A MITEL
PRODUCT
GUIDE

MiContact Center Enterprise

E-mail Configuration - Operating Instructions

Release 9.6 SP1
Document Version 1.0

June 2023

Mitel
Powering connections

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®).** The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

TrademarksE-

The trademarks, service marks, logos and graphics (collectively “Trademarks”) appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

®,™ Trademark of Mitel Networks Corporation

INTRODUCTION

MiCC Enterprise may be integrated with e-mail servers for routing e-mails to agents or processing through the IVR. One e-mail server may be configured per tenant. All e-mail servers supporting standard IMAP4/SMTP as well as Office 365 using Microsoft Graph should be supported by MiCC Enterprise; however, MiCC Enterprise has only been tested with Office 365, Microsoft Exchange, Lotus Domino and Gmail. A general knowledge of IMAP and SMTP or Azure/Office 365 configuration should be understood by the MiCC Enterprise Administrator.

E-MAIL SERVER CONFIGURATION

This section shall describe the setup procedure for tested e-mail servers including Microsoft Exchange, Lotus Domino and Gmail. Any e-mail system supporting IMAP4 and SMTP may be used with the following conditions:

- IMAP and SMTP servers must support basic authentication.
- All incoming e-mail must be delivered to a single mailbox. This shall be known as the master mailbox throughout this document. E-mail may be forwarded from other accounts.
- The original “To” address of incoming e-mails must be maintained.
- Incoming and outgoing servers must support HTML and plain text e-mail.
- SMTP server must support changing the “From” address for outgoing e-mails. This may require setting authorization parameters on the server.
- No e-mail cleanup procedures should be performed on the master mailbox. For example, auto archiving, move to trash on delete. MiCC Enterprise will perform these actions based on the configured settings.
- All throttling in the servers should be disabled. An extensive amount of activity may be performed over a single connection to the servers and throttling may cause unwanted disconnects.

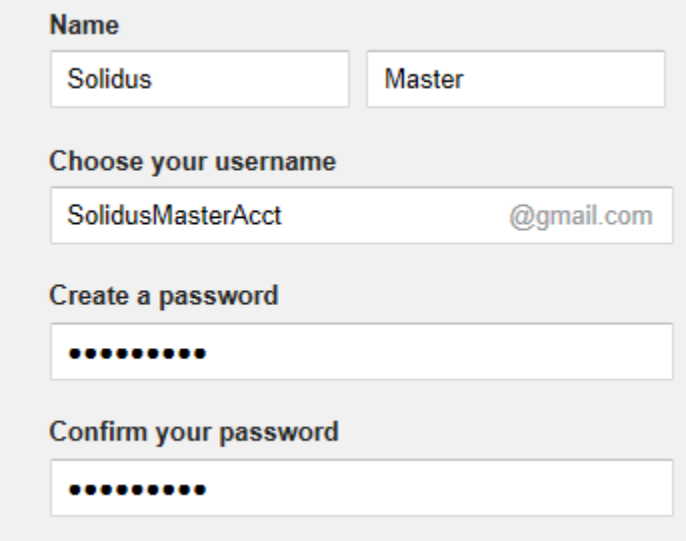
STANDARD IMAP/SMTP PORT NUMBERS

SERVER	ENCRYPTION	PORT
IMAP	SSL	993
	TLS	143
	None	143
SMTP	SSL	465
	TLS	25
	None	25
Gmail SMTP	TLS	587

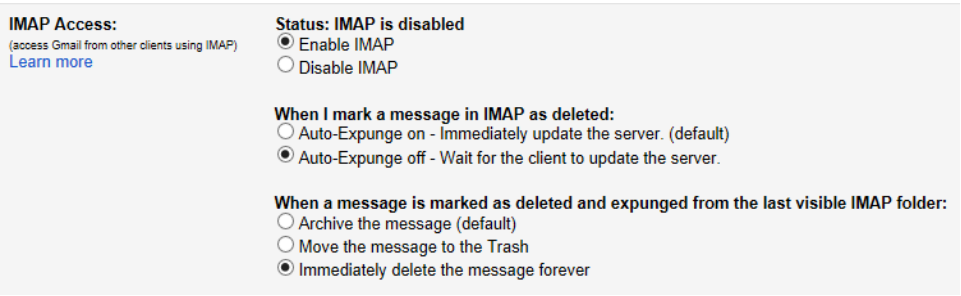
GMAIL

CREATE THE MASTER MAILBOX E-MAIL ACCOUNT

1. Access Gmail through your browser and select **Create an account**.



2. For the purpose of this instruction, the name of the account will be SolidusMasterAcct, however, you may choose any available account name. Make note of the username and password. Select Next.
3. Gmail may require account verification. Follow the verification procedure and continue to Gmail.
4. Access Gmail Settings and switch to the **Forwarding and POP/IMAP** tab.



5. Set the following options:
   a. Status: Enable IMAP
   b. When I mark a message in IMAP as deleted: Auto-Expunge off
   c. When a message is marked as deleted and expunged from the last visible IMAP folder: Immediately delete the message forever
6. Save the changes.
7. Access the settings for the Google account and ensure that the “Access for less secure apps” setting is turned on.

ENABLE 2-STEP VERIFICATION

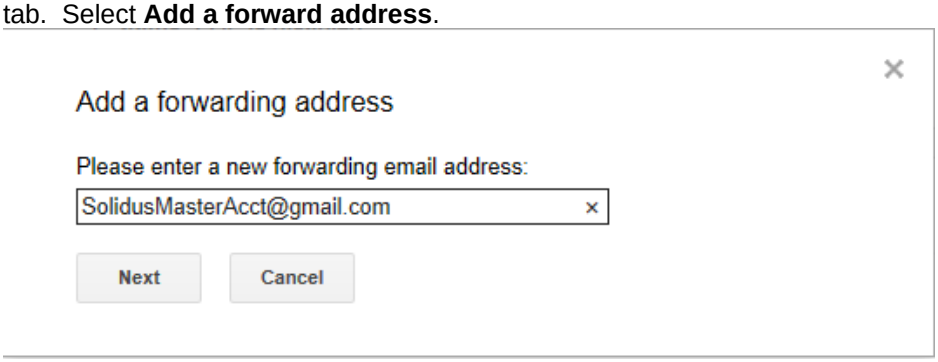
Due to recent security enhancements in Gmail, it may be required to enable 2-step verification for the Google account and generate an application password to be used with MiCC Enterprise. If you are unable to logon to the Gmail account using the standard user ID and password, enable 2-step verification using the following procedure.

1. In a Web browser, logon to the account using the standard user ID and password. It may be required to enter a phone number to receive a text message or call containing a verification code.
2. Access **Manage your Google Account**.
3. On the **Security** tab, enable 2-step verification and follow the steps to complete the setup.
4. Once again, access the **Security** tab. Under **Signing in to Google**, select **App passwords**. Add an App password for the **Mail** application and **Windows Computer** as the device. Click Generate.
5. Use the generated app password rather than the standard account password when configuring mail accounts in MiCC Enterprise.

CREATE THE SERVICE ACCESS MAILBOX E-MAIL ACCOUNTS

For each service access that will be processing e-mails, create an additional account in Gmail. For each account, you must log onto Gmail under that account and modify the settings.

1. Logon to the account and access Gmail Settings. Switch to the **Forwarding and POP/IMAP** tab. Select **Add a forward address**.

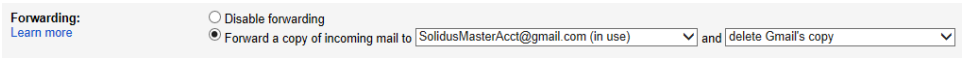


2. Enter the address of the master mailbox and click Next.
3. Gmail requires verification from the account that will be receiving the e-mails. An e-mail will be sent to this account asking for verification along with a confirmation code. The service access account will be waiting for you to enter the confirmation code. You do not need to enter the code at this point.
4. Logoff and logon to the master account. Open the verification e-mail and click on the link to confirm the request.
5. Access Gmail Settings for the master account. Switch to the Accounts and Import tab.
6. Under Send mail as, select Add another email address you own. Enter the name and email address. The name may be any descriptive name. The email address should be the address of the service account that you just created. Uncheck Treat **as an alias**. Click **Next Step**. A verification e-mail must be sent to the service access account. Click **Send Verification**.

Note: Only addresses specified under Send mail as may be used as the sender address. For Gmail, these addresses are case-sensitive. Any address used in MiCC Enterprise

configuration should match exactly with the address configured in Send Mail as.

7. Logoff and logon to the service access account just created. Open the verification e-mail and click the link to confirm the request.
8. Access Gmail Settings for the service access account. Switch to the F**orwarding and POP/IMAP** tab.



9. Select **Forward a copy of incoming mail to**. Ensure that the master account is selected. Select **delete Gmail's copy**.
10. Save the changes.
11. Repeat for each service access account.

TIP: For quick testing you can avoid creating individual service access e-mail accounts. Gmail has the ability to add a + (plus) sign and suffix to an e-mail address and still have it route to the main address. This should only be used for testing as the From: address will be incorrect for e-mail replies from agents as Gmail strips the +XXXX from addresses when it sends e-mails.

For example, if you have a master account with the address:

SolidusMasterAcct@gmail.com

You could create individual service accesses that monitor the following addresses:

SolidusMasterAcct+Sales@gmail.com
SolidusMasterAcct+Marketing@gmail.com
SolidusMasterAcct+Support@gmail.com

Sending an e-mail to any one of these addresses will route to the SolidusMasterAcct@gmail.com account.

OFFICE 365 FOR BUSINESS

Note: Due to throttling and rate limits that cannot be disabled, Office 365 is not recommended for high e-mail traffic installations.

Note: At the time of this writing, basic authentication was still supported for Office 365 using IMAP and SMTP; however, it was expected that the basic authentication support would be removed around October 2022. When that support is removed, IMAP and SMTP may no longer be used for Office 365. The specific *Office 365 using Microsoft Graph* configuration option in MiCC Enterprise must be used.

When using Office 365 the same principle of having a master email account and one mailbox for each email Service Accesses applies.

CREATE THE MASTER MAILBOX E-MAIL ACCOUNT

Follow the instructions on docs.microsoft.com for how to add a user to Office 365:
https://docs.microsoft.com/en-us/office365/admin/add-users/add-users?view=o365-worldwide

Set the password to never expire to avoid having to reset the password every 90 days.

CREATE THE SERVICE ACCESS MAILBOX E-MAIL ACCOUNTS

Follow the same procedure as for the master account above to create the mailbox.

Set Forwarding to the Master Account

Follow the instructions on docs.microsoft.com for how to set Email Forwarding:
https://docs.microsoft.com/en-us/office365/admin/email/configure-email-forwarding?view=o365-worldwide

Set Send As for the Master Account

Follow the instructions on docs.microsoft.com for how to set Send As:
https://docs.microsoft.com/en-us/office365/admin/add-users/give-mailbox-permissions-to-another-user?view=o365-worldwide#send-email-from-another-users-mailbox

EMAIL SERVER CONNECTION INFORMATION

Connecting to Office 365 may use IMAP/SMTP or it may use the Microsoft Graph API using a registered Azure application and client secret.

IMAP/SMTP

Office 365 uses the following IMAP and SMTP connection settings:

	Server name	Port	Requires SSL (TLS)
Incoming Mail (IMAP)	outlook.office365.com	993	Yes
Outgoing Mail (SMTP)	smtp.office365.com	587	Yes

Microsoft Graph using a Registered Application and Client Secret

A new application must be registered within the Azure tenant for use with MiCC Enterprise e-mail. An application may have already been registered if Single Sign-On or Azure User Synchronization has already been setup. The same application may be used.

1. Logon to Microsoft Azure Active Directory using an Administrator account under the desired AD Tenant.

2. Navigate to the *App registration* page.

3. If there is no application currently registered for use with MiCC Enterprise, select *New registration*. Enter a name for the application and select the desired account type. Click *Register*. If there is already an application registered, select the application. Note the Application (client) ID and the Directory (tenant) ID. These will be used when configuring MICC Enterprise.

4. Navigate to the *Certificates and Secrets* page.

5. Navigate to the *Client secrets* tab. Select *New client secret*. Enter a description and expiration. Click *Add*. Be sure to note the Value. This will be used when configuring MiCC Enterprise. The Value is only displayed during this session in Azure AD. Once logged off, it

can no longer be seen. If the Value is not noted or is lost, a new client secret must be created.

6. Navigate to the *API permissions* page.

7. The following permissions must be present for Microsoft Graph:

   Mail.Read
   Mail.ReadBasic
   Mail.ReadBasic.All
   Mail.ReadWrite
   Mail.Send

   If any permissions are not present, click the *Add a permission* button. Find the *Microsoft Graph* APIs. Select the *Application permissions* filter. Locate and check the missing permissions. Click the *Add permissions* button.

