

Prerequisites for Mailshadow Server Edition:

Hardware Requirements for MailShadow Server Edition

Install MailShadow Server Edition on a dedicated, server-class computers or virtual machines with equivalent capabilities. The type of hardware on which you should install the MailShadow Gateway software is dependent on the number of users you want the system to support. The following is the minimum recommended hardware configuration:

- Any dual core processor
- 1GB RAM
- One high quality SATA Hard Drive
- 100 Mbps NIC

Software Requirements for MailShadow Server Edition

Before installing MailShadow Server Edition you must install and configure the following software:

- Microsoft Windows® Server 2003 R2 or Windows Server 2003 SP2 (x64 Edition is not supported—be sure to load only the 32-bit version). Be sure your operating system is patched to the latest service pack supported by Microsoft. (Server 2008 is under testing, if you do run 2008 please turn off UAC and ensure that the account the service is running as has admin access to the server)
- Microsoft Outlook 2007 - Fully patched
- .NET 3.5 Framework is required for MailShadow Server Edition

MailShadow Server Edition supports the following Exchange Servers:

Exchange 2003 (SP2 or higher). Be sure your operating system is Windows Server 2003 and is patched to at least SP1.

or

Exchange 2007 (SP1 or higher). Be sure your operating system is Windows Server 2003 and is patched to at least SP1.

Please note: Do not co-mingle other apps on the server running Server Edition. It has not been tested. It is very important that Exchange Management Console or Exchange System manager is not installed on the same machine. There are instances where that will work but not always.

Pre-Installation of Mailshadow Server Edition:

MailShadow needs a service/administrative account for each endpoint that has a unique name. The account must have the access so that it can accomplish the task of doing the 2 way replication.

Please note: At this time the service accounts cannot be named the same on any endpoint.

Google Endpoints: Please give any user that is marked as an administrator in the Google Premier Account. Also, please turn on the API Enable/Disable Setting under "Users"\ "Settings" in the admin portion of the Google Premier Account portal.

Microsoft BPOS Endpoints: Please give any user that is marked as an administrator.

Exchange Endpoints: This is very similar to BES Service Account and you are allowed to reuse that account if you prefer. Users and security groups should not be in other groups whenever possible because many groups remove access to Exchange. These rights are granted under the configuration naming context in Active Directory at: [Configuration root object]\Services\Microsoft Exchange\[Organization Name]

The rights needed to allow the service account to login to a different user's mailbox

Receive As

Send As

Please note: At this time the service accounts cannot be named the same on any endpoint.

Manual installation steps using ADSIEdit.msc (Preferred)

1. Launch ADSIEdit
2. Navigate to [Configuration root object]\Services\Microsoft Exchange
3. Right click and select properties on the folder with your Exchange Organization name (this is usually named something like "CN=Cemaphore Systems") identified by the class msExchOrganizationContainer
4. Select the Security tab
5. Select the Advanced button
6. Select the Add button
7. Enter the name of the Security group or user and Select OK.
8. Confirm that the "Apply onto" section is "This object and all child objects"
9. Specify the following Allow rights in the permissions area (usually near the bottom of the list)
 - Receive As
 - Send As
10. Select OK on all dialogs to save the security permissions.

Manual installation steps using Exchange 2003 System Manager

1. To enable the security tab within Exchange System Manager
 - a. On the machine that you will be running Exchange System Manager (from Exchange 2003) run regedit.

- b. Navigate to HKEY_CURRENT_USER\Software\Microsoft\Exchange\ExAdmin
 - c. Right-click EXAdmin and select New > DWORD Value
 - d. Enter "ShowSecurityPage" for the name
 - e. Enter 1 for the value
2. Launch Exchange System Manager
 3. Select the root most object. This is the Organizational object.
 4. Right-click this object and select properties
 5. Select the Security tab
 6. Select the Add button
 7. Specify the group/user
 8. Specify the following Allow rights in the permissions area
 - Receive As
 - Send As
 9. Select OK to save the security permissions

Using the Exchange Management Shell for Exchange 2007 only organizations

Choose from the following commands depending on company security policies and run the command from the Exchange Management Shell.

