart the Exchange transport service after changes in Recipient Validation configuration.

Step 4: Allow access to the Default receive connector

1. Open the Exchange Administrative Center.

2. Navigate to **Mail Flow > Receive Connectors**.

3. Select your Default connector, and click **Edit**.

4. Open the **Security** tab and ensure that **Anonymous users** are allowed.

5. Restart the Exchange transport service to apply the changes.

6. If your GFI OneConnect server accesses your mail server via your firewall, ensure that port 2525 is allowed.

Step 5: Test Recipient Filtering

Check if the Recipient Filtering actually works by opening a telnet session via port 2525 on the mail server and try to send an email to an invalid user. The connection should not be completed.

For more information on how to perform a telnet test see [https://technet.microsoft.com/en-us/library/aa995718\(v=exchg.65\).aspx](https://technet.microsoft.com/en-us/library/aa995718(v=exchg.65).aspx)

Step 6: Configure GFI OneConnect to use port 2525 for Dynamic Recipient Verification

To edit a GFI OneConnect domain:

1. [Login](#) to GFI OneConnect with an administrator account.

2. From the top-right menu, navigate to **Settings > Domains**.

3. Click  from the right-top corner of the domain box.

4. Open the **Recipient Verification** tab and under the **MailServer** enter the public FQDN or the public IP address of the mail server followed by port **2525**. For example:

- 192.168.0.1:2525
- mail.example.com:2525

Step 7: (Optional, but recommended) Disable other Anti-Spam Agents

You may want to disable other Anti-Spam Agents so that only recipient verification is enabled. This prevents issues such as for example your mail server blocking the GFI OneConnect Quarantine Report. This report contains a list of Subject lines from spam emails and may be blocked as spam by the Content Filter Agent.

To disable other anti-spam agents:

1. Open the Exchange Management Shell.

2. Run the following commands:

```
Set-SenderFilterConfig -Enabled $false  
Set-SenderIDConfig -Enabled $false  
Set-ContentFilterConfig -Enabled $false  
Set-SenderReputationConfig -Enabled $false
```

3. Type Y to accept the changes.

4. Restart the Exchange transport service.

Microsoft Exchange 2007/2010

Follow these steps to enable Recipient Verification in Microsoft Exchange 2007/2010:

1. Login to the Microsoft Exchange Server with administrative credentials.

2. Open the Exchange Management Shell.

3. Run the following command:

```
Set-RecipientFilterConfig -Enabled $true
```

4. Restart the Exchange transport service.

For more information see [https://technet.microsoft.com/en-us/library/bb124087\(v=exchg.141\).aspx](https://technet.microsoft.com/en-us/library/bb124087(v=exchg.141).aspx)

4.3.5 Deleting a domain

To delete a domain from GFI OneConnect:

1. [Login](#) to GFI OneConnect with an administrator account.

2. From the top-right menu, navigate to **Settings > Domains**.

3. Click on the  icon on the right-top corner of the domain box.

4. Click **Delete**.

5. Click **OK** to confirm the deletion.

When a domain is deleted, GFI OneConnect no longer processes or protects emails that it receives that are addressed to the deleted domain.

NOTE

A deleted domain is not recoverable. All GFI OneConnect settings for that domain are permanently lost. You have to reconfigure the domain from scratch if to re-add it back in GFI OneConnect.

4.4 Downloads page

GFI OneConnect provides various installable components which can be downloaded from the Admin Console.

To access the Downloads page:

1. Login to GFI OneConnect with an administrator account.
2. From the top-right menu, navigate to **Settings > Downloads**.

The screenshot shows the 'Downloads' section of the GFI OneConnect Admin Console. At the top, there are tabs for 'Users', 'Authentication', 'Domains', and 'Downloads'. Below the tabs, the word 'Downloads' is displayed. The page lists several installable components with their descriptions, icons, download links, and 'Read More' links.