Security Note: MiCC Enterprise accesses the e-mail accounts through a back-end service. For this reason, *Application* permissions must be used rather than *Delegated* permissions. *Delegated* permissions act on behalf of a specific user which requires user interaction to logon which cannot be done from a back-end service. Application permissions will allow MiCC Enterprise to access any mailbox for the Office 365 tenant. This presents a potential security risk. To limit the mailboxes that MiCC Enterprise and the registered Application have, Microsoft recommends configuring an Application Access Policy limiting the registered Application to a specific security group containing only the specific mailboxes to allow access to. See the following Microsoft article describing this process.

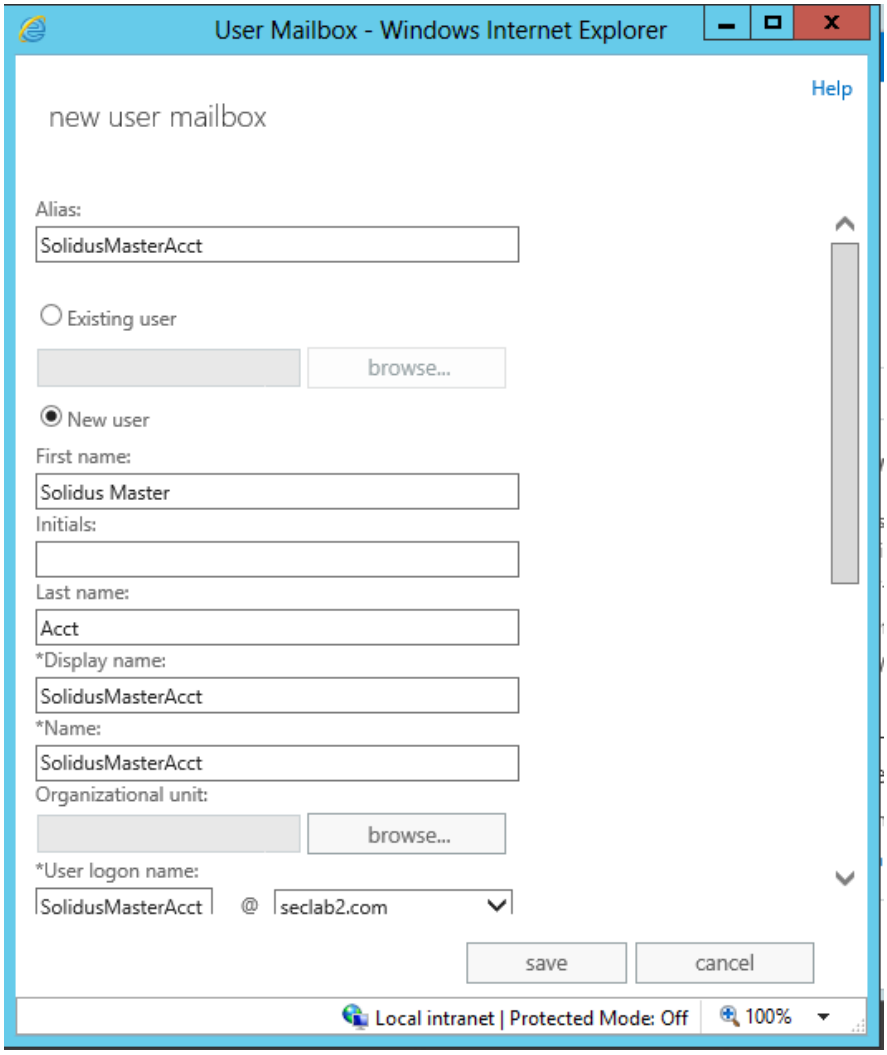
https://learn.microsoft.com/en-us/graph/auth-limit-mailbox-access

MICROSOFT EXCHANGE 2013

IMAP and SMTP must be enabled on the Exchange server prior to setup. Contact the Exchange Administrator for enabling these protocols.

CREATE THE MASTER MAILBOX E-MAIL ACCOUNT

1. Launch the Exchange Admin Center.
2. Select the **recipients/mailboxes** page.
3. Click the + button and choose user mailbox.

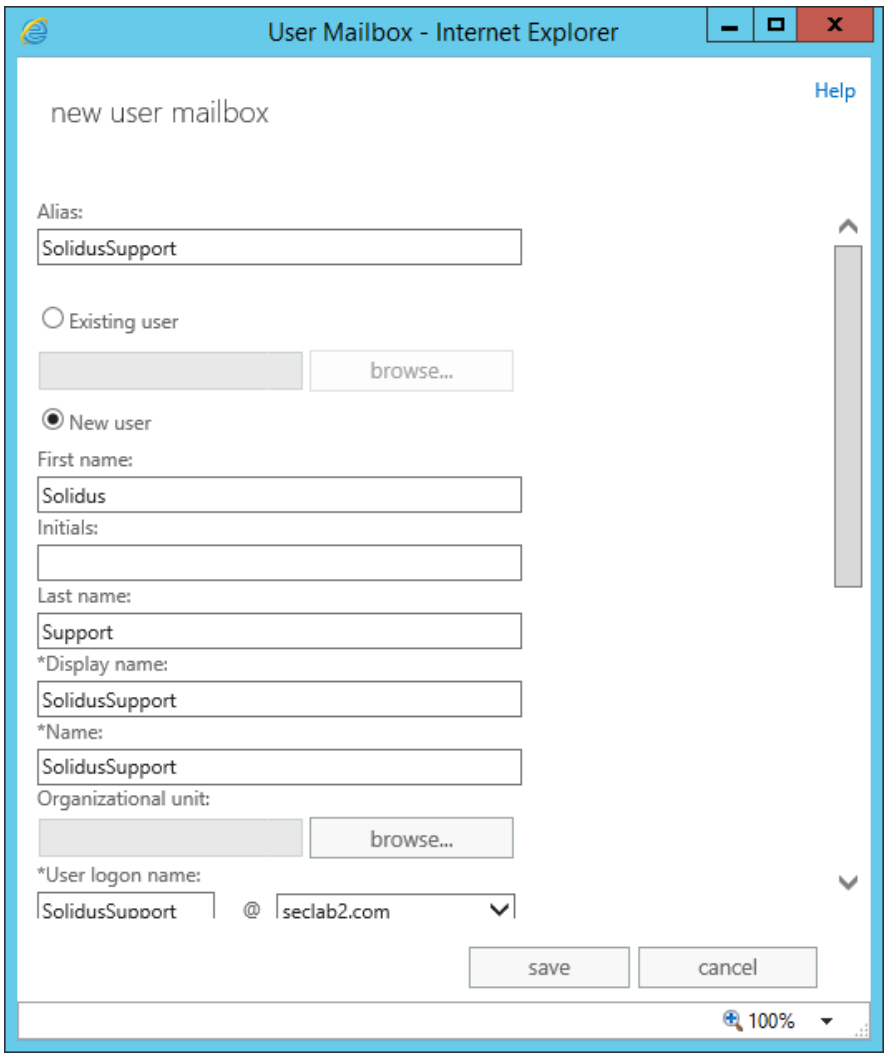


4. Select **New User**, enter the mailbox information and click **save**. For the purpose of this instruction, the name of the account will be SolidusMaster.

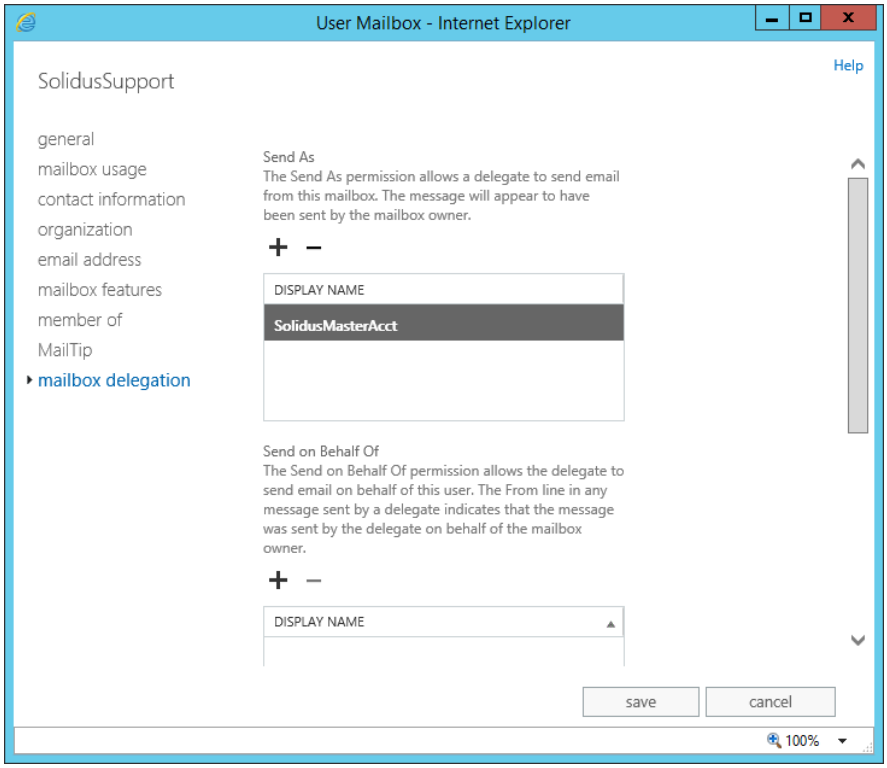
CREATE THE SERVICE ACCESS MAILBOX E-MAIL ACCOUNTS

For each service access that will be processing e-mails, create a security group that will route e-mails to the master account.

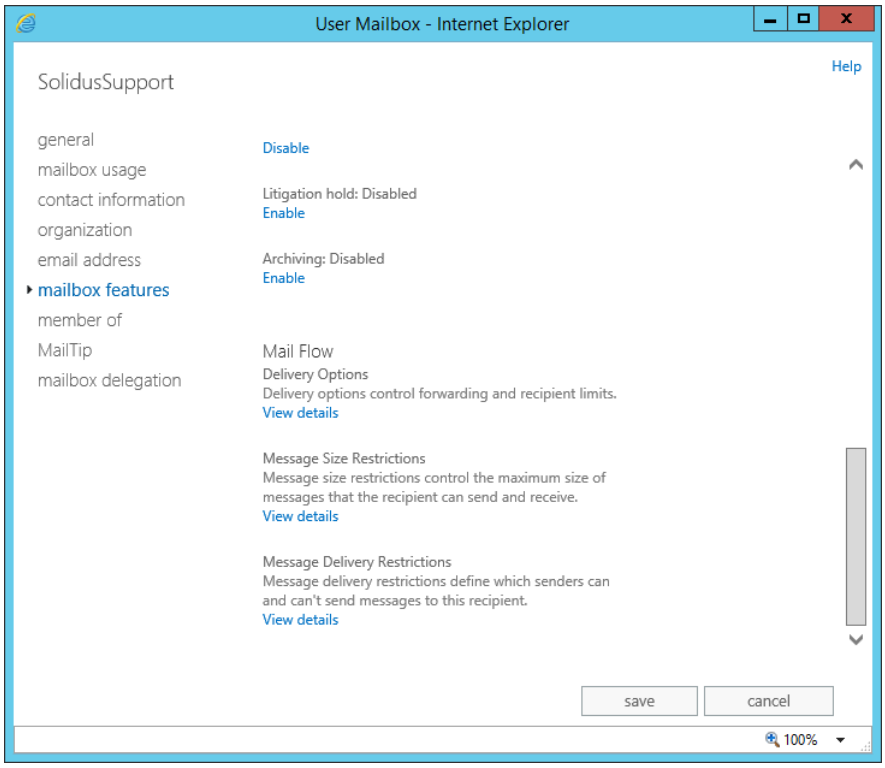
1. Launch the Exchange Admin Center.
2. Select the **recipients/mailboxes** page.
3. Click the + button and choose user mailbox.



4. Select **New User**, enter the mailbox information and click **save**. For the purpose of this instruction, the name of the account will be SolidusSupport.
5. Select the newly created account and click the **edit** button.
6. Switch to the **mailbox delegation** page.
7. Click the + button for the **Send As** permission.
8. Add the SolidusMasterAcct account and click **ok**.