Setting send-as \ receive-as permissions at the Organization level

```
get-organizationconfig | add-adpermission -user vsa@domain.com -extendedrights send-As,receive-As
```

Setting send-as \ receive-as permissions to all mailbox databases on a specified Mailbox server

```
get-mailboxdatabase | where-object {$_.distinguishedname -ilike "*CN=server_name*"} | add-adpermission -user vsa@domain.com -extendedrights send-As,receive-As
```

Installing Mailshadow Server Edition:

Now that you have downloaded software and created the service accounts the next step is easy. The installation.

Installation

1. First add the service account you created in section 2 for your on-premise email as a local admin to the gateway you have setup.
2. Logon to the gateway as that service account.
3. Run the installer.
4. During the the install you will be asked for the service account credentials. Please put them in again. Please use the forum "user@domain.com".
5. Again make sure that Outlook and the OS (Server 2003 or Server 2008 32 bit) are fully patched. We understand fully patched to mean that Microsoft Update shows not critical or optional patches required.
6. Launch the UI. It will prompt for "Run As" user. Please put the service account in again.

Basic Configuration

1. Launch the UI.
2. Click on "Endpoints".
3. Click on "Manage Endpoints".
4. Click on new and create the on-premise Exchange endpoint first.

Create a name.

Choose the type. For Exchange leave the default Exchange setting.

Input the "Login Name". This is what the service account would logon to the computer with. "user@domain.com" form is preferred.

Password and Confirm Password are self explanatory.

SMTP address is just that, the address of the service account created for the on-premise Exchange users.

Exchange server FQDN. Again this should be the FQDN of the Exchange server the mailbox for the service account resides on.

If you are running inside the firewall in relation to the Exchange server you do not need the "Additional Settings", you can click on "Test Connection" and it should be OK. If it is not, please verify by creating a normal Outlook profile for the service account on the gateway to verify operation.

5. Click OK and you are done with the first (Exchange) endpoint.

6. Repeat this process for the second endpoint if it is an Exchange endpoint.

7. For a Google endpoint it is a little simpler.

Create the name and change the endpoint type to "Google".

Password and Confirm Password should be clear.

Under "Additional Setting" you will need to provide a "Default Password". This is the password you create new accounts with on the Google hosted domain. Having all of the users be the same password to perform the initial sync is the easiest best practice.

Click "OK" and then "Test Connection" and you should be done on a Google endpoint.

8. For a Microsoft Online (BPOS) endpoint it is a little more complicated.

Create the name and change the endpoint type to "Exchange Online".

Password and Confirm Password should be clear.

Fill out the "Login Name" and SMTP Address as usual for the BPOS service account. We suggest not having a separate BPOS service account just make a user an admin user so you don't waste an account in BPOS. Exchange server FQDN is greyed out because we can auto-discover it.

Click on "Additional Settings" and put in the URL for the proxy server in BPOS (this will be RED001.mail.microsoftonline.com for almost everyone in North America). In the "Principal name for proxy server" put in "msstd:*.mail.microsoftonline.com" (this should be the same for all users).

Click "OK" and then "Test Connection" and you should be done on a BPOS endpoint.

9. Now create the "Pairings". Click on "Pairings" and then "Manage Mailbox Pairings". In the "Provider #1" box select your Exchange on-premise endpoint. It will load an address list for that side. It could take several minutes. Repeat the process for the BPOS or Google endpoint. The BPOS endpoint has a tendency to take an extra minute or so please be patient. If it fails it will return an error.

10 Now you can add pairings. The auto match feature is convenient but by all means double check that the pairings look right.

Checking Installation Health of Mailshadow Server Edition:

GUI Health Indicators

In the Status column these are the four states:

- Unknown (what is seen prior to a first pass as we're gathering details about the mailbox)
- Failure (indication for admin to check logs)
- Success (first sync has been completed)
- Initial Sync

In the State column these are the following four states:

- Synchronizing (currently being processed in one of the threads – up to 15)
- Active (credentials have been accepted)
- Pending Credentials (pairing has been added but credentials have been changed or not yet configured – particularly true in the case of Google Apps mailboxes where admin accounts do not have the capability to give access to individual mailboxes)
- Stopped (Not yet implemented as of 6/16/2009)

Last Updated:

- The date & time of the last full loop completed

NOTE: we appreciate your input & will be responsive to suggestions.