Installer	Description	Download	Read More
On-Server Site components	Install these components on a server in your network. The purpose of these components is to run background services such as synchronization of data, mail redirection, and user authentication. These components are installed at one go when running this installer.	Download	Read More
Microsoft Outlook Extensions	A Microsoft Outlook plugin that provides access to email via Microsoft Outlook during an outage. Users that have the Outlook Extension installed can continue sending and receiving emails seamlessly during a Continuity activation.	Download x86 Download x64	Read More
Import Manager	Import emails easily from your users directly from your PST, EML or Microsoft Exchange to GFI OneConnect Archive service.	Download	Read More
GFI OneConnect Exchange Redirector	To switch on Continuity to a subset of users or mailboxes only (Partial activation), install this Exchange Redirector on all Exchange Hub Transport Servers. The GFI OneConnect Exchange Redirector is a transport agent that enables dynamic rerouting of messages in Exchange environments. Without this component, Continuity can only be switched on for all mailboxes.	Download	Read More
Android Application	An Android app for your organization's end-users to access the Continuity Web Mail when Continuity is activated. This provides a quick and easy way for your end-users to continue using email directly from their Android devices when your email infrastructure is down.	Download	Read More
iOS App	An iOS app for your organization's end-users to access the Continuity Web Mail when Continuity is activated. This provides a quick and easy way for your end-users to continue using email directly from their iOS devices when your email infrastructure is down.	Download	Read More

Screenshot 83: Downloads page with installers available

Download any of the available installers:

Installer	Description
On-Server Site Components	Install these components on a server in your network. The purpose of these components is to run background services such as synchronization of data, mail redirection, and user authentication. These components are installed at one go when running this installer. For more information, refer to Installable Components (page 5).
Microsoft Outlook Extension	The Outlook Extension is a plugin that provides access to email via Microsoft Outlook during an outage. Users that have the Outlook Extension installed can continue sending and receiving emails seamlessly. Through Outlook Extension user also have a link to access their archived emails. Two MSI files are available. One for 32-bit installation and another to 64-bit. Select the installer according to the version of your Outlook installation. For more information, refer to Outlook Extension (page 58).

Installer	Description
Import Manager	Import emails easily from your users directly from your PST, EML, Microsoft Exchange or Microsoft Office 365 to GFI OneConnect Archive service. For more information, refer to Import Manager (page 105).
GFI OneConnect Exchange Redirector	To switch on Continuity to a subset of users or mailboxes only (Partial activation), RedirectorAgents must be installed on all Exchange Hub Transport Servers. RedirectorAgents are transport agents that enable dynamic rerouting of messages in Exchange environments. Without RedirectorAgents, Continuity can only be switched on for all mailboxes. For more information, refer to RedirectorAgents & Partial activation (page 26).
Android Application	An Android app for your organization's end-users to access the Continuity Web Mail when Continuity is activated. Mobile apps provide a quick and easy way for end-users to continue using email directly from a mobile device while the email infrastructure is down. Through the Mobile apps users also have access to their archived emails. For more information, refer to Continuity mobile apps (page 64).
iOS app	An iOS app for your organization's end-users to access the Continuity Web Mail when Continuity is activated. Mobile apps provide a quick and easy way for end-users to continue using email directly from a mobile device while the email infrastructure is down. Through the Mobile apps users also have access to their archived emails. For more information, refer to Continuity mobile apps (page 64).

3. Click **Download**.

4.5 Uninstalling the components

This topic describes how to remove the GFI OneConnect components from the GFI OneConnect server.

1. Exit GFI OneConnect.
2. From **Control Panel** select **Programs and Features**.
3. From the list of installed software select **GFI OneConnect** and click **Remove** or **Uninstall**.
4. Follow on-screen instructions.

NOTE

This procedure does not remove the Exchange Redirectors. To remove Exchange RedirectorAgents, repeat the above procedure on each Exchange Hub Transport server where the Exchange RedirectorAgents were installed.

5 Troubleshooting and support

For a list of common issues encountered when using GFI OneConnect, go to http://go.gfi.com/?pageid=oneconnect_help#cshid=troubleshooter

Most issues can be solved through the information in this help system. If you cannot find a solution to your problem or if you think that our content can be improved in any way, let us know by sending an email to documentation@gfi.com

Other sources of information available to solve issues with our software are:

GFI Knowledge base

GFI maintains a comprehensive repository of answers to the most common problems. GFI knowledge base always has the most up-to-date listing of technical support questions and patches. If the information in this guide does not solve your problems, refer to [knowledge base](#).