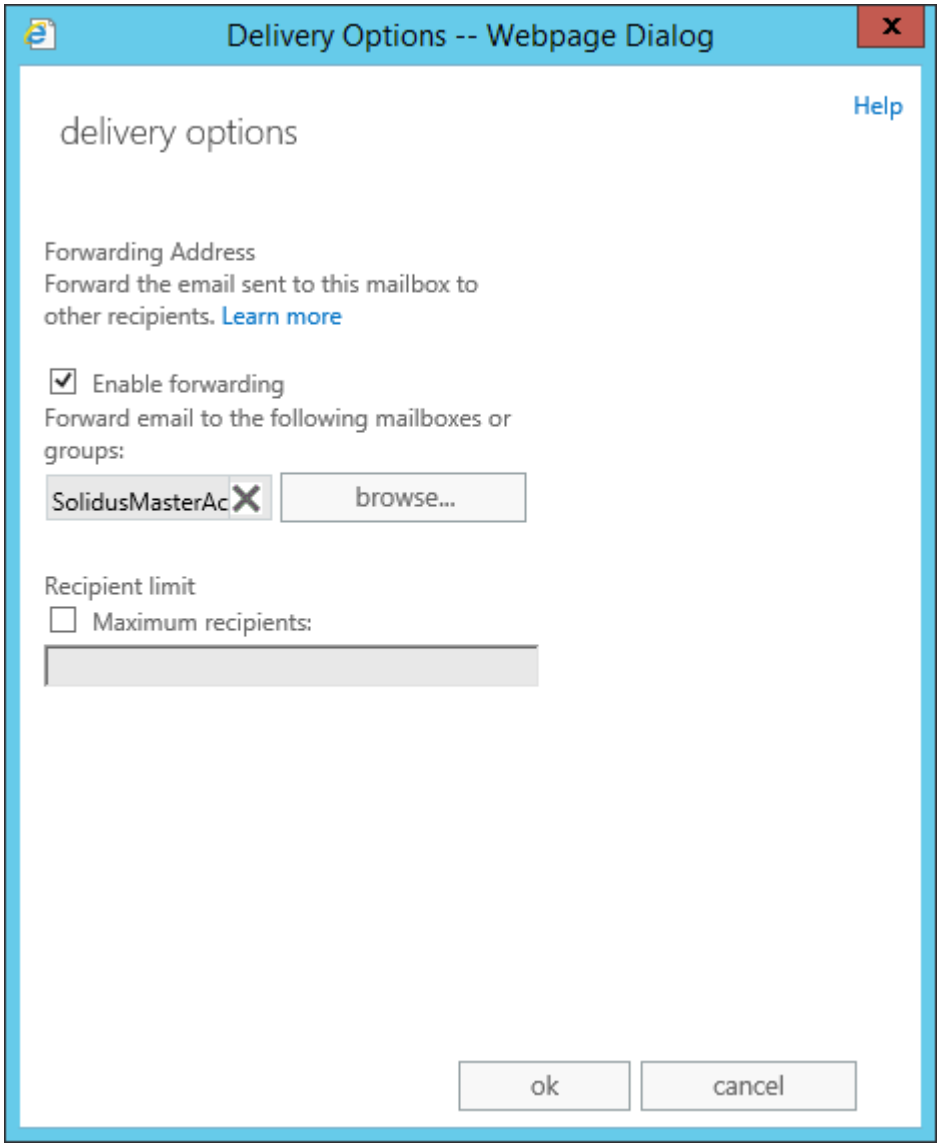
9. Switch to the **mailbox features** page.



10. Click **View details** under the **Delivery Options** heading.

11. Check the **Enable forwarding** option.

12. Click the **browse…** button.
13. Select the SolidusMasterAcct account and click **ok**.



14. Click **ok** to save the delivery options.
15. Click **save** to save the mailbox settings.
16. Repeat steps 2 through 15 for each service access e-mail account.

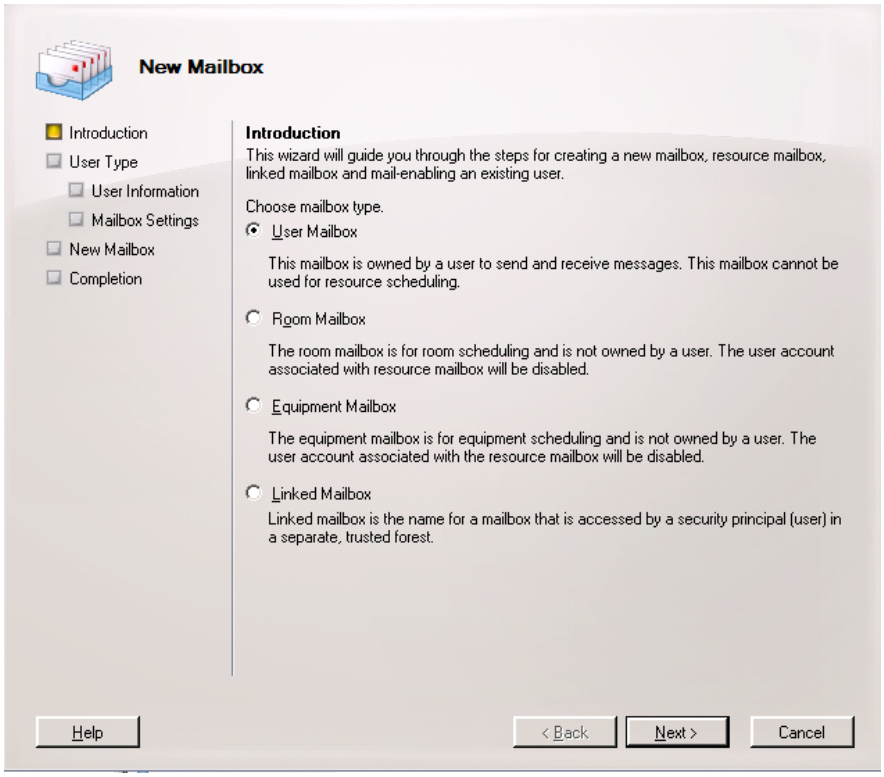
MICROSOFT EXCHANGE 2007/2010

IMAP and SMTP must be enabled on the Exchange server prior to setup. Contact the Exchange Administrator for enabling these protocols.

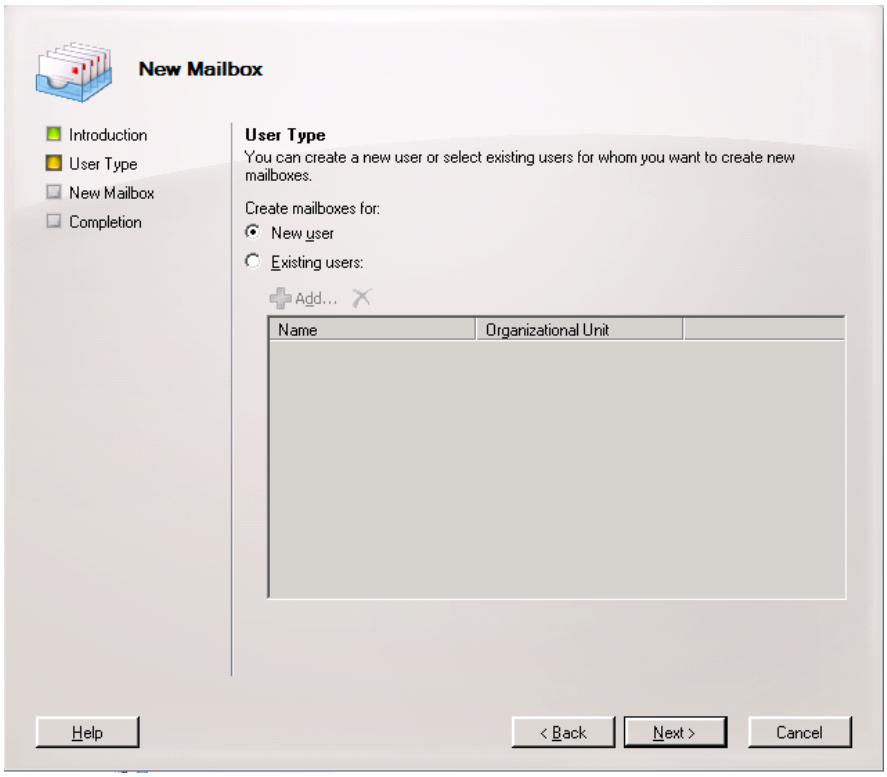
CREATE THE MASTER MAILBOX E-MAIL ACCOUNT

1. Launch the Exchange Management Console.

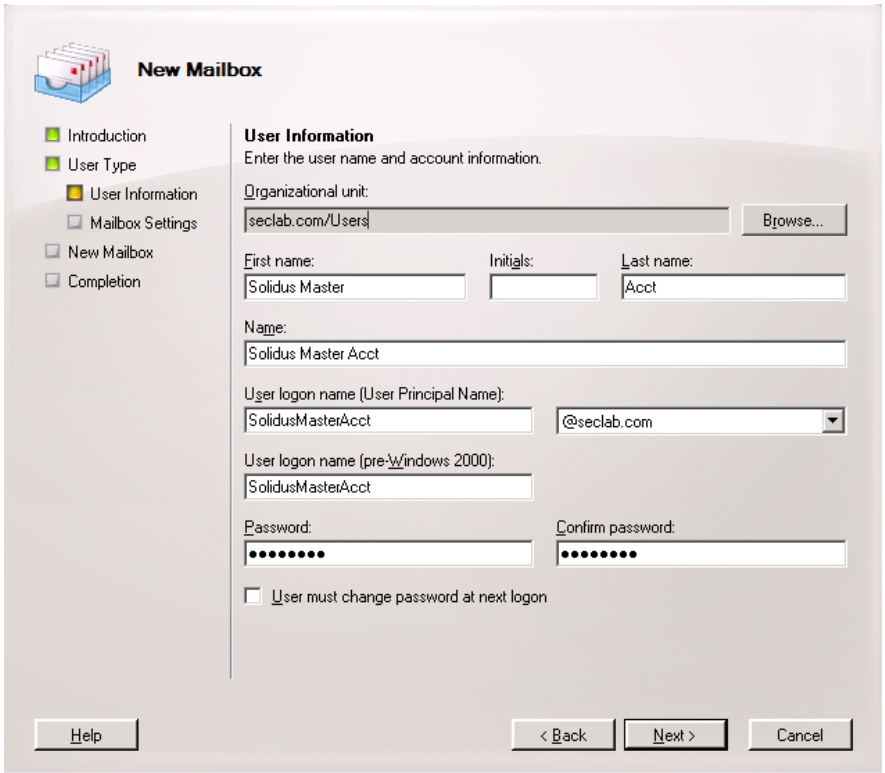
2. Right click on the **Recipient Configuration/Mailbox** node.
3. Select **New Mailbox**…



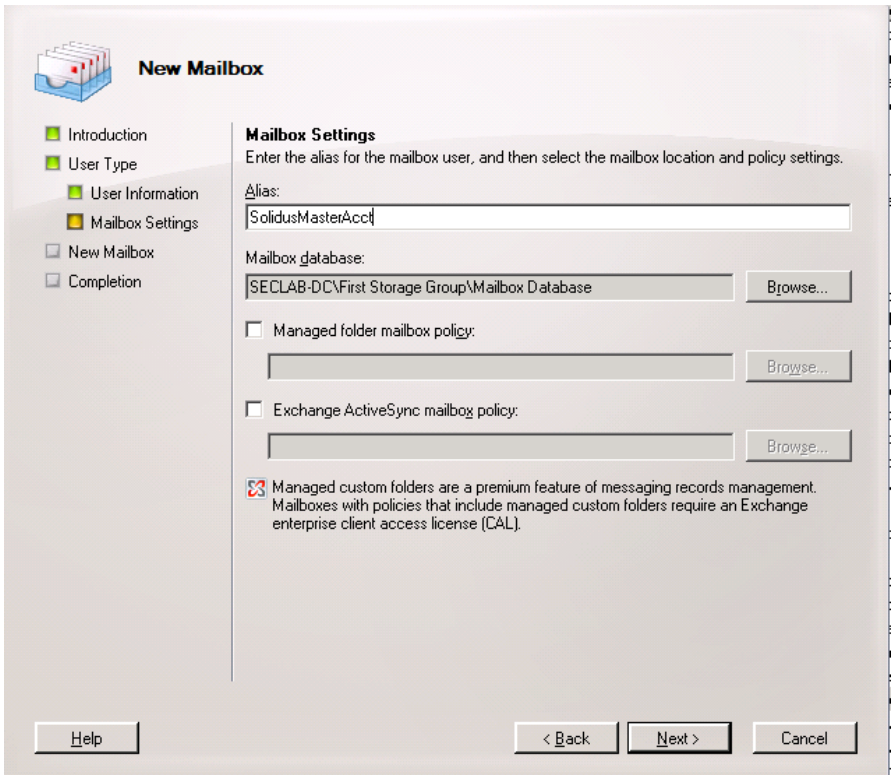
4. Choose **User Mailbox** and click Next.