Problems with Mailshadow Server Edition:

UI getting an error during test connection?

Please download this file:

<http://www.cemaphore.com/download/ExDirectory.exe>

Stop the services on the MailShadow Gateway and replace the existing version of the file with this one and try again.

Blackberry Rights and MailShadow?

You can use the same rights as the BES server: (via Powershell)

```
# Grant the user account MayLContact the right to create items in the public folder May Contacts.  
Add-PublicFolderPermission "May Contacts" -User MayLContact -AccessRights "CreateItems"
```

```
# Grant the user account BESAdmin Send As permission  
add-adpermission "Blackberry User" -extendedrights Send-As -user yourdomain\BESAdmin
```

```
# Grant the user account BESAdmin Exchange View Only Administrator permission  
add-exchangeadministrator BESAdmin -role ViewOnlyAdmin
```

```
# Grant the user account BESAdmin Send As, Receive As and Exchange Store Admin rights  
add-adpermission -user BESAdmin -accessrights ExtendedRight -extendedrights Send-As, Receive-As,  
ms-Exch-Store-Admin
```

```
# Grant the user account BESAdmin rights to access the store with all Outlook versions  
Set-CasMailbox BesAdmin -MAPIBlockOutlookVersions:$null
```

Archiving and Gmail?

There is a useful Advanced IMAP Controls feature under Google Apps Email/Settings/Labs that I recommend you adopt at Starfield for all your Google Accounts that MailShadow will be syncing. See below screenshots and the Google Blog on the feature here:

<http://gmailblog.blogspot.com/2008/10/new-in-labs-advanced-imap-controls.html>

When you Enable the Advanced IMAP Controls in Labs (and Save Changes), it exposes (in Gmail/Settings/Forwarding and POP/IMAP tab) the ability to turn OFF "Auto-Expunge" when messages are deleted via the Gmail IMAP interface (which MailShadow uses for the email data sync). We recommend you enable the Advanced IMAP Control in Labs, Save Changes, and then go into Gmail/Settings and under Auto-Expunge, select "Do not automatically expunge messages", and Save Changes.

Also, make sure "Archive the Message" is selected under the When a message is expunged..." section as

well. This will ensure that message deletes in Outlook/Exchange that MailShadow propagates to Google via IMAP will remain in the Google Apps mailbox (under All Mail), where they can continue to be accessed/searched/discovered for historical record-keeping purposes.

We recommend all your Google Apps users make these settings changes.

Upgrade issue from Build Prior to 3.2.19?

1. Remove the MailShadow shortcut from the autorun group in Windows.

2. Stop MailShadow.

3. Do a manual search and replace for: "MailboxName" and replace it with "SMTPName".

4. Run the upgrade.

Also you might need to adjust the "Run As" settings under the gateway settings. If the service is running as a domain user the account needs to be "user@domain.com". If the the service is running as a local user it needs to be specified as the just the user name like "Administrator".

Install Issues: To enable Windows Installer Logging?

Windows Installer can use logging to help assist in troubleshooting issues with installing software packages. This logging is enabled by adding keys and values to the registry. After the entries have been added and enabled, you can retry the problem installation and Windows Installer will track the progress and post it to the Temp folder. The new log's file name is random, but begins with the letters "Msi" and end with a .log extension. To locate the Temp folder location, type the following line at a command prompt:

```
cd %temp%
```

Open the registry with Regedit.exe and create the following path and keys:

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer

Reg_SZ: Logging

Value: voicewarmupx

The letters in the value field can be in any order. Each letter turns on a different logging mode. Each letter's actual function is as follows for MSI version 1.1:

v - Verbose output

o - Out-of-disk-space messages

i - Status messages

c - Initial UI parameters

e - All error messages

w - Non-fatal warnings
a - Start up of actions
r - Action-specific records
m - Out-of-memory or fatal exit information
u - User requests
p - Terminal properties
+ - Append to existing file
! - Flush each line to the log
x - Extra debugging information. The "x" flag is available only on Windows Server 2003 and later operating systems, and on the MSI redistributable version 3.0, and on later versions of the MSI redistributable.