Web Forum

User to user technical support is available via the GFI [Web Forum](#).

Request Technical Support

If none of the resources listed above enable you to solve your issues, contact the GFI Technical Support team by filling in an online support request form or by phone.

- » **Online:** Fill out the support request form and follow the instructions on this page closely to submit your support request on: <https://www.gfi.com/support/technical-support-form>
- » **Phone:** To obtain the correct technical support phone number for your region visit: <https://www.gfi.com/contact-us>

NOTE

Before contacting Technical Support by telephone, have your Customer ID available. Your Customer ID is the online account number that is assigned to you when first registering your license keys in the GFI Customer Area at: <http://customers.gfi.com>

6 Glossary

A

Activation

The process by which the administrators activates Continuity. When activation is enabled emails are queued in the GFI OneConnect Data Center, and users can use WebMail or the Outlook Extension to send and receive emails.

Active Directory

A technology that provides a variety of network services, including LDAP-like directory services.

Admin Console

A web interface for administrators to manage and configure GFI OneConnect.

Administrator Account

Account of a user with administrative rights to manage and configure GFI OneConnect.

Antivirus

A software countermeasure that detects malware installed on a computer without the user's knowledge.

Archive

A feature provided by GFI OneConnect that can archive all internal and external email into the GFI OneConnect Data Center.

Auto-reply

An email reply that is sent automatically to incoming emails.

B

Blacklist

A list of email addresses and domains from which emails are always blocked.

C

Continuity

A feature provided by GFI OneConnect that queues the emails sent and received in a Data Center and ensures that your organization can keep the mail flow even when the email infrastructure is down.

CSV

A comma separated values file format.

Custom authentication

One of the authentication methods allowed by GFI OneConnect. When this method is used client will receive an email with the URL to log in, their username and temporary password. The user must change their password at the first login.

D

Dashboard

A graphical representation that indicates the status and statistics of various operations.

Data Center

A remote location on a GFI OneConnect Server through which the email traffic is sanitized and then routed to the Exchange Server. It is also used for queuing emails during outage and for storing archives and synchronized calendar and contact information.

Directory Harvesting

Email attacks where known email addresses are used as a template to create other email addresses.

DNS

Domain Name System (DNS) is a database used by TCP/IP networks that enables the translation of hostnames into IP numbers and to provide other domain related information.

Domain

Address or URL of a particular network.

Domain Controller

A server that responds to security authentication requests within a domain, such as when logging in and checking permissions.

E

EWS

Exchange Web Services

F

False Positives

Legitimate emails that are incorrectly identified as spam.

G

GFI OneConnect Server

The machine where GFI OneConnect is installed.

GPO

Group Policy Object (GPO) is an Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.

H

Hyper-V

Microsoft's virtual machine capability.

I

inbound email

Email to be received.

Infrastructure

A collection of physical or virtual resources that supports an overall Email environment

J

Journaling

A feature that generates and sends a copy of every email that passes through the mail server. Do not confuse it with Archiving.

M

Mail server

The server that manages and stores client emails.

Mailbox

A directory or folder on the mail server used for receipt, filing, and storing emails.

Malware

All malicious types of software that are designed to compromise computer security and which usually spread through malicious methods.

MX Records

A mail exchanger record. It is a type of resource record in the Domain Name System that specifies a mail server responsible for accepting email messages on behalf of a recipient's domain, and a preference value used to prioritize mail delivery if multiple mail servers are available.

N

NETBIOS

An acronym for Network Basic Input/output. This system provides services to allow applications on different computers within a network to communicate with each other.

O

outage

Refers to a situation when the email server is down or offline.

outbound email

Email to be sent.

P

Partial Activation

Activating Continuity for a subset of your users only.

Q

Quarantine

A email database where emails detected as spam and/or malware are stored in a controlled enviornment. Quarantined emails are not a threat to the network

R

Real-time Blackhole List

A list of domains and IP addresses that have been classified as spammers

Redirectors

Transport agents that enable dynamic rerouting of messages in Exchange environments.

Reviewer Group

Archive users who have the ability to search and read emails that are within the scope of a group of users.