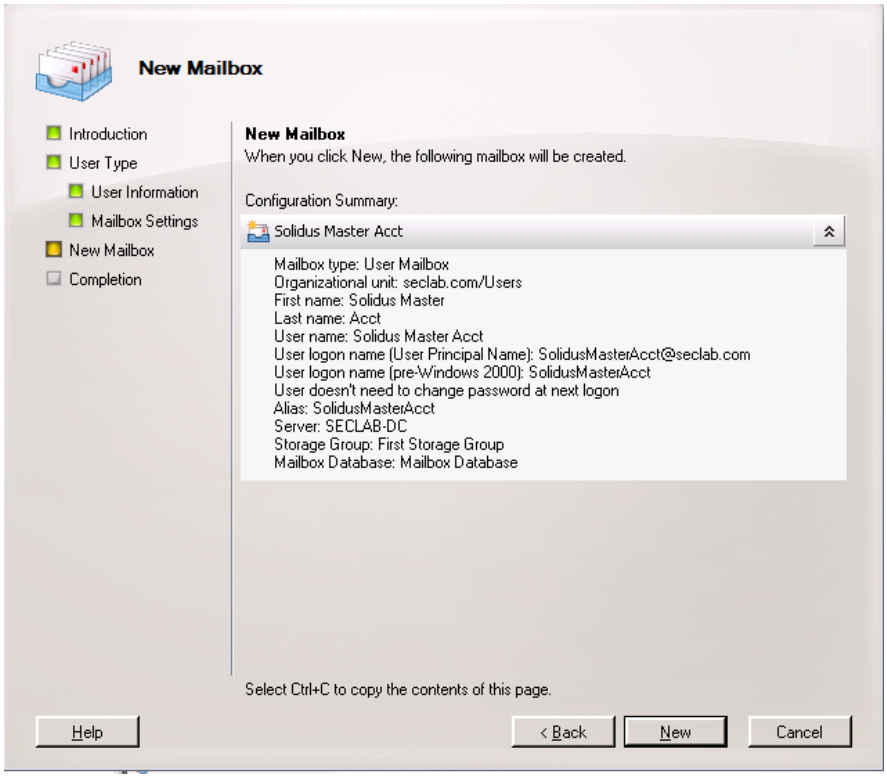
5. Select **New user** and click **Next**.



6. Enter the mailbox information and click **Next**. For the purpose of this instruction, the name of the account will be SolidusMasterAcct.



7. Contact your Exchange Administrator for the location of the Mailbox database. Click **Next**.

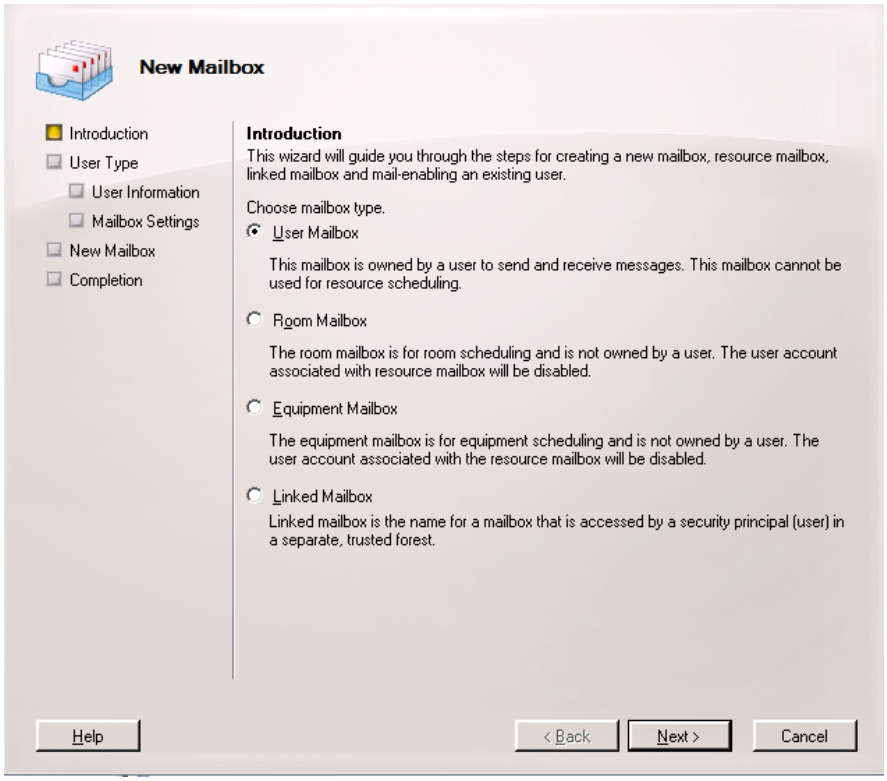


8. Verify the new mailbox settings and click **New** to create the mailbox.

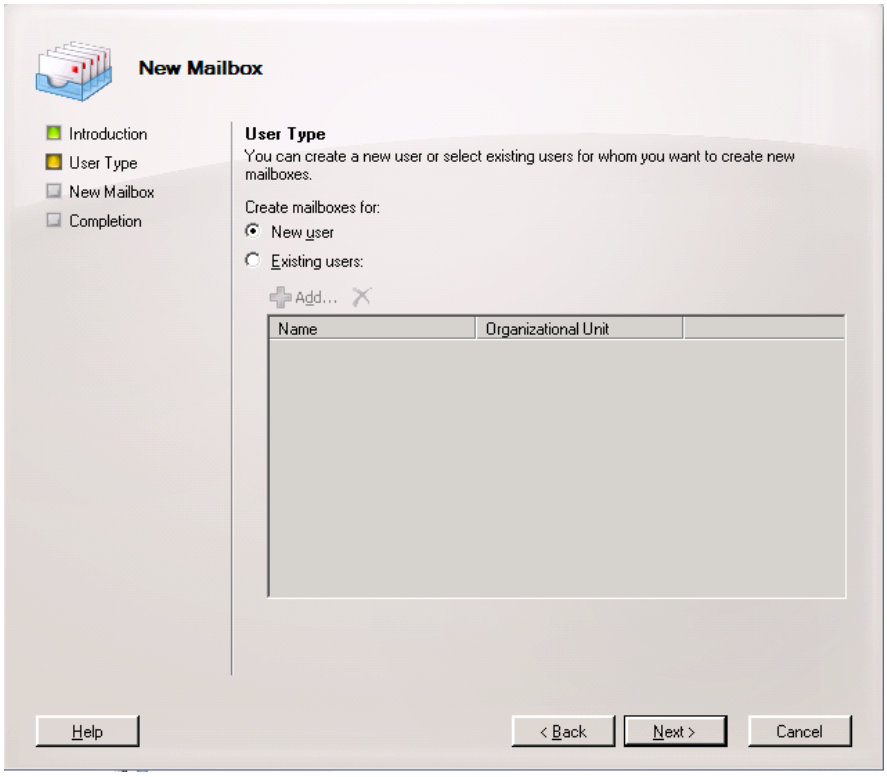
CREATE THE SERVICE ACCESS MAILBOX E-MAIL ACCOUNTS

For each service access that will be processing e-mails, create a user mailbox that will route e-mails to the master account.

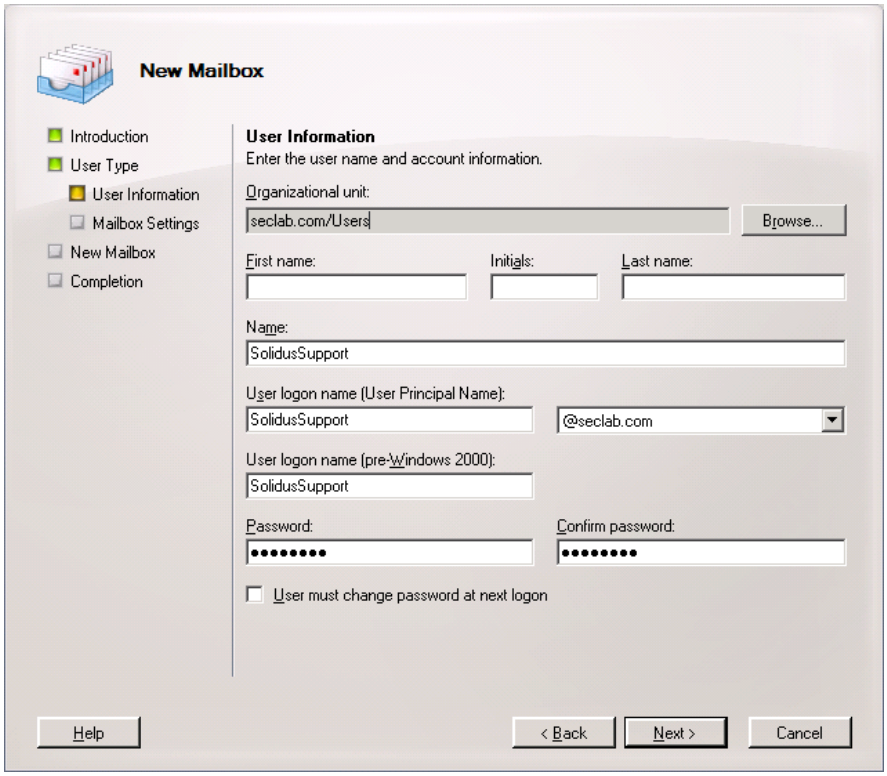
1. Launch the Exchange Management Console.
2. Right click on the **Recipient Configuration/Mailbox** node.
3. Select **New Mailbox**…



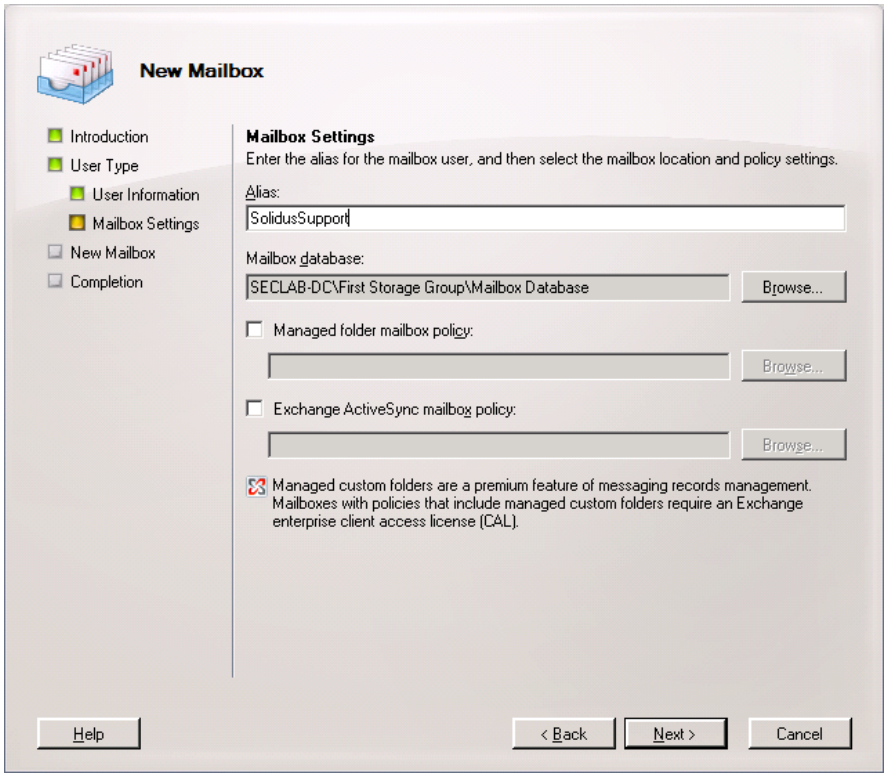
4. Choose **User Mailbox** and click Next.



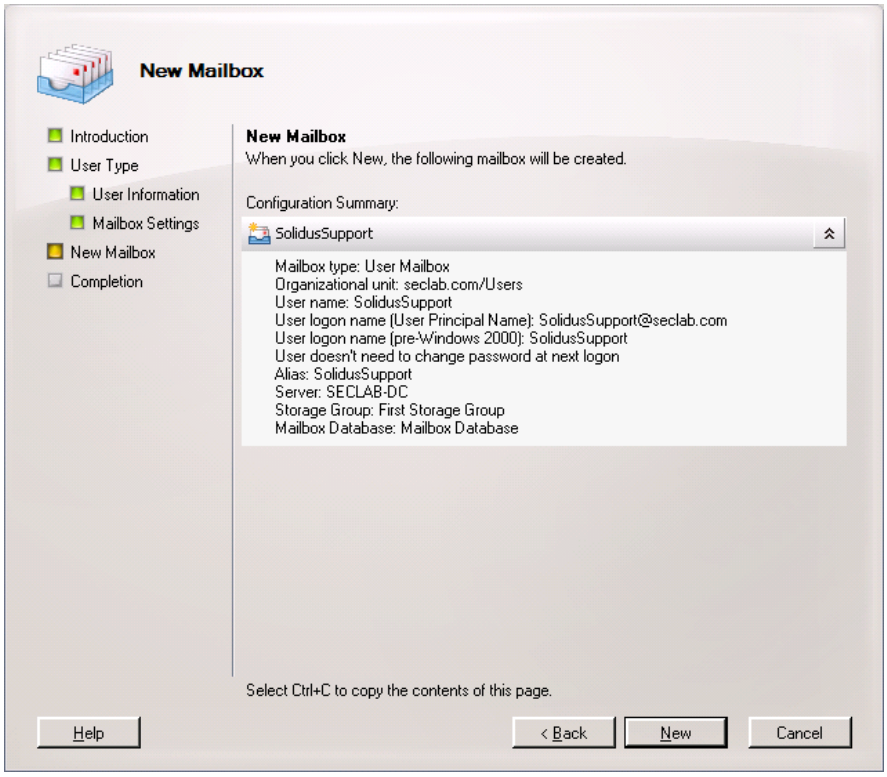
5. Select **New user** and click **Next**.