"*" - Wildcard, log all information except for the v and the x option. To include the v and the x option, specify "/!*vx".

Note This should be used only for troubleshooting purposes and should not be left on because it will have adverse effects on system performance and disk space. Each time you use the Add/Remove Programs tool in Control Panel, a new Msi*.log file is created.

Folder name Problems?

If you have a folder named the same thing as a pre-defined folder like "Calendar" it can cause a failure to sync. For example if you have an email label in Google at the Root level named 'Calendar'. We map together the user's Google calendar '(User Name)' with his Exchange calendar 'Calendar', and then when we go to map the Google email label 'Calendar' it collides with the already mapped Exchange calendar and we stop trying to sync that folder.

This is a collision induced by allowing folders with roles (meaning Calendar, Tasks, Contacts, etc) to have different names, not a collision induced by different container classes. This is working as designed right now. The workaround is to change the name of the email folder so it doesn't have the same name as the pre-defined folder names like Calendar, task, Contacts, etc.

Password Lockout in Gmail?

Google periodically prompts the user to enter the text from a graphic that is not computer readable. Please go to:

<https://www.google.com/accounts/DisplayUnlockCaptcha>

and unlock Captcha.

How MailShadow Retries after an error or outage?

The service keeps a count of consecutive failures. After each task run, the error code is checked. If the code is 0x80040111 or 0x8004011d (MAPI_E_LOGON_FAILED or MAPI_E_FAILONEPROVIDER) the failure count is bumped. If the count reaches or exceeds the number of workers or the number of syncable pairings, the workers are shut down and, once the last is gone, restarts them. The failed tasks are simply added to the bottom of the pool to be “retried”. Since MAPI returns the same error for MAPI session problems and mailbox store issues, regardless of the error there is no task involving Exchange that will not be added back to the pool.

There are three Google errors that will cause a pairing to stop synchronizing. These are E_UNINITIALIZED_CALENDAR, E_IMAP_DISABLED and E_INVALID_CREDENTIALS. These errors refer to conditions that will require manual intervention to correct. The UI/service work has yet to be done that will cause the administrator to affect the Google endpoint password or resend the email to the recipient. So, for now, only restarting the service will allow pairings with these errors to “retry”. All other Google errors will still allow the task to be added to the bottom of the pool.

Since many errors could have been caused by overloaded systems or outages, any failed pairing synchronization will not be retried in the normal sync time interval (default is 5 minutes but settable by the registry value LastSyncTimeInterval). Instead, additional time is added to the LastSyncTimeInterval based on the new registry value “Error Retry Bump”. The default is 15 minutes but could be set to 0 in the registry. So, if a pairing fails, it will try again in LastSyncTimeInterval + Error Retry Bump minutes or 20 minutes if the values are not found in the registry.

Registry Key to Print Configuration (Important for Support)?

We have added an optional registry value, “Print Configuration”, to our Parallel Synchronizer service that will log the configuration data that is read from the configuration XML file at service start. It is a DWORD that, when greater than 0, will cause the configuration logging. This will allow us to validate that the parser is working as designed and that your configuration is loaded as expected. If you need to contact support, turning this on and restart will put useful information in the service log.

Exchange Management Tool and MailShadow Desktop?

We have found that if you have the Exchange Management Tools installed on your workstation the version of the MAPI dll's are different than we expect. This is not a supported config for Outlook and will not be a supported config for MailShadow for Exchange Online at this time.

Best way to contact support and give information (logs)?
Please send the logs zip'd up to support@cemaphore.com.

MailShadow Online Edition:

To initiate service we will need several things.

Service accounts according to Page 2 of this document. We need one service account for each syncing endpoint. As the document indicates we can reuse a service account for the BES server if present.

We need to ability to logon with Outlook outside your firewall to your Exchange server to the service account you have offered. All instructions for your end users to connect with Outlook outside the firewall would be useful.

We need these things for the on premise Exchange server:

- FQDN of the Exchange server the Service account is on

- User name of the service account

- Connection setting type (basic or NTLM)

- Front end server URL

- Proxy server name listed in the certificate (This is found in the Outlook profile if needed for your organization).

Any URL's we would need to allow for unprompted access to the email web access.

Please send this information to support@cemaphore.com