

Permissions Summary for Exchange Self Service Admins

Exchange self service admins are delegated permissions to perform many common Exchange related tasks. Microsoft has not made it easy for us to delegate permissions so that admins can do the work they need to do, but not more than that. These permissions are assigned through four separate mechanisms.

- Accounts OU Permissions as an OU Admin

OU Admins have certain permissions by virtue of being a Central Accounts OU Admin, which gives them the ability to change various attributes of unique user objects that have been moved to their accounts OU. We have taken the approach of allowing all attributes to be changed with the exception of a small number of attributes that can't be changed. The list of locked attributes was decided upon when changing an attribute could adversely affect the user to access other resources on campus or conflict with an automatically updated attribute such as unique. The complete list of those attributes that can't be changed are listed at the following URL: <http://www.umich.edu/~lannos/windows/central-accounts-attributes.html>.

ITCS has created for LSA an lsa-ouadmins groups that has permissions over the entire LSA Accounts OU structure and a number of lsa-dept-ouadmins groups that have control over their sub-ous.

- Organizations OU Admin

As an OU Admin, self service admins can create and delete user objects in their Organizations OU for creating department and resource mailboxes. OU Admins have full control over ALL the user attributes of these users.

ITCS has created for LSA an lsa-ouadmins groups that has permissions over the entire LSA Accounts OU structure. Further delegation of sub-Ous is done by LSAIT.

- Exchange Self Service Admins

In addition to the regular delegated OU Admin permissions granted, Exchange Self Service Admins are added to a special group that grants them the "Exchange View Only Admin" permission for the ITCS backend Exchange servers. The ability to create/delete mailboxes and mail enable groups comes from a combination of this permissions and the user object permissions above.

Who in LSA should be added to this group? Just lsa-ouadmins, other lsa-dept-ouadmins?

- Exchange Full Admins

Some individual admins have been granted "Exchange Full Admin" permissions over the entire Exchange system that allows them to make major changes to Exchange systems in ITCS, LSA, Engin, Bus, etc. These individuals are members of the Exchange Cartel. They are highly trained and skilled and have been limited to the primary Exchange server admins in the various departments. Paul Napolitano from LSA and 5 other members on campus are currently members of this group. This will allow him to perform more Exchange tasks than other LSA Exchange Self Service Admins. It has not been decided whether Paul will stay a member of this group once LSA has fully migrated from their Exchange servers. It is very unlikely this permission would be granted to others in LSA or any other department for that matter. No other self service admins currently have this permission.

The following is a list of specific Exchange tasks, who can perform them, where their permissions derive from and comments about why they can or can't perform the task.

Permissions Summary for Exchange Self Service Admins

Create and Delete Mailboxes for Uniqname Users - Self Service Admins - Yes

Mailboxes can be created and deleted for uniqname users that have been moved into the Admin's Accounts OU using the Central Accounts web site. Mailboxes can only be created in designated mailbox stores on the various ITCS Exchange servers. Admins have the choice of creating mailboxes in mailstores with 400MB or 2GB quotas. These permissions are derived from the first and second set of permissions above.

Comments: The available mailstores will change from time to time in order to help spread users equally across all mailstores. Only designated mailbox stores are visible to self service admins. An Exchange self service admin will not be able to delete a mailbox in a mailstore that was once available to them for creating mailboxes and has since been removed from the list. In this case the self service admin needs to contact Exchange Support who will either delete the mailbox or grant the needed permissions.

Permissions derived from: Accounts OU Admin, Exchange Self Service Admin

Create and Delete Mailboxes for Department and Resource mailboxes- Self Service Admins - Yes

Mailboxes can be created and deleted for department and resources users (helpdesk, conference room, etc.) by creating user objects within their Organizations OU. Mailboxes can only be created and deleted in the same way as Uniqname users.

Comments: Same as Uniqname users above. Admins must follow user object naming conventions that prefix their Account names and Display Names with agreed upon prefixes. For example, user objects in LSA must be of the form, "lsa-userobjectname". Calendar Resource user objects must be created in an OU named "Calendar Resources" in order to not be billed for that mailbox.

Permissions derived from: Organizations OU Admin, Exchange Self Service Admin

Moving Mailboxes between Mail Stores - Self Service Admins - No, Exchange Full Admin - Yes

Self service admins do not have the ability to move mailboxes between mailstores and will need to contact Exchange Support for this task. This includes moving them between mailstores to change their quota. The reason for this is that moving a mailbox requires granting complete access to entire Exchange servers.

Comments: Paul Napolitano currently has Exchange Full Admin permissions and can perform mailbox moves between LSA servers and ITCS servers to facilitate the migration. This also gives him the ability to move mailboxes between ITCS mailstores to change basic quotas.

Permissions derived from: Exchange Full Admin only

Change Passwords on Uniqname, Department and Calendar Resources user accounts - Self Service Admins - yes

Passwords can be changed by admins with the regular AD tools for both Uniqname user accounts they manage in their Accounts OU or for Department/Calendar user accounts they create in their Organizations OU.

Permissions Summary for Exchange Self Service Admins

Comments: Users can change the password for their unqname by authenticating to an ITCS provided password change web page with their UM-Kerberos credentials and then changing their Windows password.

Permissions derived from: Accounts OU Admin, Organizations OU Admin

Creating Mail Enabled Groups - Self Service Admins - Yes

Self service admins can create security or distribution groups in their Organizations OU and then choose to mail enable them.