6. Enter the mailbox information and click **Next**. For the purpose of this instruction, the name of the account will be SolidusSupport.

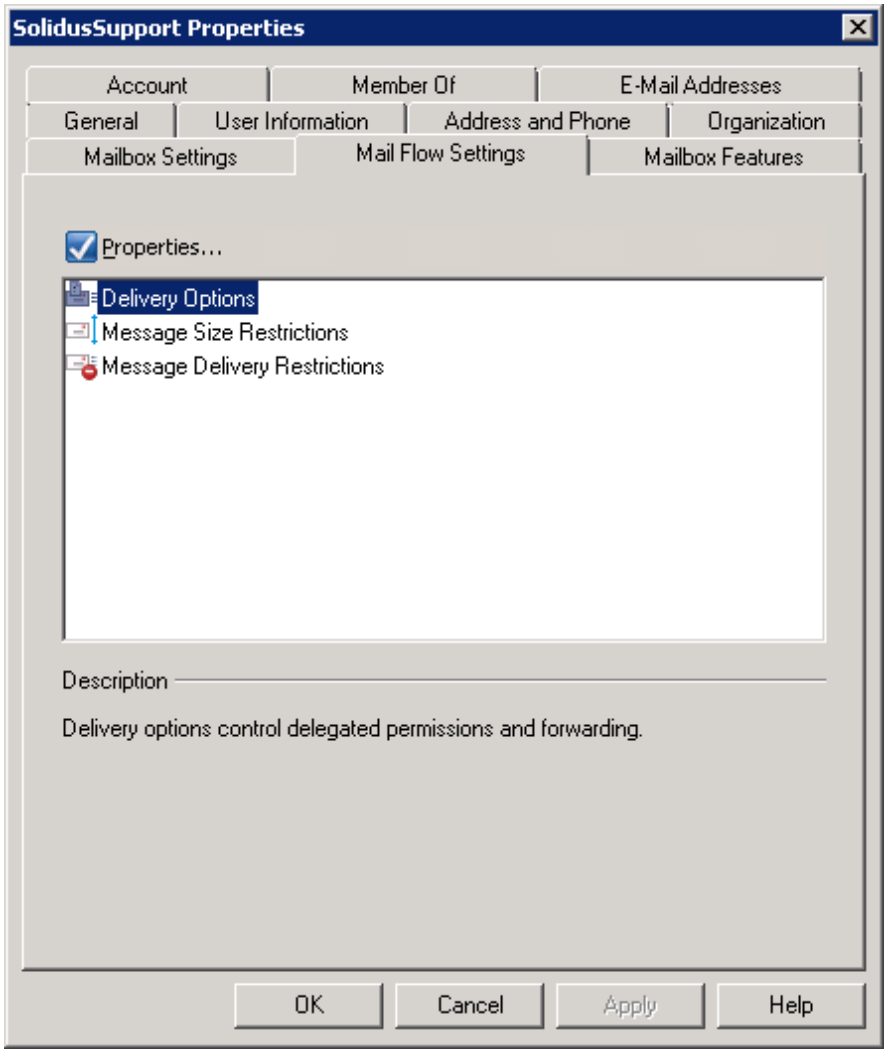


7. Contact your Exchange Administrator for the location of the Mailbox database. Click **Next**.

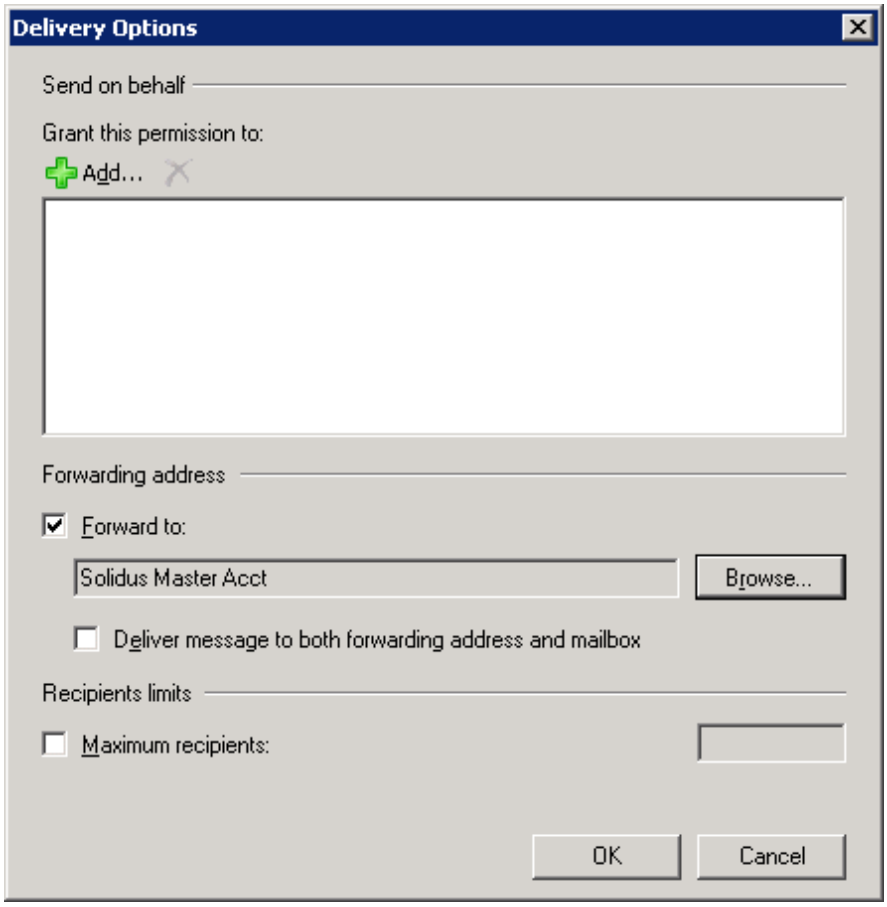


8. Verify the new mailbox settings and click **New** to create the mailbox.

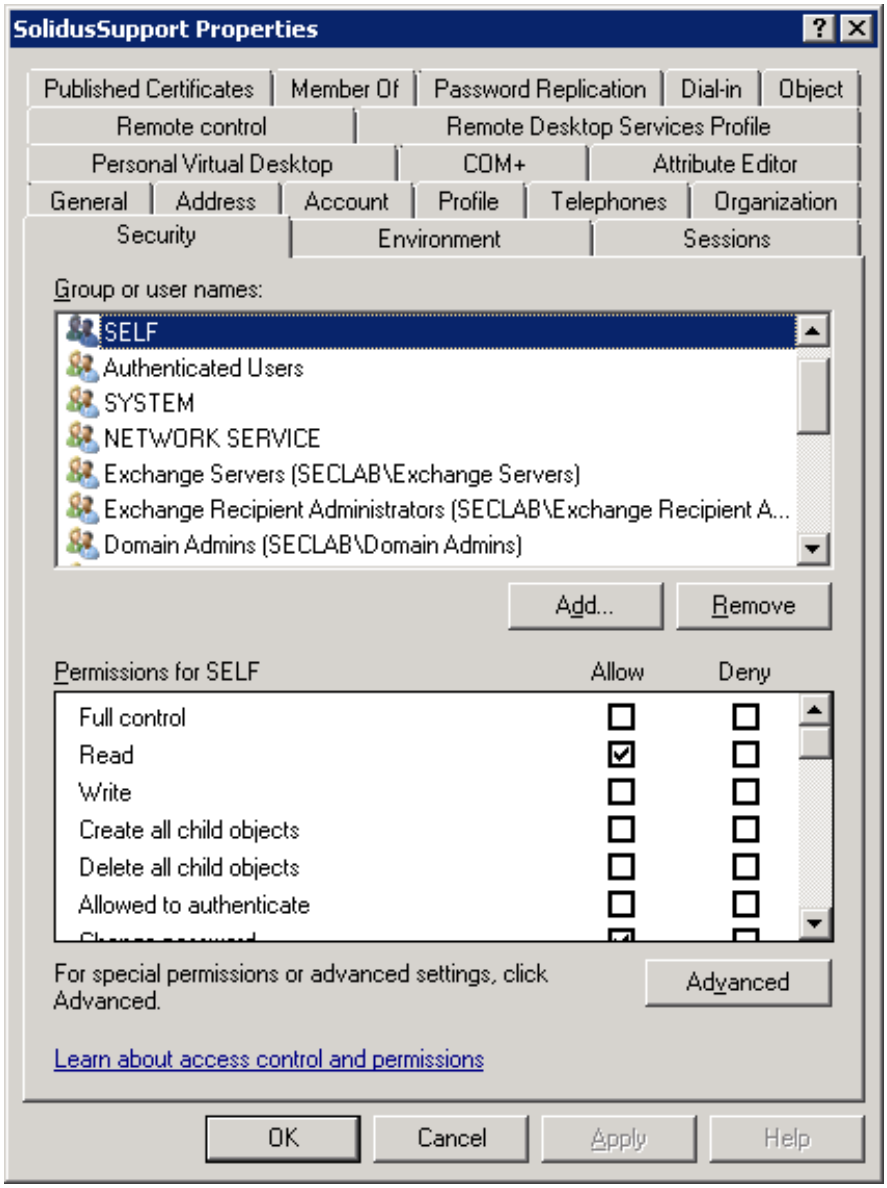
9. Locate the new mailbox under the **Recipient Configuration/Mailbox** node.
10. Right click on the mailbox and select **Properties**… Select the **Mail Flow Settings** tab.



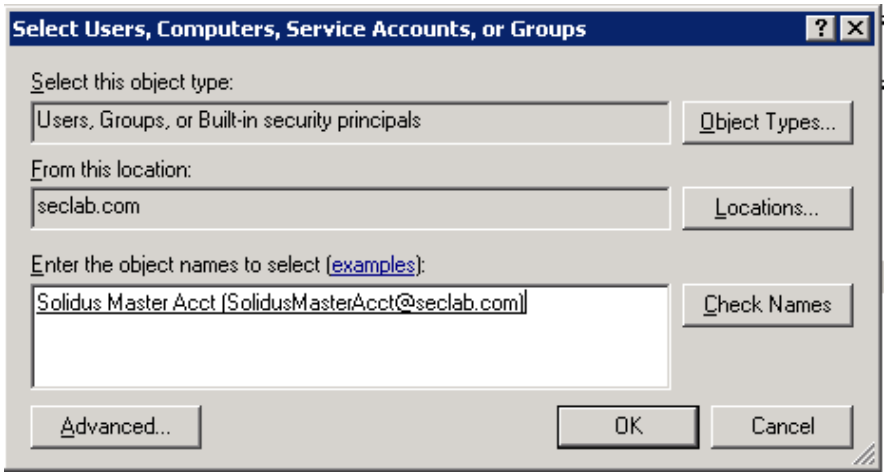
11. Select **Delivery Options** and click **Properties…**