Root Account

The user credentials used to register for a GFI OneConnect account.

S

Security

A service provided by GFI OneConnect that protects your inbound email from viruses, filters out spam and provides mail monitoring features.

SMTP

Simple Mail Transfer Protocol (SMTP) is an Internet standard used by GFI OneGuard for electronic mail (email) transmission. SMTP by default uses TCP port 25.

Spam

An irrelevant or unsolicited email sent over for the purposes of advertising, phishing, spreading malware, etc.

SSL

Secure Sockets Layer (SSL) is a computer networking protocol for securing connections between network application clients and internet.

T

TCP ports

Acronym for Transmitting Control Protocol. This protocol is developed to allow applications to transmit and receive data over the internet using the well-known computer ports.

TLS

Transport Layer Security (TLS) is a predecessor of Secure Sockets Layer (SSL), and just like SSL, it provides communications security over a computer network.

U

URL

The Uniform Resource Locator (URL) is the address of a web page on the world wide web.

V

VMware

VMware is a virtualization and cloud computing software provider for x86-compatible computers.

W

WebMail

A web-based email client provided by GFI OneConnect that is available when your organization's primary email infrastructure is unavailable.

Whitelist

A list of email addresses and domains from which emails are always received.

7 Index

A

Activating 34, 143
Activation 37, 50, 96, 143
Admin Console 5, 7-8, 17, 21, 28, 33-35, 45-46, 48-49, 53-56, 61, 72, 112, 144, 146, 148-149, 157, 165
Administration 52, 62, 65, 73, 112, 137, 144, 146, 149
Archive 5, 7, 38, 51, 66, 73, 87, 89, 91-92, 95, 113-115, 123, 126, 135-136, 166
Archiving 66, 68, 70-72, 74-75, 77, 79, 83, 87-91, 96, 116
Authentication 5, 18, 22, 25, 28, 47, 57, 61, 139-140, 150-152, 154-156

B

Blacklist 118, 127

C

Cloud services 87
Components 5, 10, 25, 33, 165
Configuration 17, 21, 47, 63, 80, 84
Configuring 23, 80, 84, 87, 109, 133

D

Dashboard 30, 119
Domain Policies 120, 128
Domains 8, 30, 120, 130, 157-158, 160, 163-164
Download 7, 63, 66, 107-108, 135, 140

E

Email Routing 47
EWS 21, 25, 40, 101
Exchange Web Services 18, 21
Extension 6, 22, 32, 34, 43, 58-59, 61-64, 104, 165

H

Home page 29, 56

I

Installation 15, 26, 61, 63, 108
Installing 15, 26, 61, 63, 151

L

Lockout 156

M

Monitor 7, 22, 67
Monitoring 27, 44

O

On-premise 7, 47, 73-74
On-premise archiving 73
Outlook Extension 6, 22, 32, 34, 43, 58-59, 61-64, 104, 165

Q

Quarantine 128, 164

R

Recovery 20, 30, 37, 51, 58, 67, 89-90, 95, 140
Redirector Controller 27
RedirectorAgents 6, 19, 26, 47, 166
Redirectors 27, 47, 143, 166
Reports 46, 49-53, 124, 126, 130, 133, 135-136
Requirements 9, 11
Restore 37, 67, 95
Restoring emails 95
Retention 51, 66-68, 70-72, 89, 91, 113-116
Retention Policies 51, 66-67, 69-72, 113-115
Reviewer 51, 67-68, 72, 89-91, 95, 117
Reviewer Groups 51, 67, 89-90, 95

S

Secondary installation 18
Security 5, 7, 11, 31, 47, 118-120, 124, 127-128, 130, 135-136, 138, 146, 157, 160, 163
Sign-in 36
Signing up 7
Storage 67, 116
Synchronization 18, 46
SyncManager 5, 7, 10, 13, 18, 21, 23, 30, 40, 45, 47, 54, 56, 61, 101, 137, 148-149, 155, 161
System Requirements 9

T

Troubleshooting 46, 167

U

Uninstall 28, 64
Uninstalling 166
User Policies 124, 128

W

WebMail 22, 28, 33-35, 45, 55, 58, 60, 64, 150
Whitelist 118, 127, 129