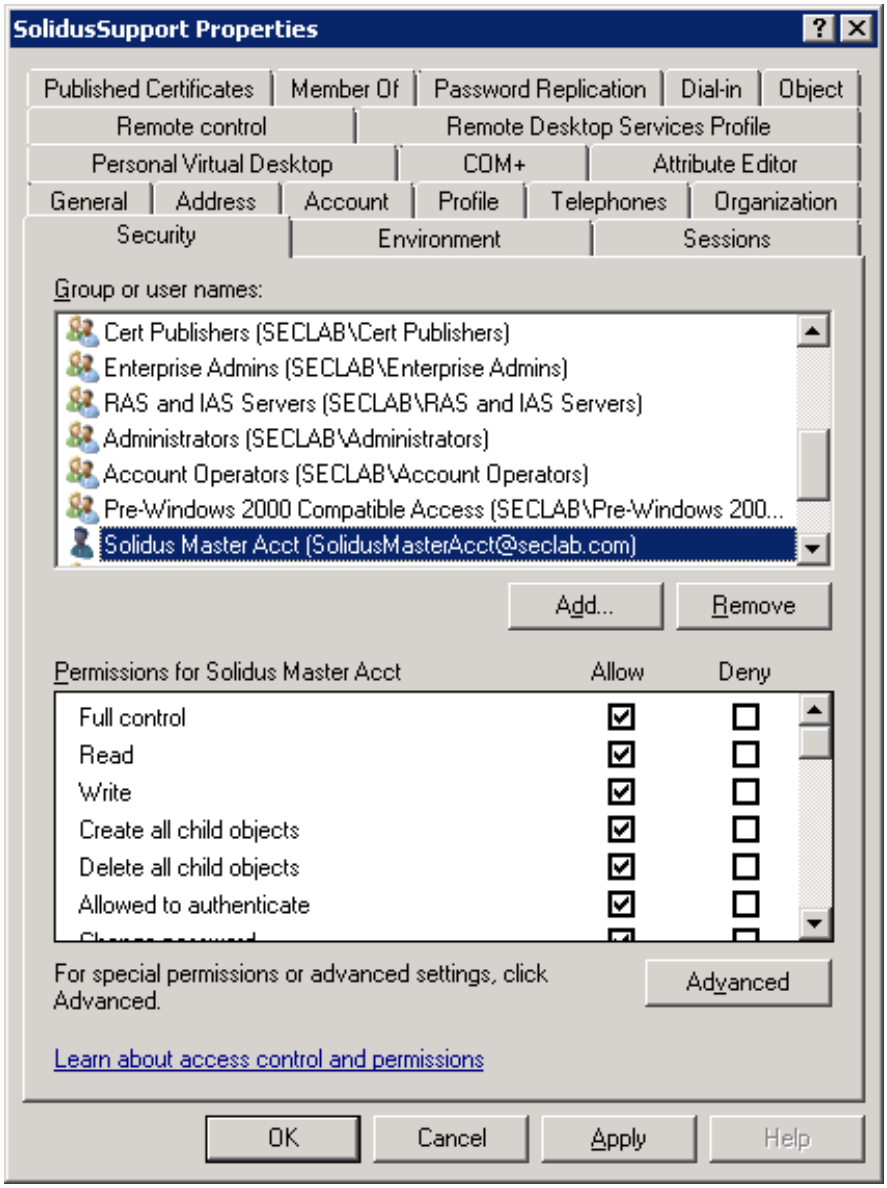
12. Check the **Forward to:** option. Choose the **Browse…** button and select the master account. The **Deliver message to both forwarding address and mailbox** should be unchecked.
13. Click **OK**.
14. Repeat steps 3 through 13 for all service access e-mail accounts.
15. Launch the **Active Directory Users and Computers** snap-in.
16. Select the **Users** node (or whatever the location is for the user mailboxes that you created).
17. For each service access e-mail account that you created, right click on the account and select **Properties**… Go to the **Security tab**.


SolidusSupport Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Remote control
Remote Desktop Services Profile
Personal Virtual Desktop
COM+
Attribute Editor
General
Address
Account
Profile
Telephones
Organization
Security
Environment
Sessions
Group or user names:
SELF
Authenticated Users
SYSTEM
NETWORK SERVICE
Exchange Servers (SECLAB\Exchange Servers)
Exchange Recipient Administrators (SECLAB\Exchange Recipient A...
Domain Admins (SECLAB\Domain Admins)
Add...
Remove
Permissions for SELF
Allow
Deny
Full control
Read
Write
Create all child objects
Delete all child objects
Allowed to authenticate
For special permissions or advanced settings, click Advanced.
Advanced
Learn about access control and permissions
OK
Cancel
Apply
Help

18. Click **Add**.



19. Enter the master account and click **OK**.



20. With the master account selected, click the Allow checkbox for the Full control permission.

21. Click OK to dismiss the Properties dialog.

22. Repeat steps 17 through 21 for each service access e-mail account.

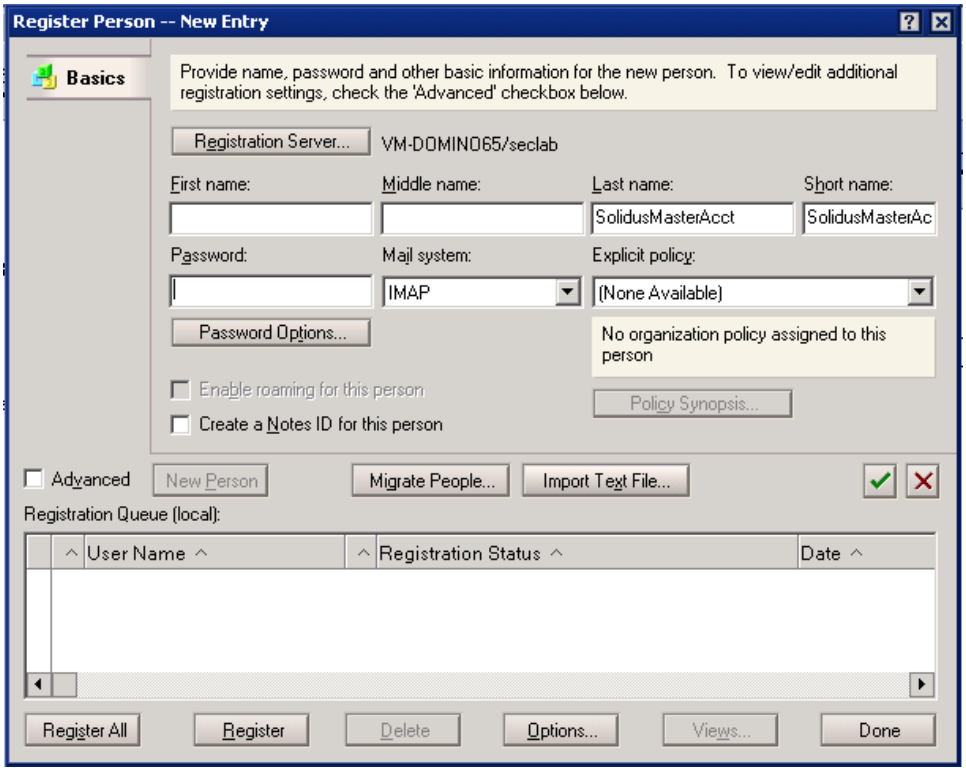
Note: This procedure slightly differs from previous versions of MiCC Enterprise. The recommended procedure in previous versions was to give Send on behalf permission to the master account. For upgrades, the existing setup may be maintained, however, “Send As” permission must be given to the master account from each user mailbox account.

LOTUS DOMINO 8.5

IMAP and SMTP must be enabled on the Domino server prior to setup. Contact the Domino Administrator for enabling these protocols.

CREATE THE MASTER MAILBOX E-MAIL ACCOUNT

1. Launch the Domino Administrator
2. Register a **New Person**.

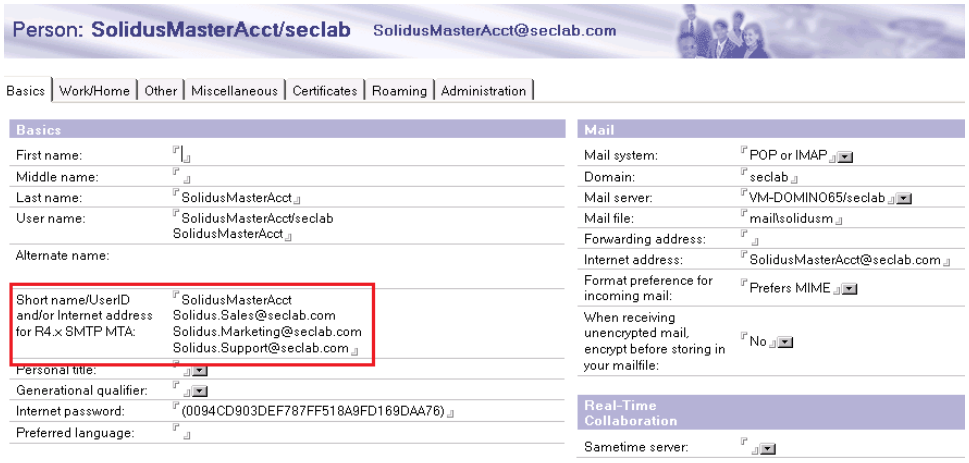


3. Enter the new account information. For the purpose of this instruction, the name of the account will be SolidusMasterAcct.
4. Set the **Mail system** to IMAP.
5. Uncheck **Create a Notes ID for this person**.
6. Complete the registration process.

ADD THE SERVICE ACCESS E-MAIL ADDRESSES

For each service access that will be processing e-mails, the e-mail address must be added to the list of addresses configured for the master account.

1. Launch the Domino Administrator.
2. Locate the master account Person.
3. Edit the Person.



4. Add the e-mail address to the **Short name/UserID and/or Internet Address** for each service access that will be processing e-mails.
5. Save the Person document.

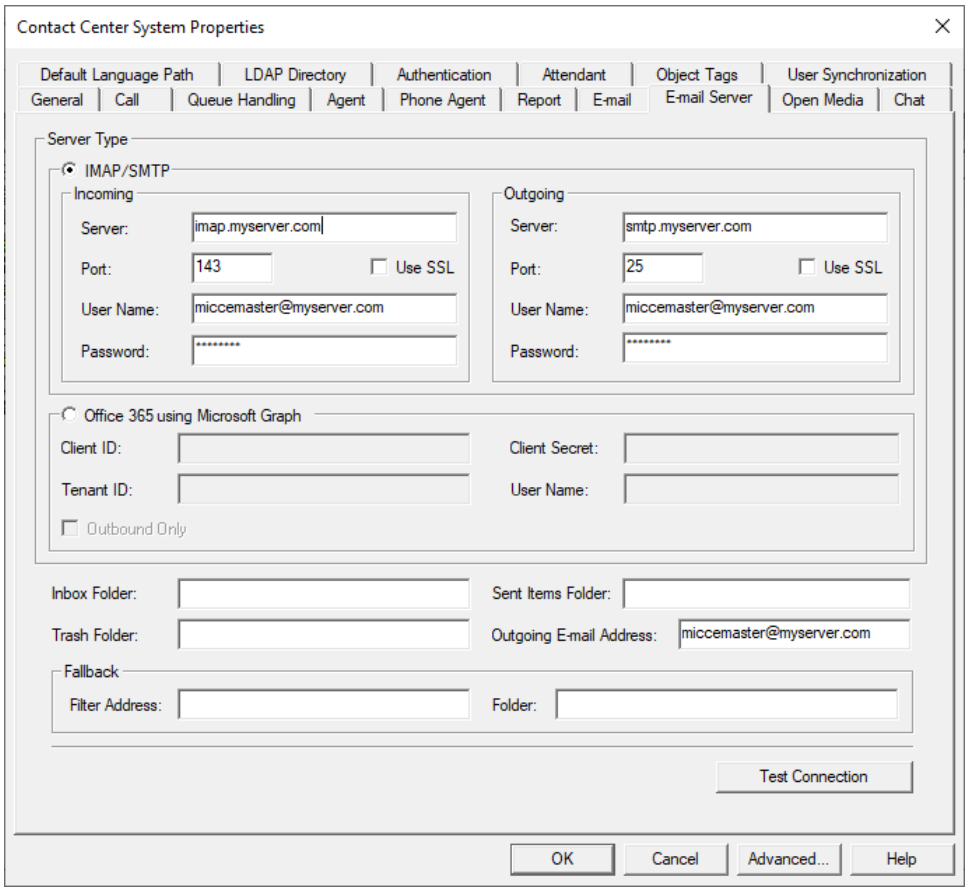
Note: This procedure differs from previous versions of MiCC Enterprise. The recommended procedure in previous versions was to create individual Person documents for the service group e-mail accounts. These accounts would forward their e-mails to the master mailbox. For upgrades, the existing setup may be maintained, but the master account must be changed to use IMAP for its mail system.

MICC ENTERPRISE E-MAIL CONFIGURATION

This section describes the basic setup of e-mail in MiCC Enterprise. For a more detailed description of the available e-mail options, refer to the Configuration Manager User's Guide.

CONNECTING TO THE E-MAIL SERVER

1. Launch the MiCC Enterprise Configuration Manager.
2. Open the System Properties for the desired tenant or system.
3. Switch to the E-mail Server tab.



4. Select IMAP/SMTP or Office 365 using Microsoft Graph.
5. Enter the master account connection information for the incoming (IMAP) and outgoing (SMTP) e-mail servers or the Office 365 Tenant ID, Client ID, Client Secret and master account User Name.
6. MiCC Enterprise attempts to automatically detect the Inbox, Sent Items and Trash folders using common names and attributes. If the folders cannot be detected such as them being localized in a specific language, they must be entered manually.
7. The outgoing E-mail Address is used in outgoing e-mail where a sender address might not be available. For example, e-mail notifications for generated reports.

8. The **Test Connection** button can be used to check the validity of the connection settings.

Note: If you do not wish to enable inbound e-mail routing to service accesses, you do not need to enter the connection information for the Incoming server. You may enter only the Outgoing server information for SMTP. For Office 365 using Microsoft Graph, check the Outbound Only option. This will allow functions such as the e-mail notifications for reports or sending new outgoing e-mails from agents.

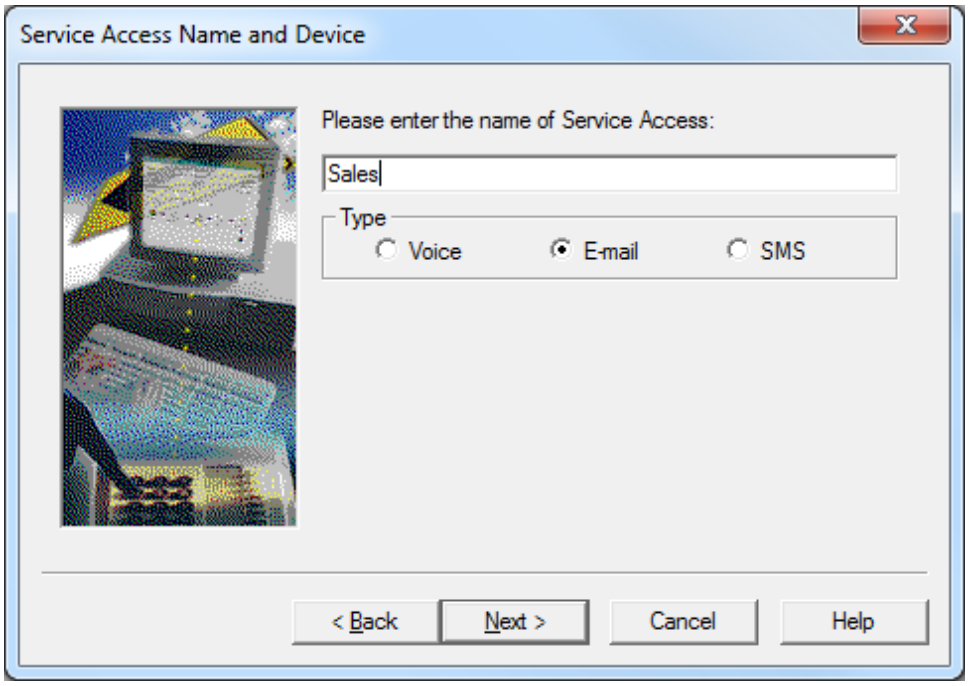
GMAIL CONNECTION SETTINGS

The following table lists the typical connection settings for Gmail. Refer to Gmail documentation if there are any issues using these settings.

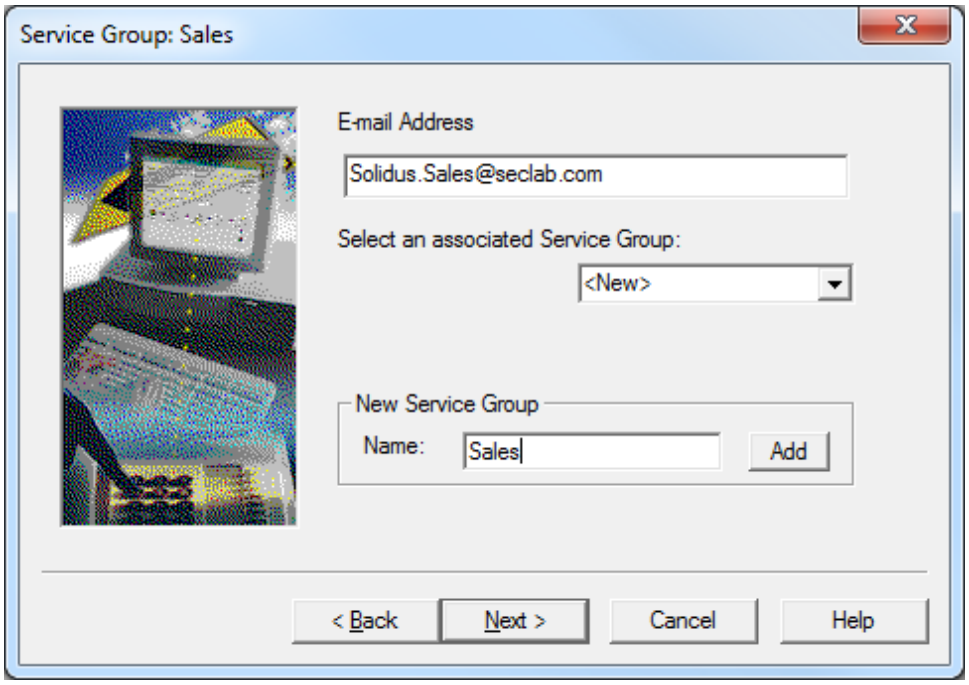
	SERVER	PORT	USE SSL
Incoming	imap.gmail.com	993	Yes
Outgoing	smtp.gmail.com	587	Yes

CREATE E-MAIL SERVICE ACCESSES

1. Launch the MiCC Enterprise Configuration Manager
2. Add a new Service Access.



3. Enter the name and set the type to E-mail. Click **Next**.



4. Enter the e-mail address of one of the service access e-mail accounts that was setup during the **E-mail Server Configuration** phase.

Note: Wildcards may be used for the e-mail address. For example, if you had 2 e-mail accounts with the address:

Solidus.Sales.Retail@seclab.com
Solidus.Sales.Commercial@seclab.com

You could enter:

Solidus.Sales.*@seclab.com

This would route all e-mails starting with Solidus.Sales.

If multiple Service Accesses are defined with the same e-mail address, they can be activated at the same time. However, e-mails will only be routed to the first Service Access activated. Caution should be exercised when defining e-mail addresses for Service Accesses to avoid overlapping e-mail addresses.

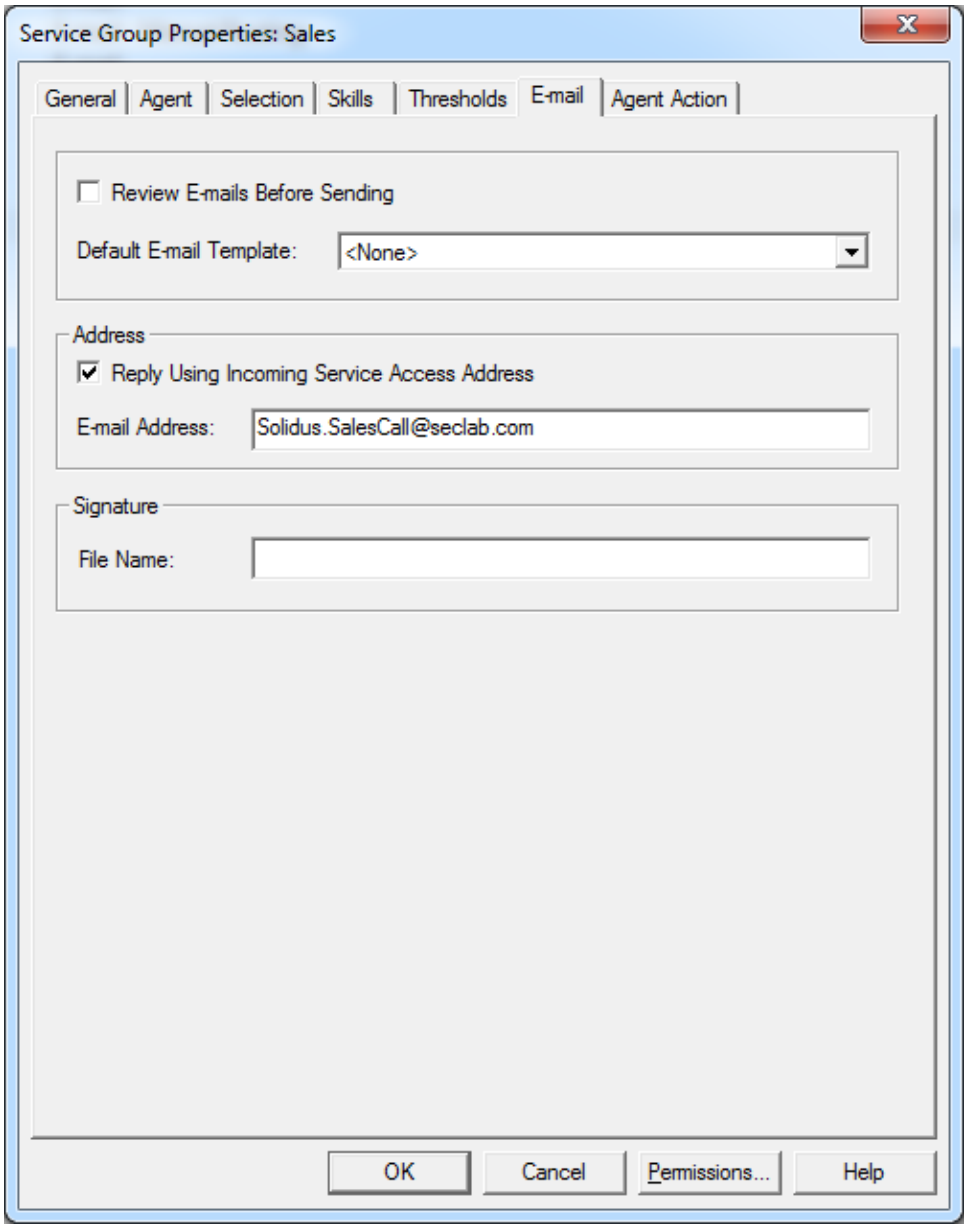
Note: If multiple Service Accesses are defined with the same e-mail address(es), they can be activated at the same time. However, e-mails will only be routed to the first Service Access activated. Caution should be exercised when defining e-mail addresses for Service Accesses to avoid overlapping e-mail addresses.

5. Select <New> for the associated Service Group and enter the Service Group name.
6. Click **Add** for the Service Group.
7. Complete the rest of the Service Access wizard.

SETUP OUTGOING E-MAIL SERVICE GROUPS

Service Groups may be used when routing e-mails to agents, but they may also be used when sending a new outgoing e-mail from MiContact Center Agent. Typically, when an agent responds to an e-mail, the e-mail will be sent using the e-mail address. You may override this address as well as setup the service group for new outgoing e-mail.

1. Launch the MiCC Enterprise Configuration Manager.
2. Create a new e-mail service group or modify an existing one.
3. Switch to the **E-mail** tab.



4. Specify the e-mail address. For new outgoing e-mails, this address will be used as the sender. Only service groups that have an address specified may be used for new outgoing

e-mails in MiContact Center Agent. If the Reply Using Incoming Service Access Address is unchecked, this address will be used when an agent replies to an incoming e-mail.

Note: The e-mail server must be capable of sending an e-mail using this address from the master account. This may require setting up another account on the e-mail server and associating it to the master account.

E-MAIL TEMPLATES

E-mail templates may be created for use as default incoming and outgoing messages as well as automatic e-mail confirmations and service group or agent signatures. The templates may be standard text based files (*.txt) or html format files (*.htm, *.html). The files may contain placeholders which will be replaced by data associated to the incoming or outgoing e-mail.

It is important to ensure that replaceable identifiers are entered in a continuous string in the template files. HTML editors such as Microsoft Word may split the text while inserting HTML format tags. This will prevent the identifiers from being replaced. This may occur if text is identified as a misspelled word. The underlining used in Microsoft Word to indicate the misspelled word will be stored in the HTML file as formatting information. Always ensure that replaceable identifiers are ignored for spell checking.

SMS messages may also use the defined e-mail templates. SMS messages do not support rich text. They can use the same HTML templates; however, the template will be converted to plain text.

Replaceable Identifiers

IDENTIFIER	REPLACEMENT
$Subject$	E-mail subject
$From$	Sender name and e-mail address. For example, John Smith (john.smith@company.com)
$From.Name$	Sender name
$From.Address$	Sender e-mail address
$Date$	Current date formatted using the short date format of the current locale
$Time$	Current time formatted using the short time format of the current locale
$Received$	Date and time the e-mail was received formatted using the short date and short time formats of the current locale
$Received.Date$	Date the e-mail was received formatted using the short date format of the current locale
$Received.Time$	Time the e-mail was received formatted using the short time format of the current locale
$ServiceAccess$	Service access name

$ServiceAccess.Name$	Service access name
$ServiceGroup$	Service group name
$ServiceGroup.Name$	Service group name
$ServiceGroup.Email$	Service group e-mail address
$Agent$	Agent name
$Agent.Name$	Agent name
$Agent.FirstName$	Agent first name, if defined
$Agent.LastName$	Agent last name, if defined
$Agent.ChatName$	Agent Chat Display Name, if defined. Otherwise, set to agent name.
$Customer$	Customer name (applicable when e-mail is associated with a Chat session or incoming voice call)
$Customer.Name$	Customer name (applicable when e-mail is associated with a Chat session or incoming voice call)
$Customer.Email$	Customer e-mail address (applicable when e-mail is associated with a Chat session)
$Customer.ID$	Identifier associated with customer (applicable when e-mail is associated with a Chat session)
$Customer.Number$	Phone number associated with customer (applicable when e-mail is associated with an incoming voice call and Attendant E-mail feature is invoked)
$CallID$	Internal call ID.

Note: Identifiers may not be applicable in all cases. For example, for a new outgoing e-mail, the $Received$ identifier will not be available. Identifiers that do not apply will be replaced by an empty string.

Example Automatic E-mail Confirmation in Text Format:

$Date$ $Time$

Dear $From.Name$,

Thank you for contacting $ServiceAccess.Name$. We will contact you as soon as possible.

Example Automatic E-mail Confirmation in Html Format:

```
<HTML>
<BODY>
<B>$Date$ $Time$</B><BR/><BR/>
Dear $From.Name$,<BR/><BR/>
Thank you for contacting $ServiceAccess.Name$. We will contact you as soon as possible.
</BODY>
</HTML>
```

SPELL CHECKING IN MICONTACT CENTER AGENT

MiCC Enterprise ships with only the English language dictionary for spell checking. Additional languages may be installed by placing the language dictionaries on the MiCC Enterprise server. Language dictionaries must be in Open Office format.

Language dictionaries are located on the MiCC Enterprise server under the following directory:

<InstallDir>\Services\Spelling

Each language is placed in a subfolder with the name of the culture. For example, the name for U.S. English is en-US. See table **Culture Names** for a list of culture names. Two files are required; A dictionary file named Dictionary.dic and a grammar file named Grammar.aff.

Dictionaries may be downloaded from http://extensions.openoffice.org/ in the form of an Open Office Extension. These extensions have an oxt file extension, however, they are standard ZIP compressed files.

1. Create subfolder with the name of the culture under Spelling.

2. Download extension from Open Office.

3. Rename file to a zip extension.

4. Open zip file and extract dic and aff files to culture folder. Some extensions may contain multiple dic or aff files. The typical naming convention for the main files in the extensions is the name of the culture. For example, the Spanish extension contains the files es_ES.dic and es_ES.aff.

5. Rename the *.dic and *.aff files to Dictionary.dic and Grammar.aff.

No additional configuration in MiCC Enterprise is necessary. When MiContact Center Agent runs, it queries the server for language dictionaries under the Spelling folder. If additional dictionaries are present, they will be downloaded to the client.

Note: Mitel is not responsible for the content of language dictionaries. Any omissions or incorrect entries are solely the responsibility of the MiCC Enterprise user.

Culture Names

CULTURE NAME	LANGUAGE
af-ZA	Afrikaans - South Africa
sq-AL	Albanian - Albania
ar-DZ	Arabic - Algeria
ar-BH	Arabic - Bahrain
ar-EG	Arabic - Egypt
ar-IQ	Arabic - Iraq
ar-JO	Arabic - Jordan
ar-KW	Arabic - Kuwait
ar-LB	Arabic - Lebanon
ar-LY	Arabic - Libya
ar-MA	Arabic - Morocco
ar-OM	Arabic - Oman
ar-QA	Arabic - Qatar
ar-SA	Arabic - Saudi Arabia
ar-SY	Arabic - Syria
ar-TN	Arabic - Tunisia
ar-AE	Arabic - United Arab Emirates
ar-YE	Arabic - Yemen
hy-AM	Armenian - Armenia
Cy-az-AZ	Azeri (Cyrillic) - Azerbaijan
Lt-az-AZ	Azeri (Latin) - Azerbaijan
eu-ES	Basque - Basque
be-BY	Belarusian - Belarus
bg-BG	Bulgarian - Bulgaria
ca-ES	Catalan - Catalan
zh-CN	Chinese - China

zh-HK	Chinese - Hong Kong SAR
zh-MO	Chinese - Macau SAR
zh-SG	Chinese - Singapore
zh-TW	Chinese - Taiwan
zh-CHS	Chinese (Simplified)
zh-CHT	Chinese (Traditional)
hr-HR	Croatian - Croatia
cs-CZ	Czech - Czech Republic
da-DK	Danish - Denmark
div-MV	Dhivehi - Maldives
nl-BE	Dutch - Belgium
nl-NL	Dutch - The Netherlands
en-AU	English - Australia
en-BZ	English - Belize
en-CA	English - Canada
en-CB	English - Caribbean
en-IE	English - Ireland
en-JM	English - Jamaica
en-NZ	English - New Zealand
en-PH	English - Philippines
en-ZA	English - South Africa
en-TT	English - Trinidad and Tobago
en-GB	English - United Kingdom
en-US	English - United States
en-ZW	English - Zimbabwe
et-EE	Estonian - Estonia
fo-FO	Faroese - Faroe Islands
fa-IR	Farsi - Iran
fi-FI	Finnish - Finland

fr-BE	French - Belgium
fr-CA	French - Canada
fr-FR	French - France
fr-LU	French - Luxembourg
fr-MC	French - Monaco
fr-CH	French - Switzerland
gl-ES	Galician - Galician
ka-GE	Georgian - Georgia
de-AT	German - Austria
de-DE	German - Germany
de-LI	German - Liechtenstein
de-LU	German - Luxembourg
de-CH	German - Switzerland
el-GR	Greek - Greece
gu-IN	Gujarati - India
he-IL	Hebrew - Israel
hi-IN	Hindi - India
hu-HU	Hungarian - Hungary
is-IS	Icelandic - Iceland
id-ID	Indonesian - Indonesia
it-IT	Italian - Italy
it-CH	Italian - Switzerland
ja-JP	Japanese - Japan
kn-IN	Kannada - India
kk-KZ	Kazakh - Kazakhstan
kok-IN	Konkani - India
ko-KR	Korean - Korea
ky-KZ	Kyrgyz - Kazakhstan
lv-LV	Latvian - Latvia

lt-LT	Lithuanian - Lithuania
mk-MK	Macedonian (FYROM)
ms-BN	Malay - Brunei
ms-MY	Malay - Malaysia
mr-IN	Marathi - India
mn-MN	Mongolian - Mongolia
nb-NO	Norwegian (Bokmål) - Norway
nn-NO	Norwegian (Nynorsk) - Norway
pl-PL	Polish - Poland
pt-BR	Portuguese - Brazil
pt-PT	Portuguese - Portugal
pa-IN	Punjabi - India
ro-RO	Romanian - Romania
ru-RU	Russian - Russia
sa-IN	Sanskrit - India
Cy-sr-SP	Serbian (Cyrillic) - Serbia
Lt-sr-SP	Serbian (Latin) - Serbia
sk-SK	Slovak - Slovakia
sl-SI	Slovenian - Slovenia
es-AR	Spanish - Argentina
es-BO	Spanish - Bolivia
es-CL	Spanish - Chile
es-CO	Spanish - Colombia
es-CR	Spanish - Costa Rica
es-DO	Spanish - Dominican Republic
es-EC	Spanish - Ecuador
es-SV	Spanish - El Salvador
es-GT	Spanish - Guatemala
es-HN	Spanish - Honduras

es-MX	Spanish - Mexico
es-NI	Spanish - Nicaragua
es-PA	Spanish - Panama
es-PY	Spanish - Paraguay
es-PE	Spanish - Peru
es-PR	Spanish - Puerto Rico
es-ES	Spanish - Spain
es-UY	Spanish - Uruguay
es-VE	Spanish - Venezuela
sw-KE	Swahili - Kenya
sv-FI	Swedish - Finland
sv-SE	Swedish - Sweden
syr-SY	Syriac - Syria
ta-IN	Tamil - India
tt-RU	Tatar - Russia
te-IN	Telugu - India
th-TH	Thai - Thailand
tr-TR	Turkish - Turkey
uk-UA	Ukrainian - Ukraine
ur-PK	Urdu - Pakistan
Cy-uz-UZ	Uzbek (Cyrillic) - Uzbekistan
Lt-uz-UZ	Uzbek (Latin) - Uzbekistan
vi-VN	Vietnamese - Vietnam
ar-YE	Arabic - Yemen

E-MAIL RESPONSES

A response file may be setup for each service group allowing the agents to select predefined messages to be inserted into e-mail replies. If a response file is configured, a hierarchal list of the responses is displayed in the agent e-mail form. Refer to the section on E-mail, Chat and SMS Response Files in the document **3_1543-LXA119154 – Advanced Configurations** for the response file format.

ARCHIVE CONSIDERATIONS

E-mails that are sent and received may be archived to the MiCC Enterprise database for retrieval at a later time. Due to the different languages that may be contained in e-mail subjects and bodies, the content may not be archived correctly depending on the SQL collation set for the MiCC Enterprise database. The collation of the database is set during creation and uses the collation set for the SQL server. This collation may not support all of the characters contained in the e-mail subject or body. If this situation arises, it may be necessary to manually change the collation or column type of specific table columns in the MiCC Enterprise database.

COLLATION CHANGE

The collation may be changed to support most characters. A collation should be chosen that will support the most possible characters that may be received or sent in an e-mail subject or body. The following table lists possible collations supported by SQL Server.

SQL Collations

LANGUAGE	COLLATION
Albanian	Albanian_CI_AS
Arabic (Saudi Arabia)	Arabic_CI_AS
Chinese (PRC)	Chinese_PRC_CI_AS
Chinese (PRC)	Chinese_PRC_Stroke_CI_AS
Chinese (Taiwan)	Chinese_Taiwan_Bopomofo_CI_AS
Chinese (Taiwan)	Chinese_Taiwan_Stroke_CI_AS
Croatian	Croatian_CI_AS
Russian	Cyrillic_General_CI_AS
Czech	Czech_CI_AS
Danish	Danish_Norwegian_CI_AS
Estonian	Estonian_CI_AS
Finnish	Finnish_Swedish_CI_AS
French (France)	French_CI_AS
German (Phone Book Sort)	German_PhoneBook_CI_AS
Greek	Greek_CI_AS
Hebrew	Hebrew_CI_AS

Hungarian	Hungarian_CI_AS
Hungarian (Technical)	Hungarian_Technical_CI_AS
Icelandic	Icelandic_CI_AS
Japanese	Japanese_CI_AS
Korean (Extended Wansung)	Korean_Wansung_CI_AS
Galacian (English – U.S.A)	Latin1_General_CI_AS
Latvian	Latvian_CI_AS
Lithuanian	Lithuanian_CI_AS
Spanish (International Sort)	Modern_Spanish_CI_AS
Polish	Polish_CI_AS
Romanian	Romanian_CI_AS
Slovak	Slovak_CI_AS
Slovenian	Slovenian_CI_AS
Thai	Thai_CI_AS
Spanish (Traditional Sort)	Traditional_Spanish_CI_AS
Turkish	Turkish_CI_AS
Ukrainian	Ukrainian_CI_AS
Vietnamese	Vietnamese_CI_AS

Once a collation is chosen, some SQL commands must be issued to SQL Server to change the affected columns. Open SQL Server Management Studio and execute the following commands on the nextccdb database. Replace <Collation Name> with the name of the collation chosen.

DROP INDEX IDX_email_archive_subject ON email_archive
ALTER TABLE email_archive ALTER COLUMN subject varchar(255) COLLATE <Collation Name> NOT NULL
ALTER TABLE email_archive ALTER COLUMN body varchar(max) COLLATE <Collation Name> NULL
CREATE INDEX IDX_email_archive_subject ON email_archive(subject) ON [PRIMARY]

COLUMN TYPE CHANGE

Changing the type of the column rather than setting the collation has the benefit of supporting all characters; however, the space required for the columns will be double that of the standard definition. If the number of e-mails archived is relatively small, it is better to change the type of the column rather than the collation. To change the type of the column to support all characters,

open SQL Server Management Studio and execute the following commands on the nextccdb database.

```
DROP INDEX IDX_email_archive_subject ON email_archive
ALTER TABLE email_archive ALTER COLUMN subject nvarchar(255) NOT NULL
ALTER TABLE email_archive ALTER COLUMN body nvarchar(max) NULL
CREATE INDEX IDX_email_archive_subject ON email_archive(subject) ON [PRIMARY]
```