Comments: Admins must follow group naming conventions that prefix their Group Display Names with agreed upon prefixes. For example all groups in LSA must have the form "lsa-groupname" or "LSA Group Name".

Permissions derived from: Organizations OU Admin, Exchange Self Service Admin

Display Names for Uniqnames- Self Service Admins - Yes

Self service admins have the ability to change Display Names for user objects in their Accounts OU. The Display Name attribute for users is the name that appears in the Exchange Global Address List and is in the form "LastName, FirstName". This name is initially set when the account is created the UMOD directory, but is not updated as other attributes in order to allow self service admins to change it if needed.

Comments: Admins must follow naming convention rules for Display Names. Names must remain in the "LastName, FirstName" format. Only the First Name should be changed in the case where the person is know by another name (Tony vs. Anthony). If a user has marked their UMOD entry as private, the Exchange Display Name will only be their unqname. Self Service Admins may change this to the "LastName, FirstName" format, but need to inform the user about the change and receive their permisison to publish their full name.

Permissions derived from: Accounts OU Admin

Display Names for Department and Resource mailboxes- Self Service Admins - Yes

Comments: Follow naming conventions for creating these objects

Permissions derived from: Organizations OU Admin

Disable or limit logons to Uniqname User Accounts - Self Service Admins - No, ITCS Exchange Admins - Yes

Self service admins are not able to change most options on the Accounts tab of a unqname user object in the Accounts OU. This includes the following permissions that are not set and can't be changed unless noted below.

- Disable Account
- Restrict logon hours
- Restrict logon workstation (except to add to a group that is allowed logons to certain computers)
- Expire Accounts
- Password Never Expires (this is set and can't be changed)
- Require Smartcard for Interactive Logon

Permissions Summary for Exchange Self Service Admins

- Store Password using reversible encryption
- Account is sensitive and can't be delegated
- Do not use Kerberos Pre-authentication
- Use DES Encryption types for this account

Comments: OU admins are unable to do Disable or Expire Accounts. This was done as part of the initial rollout of central accounts. In addition to resources granted to the department managing the user, they may have other resources available to them including Sites, the Library, permissions from other departments where they have partial appointments, and permissions arising from being students or alumni.

Our suggestion to admins using central accounts is to assign all resources to groups and then add users to these groups. One of these groups can limit log on to LSA owned computers. (Home directories and profiles don't lend themselves well to groups, sorry.) When a user leaves a department, the admin can remove them from all their department groups, delete their home directory and profile, delete their Exchange account if the admin is sure the user is leaving the University, and move them back to the People OU. At this point, they should have no more permissions to departmental resources than the 250,000 other active accounts in AD.

In an extreme case where a disgruntled IT Admin or other employee leaves under bad circumstances, you can contact W2ksupport and we can disable the account for you. We can discuss in advance what the policy would be for granting such a request.

Restrictions on the other attributes above result from either the same thought process or because Microsoft has bundled many of these permissions into an all or nothing permission.

Permissions derived from: Accounts OU Admin

Disable or Limit Logons to Department and Resource User Accounts - Self Service Admins - Yes

Self service admins have full control over user objects in the Organizations OU.

Comments:

Permissions derived from: Organizations OU Admin

Change Other Names Attributes of Uniqname Users - Self Service Admins - No

Most of the name type attributes are set on Uniqname accounts by a synchronization process with UMOD and cannot be changed by Self Service Admins in Active Directory. The following is a list of user attributes that cannot be changed. They are listed with a description and the LDAP name in parentheses.

- Home drive (homeDrive)
- Home directory (homeDirectory)
- Login script (scriptPath)
- Name (Cn)
- First Name (givenName)
- Initials (initials)
- Last Name (sn)
- Telephone (telephoneNumber)
- Telephone (otherTelephone)
- Home Phone (homePhone)
- Home Phone (otherhomePhone)
- Web Page (WebInformation)

Permissions Summary for Exchange Self Service Admins

- Pager (Pager)
- Pager (otherPager)
- Fax (Facsimile)
- Fax (otherFacsimile)
- Company (Company)
- Title (Title)

Comments: Decisions on limiting these attributes was made during the design of the Central Accounts project with input from all departments.

Permissions derived from: Accounts OU Admin

Change Other Names attributes of Department/Calendar Users - Self Service Admins - Yes

There are no restrictions on changing these attributes.

Comments: Naming conventions above must be followed

Permissions derived from: Organizations OU Admin

Change Department Attribute on Uniqname/Calendar/Department User Accounts - Self Service Admins - Yes

Self Service admins can change the Department attribute for all account types.

Comments: Each department needs to register a Department name with ITCS and only use this name if they wish to populate the Department field. The Department field is being used by ITCS to populate departmental address books if the department requests one.

We need to check if the department attribute is available to all Accounts OU Admins. I think we have only set LSA, Housing and Library.

Permissions derived from: Accounts OU Admins, Organizations OU Admin

Change Mailbox Quotas for Uniqname Mailboxes - Self Service Admins - Yes for now, LSA OU Admins - yes for now, but longer than other groups

Mailbox quotas (Storage Limits) are set on the mailbox stores at either 400MB or 2GB and should not be overwritten by the user object. Creating or moving a mailbox into the appropriate mailbox store is the way to assign quotas.

Comments: Currently all Account OU Admins have the ability to change quotas on user objects and needs to be changed. This is a holdover from when LSA was assigning LSA owned mailboxes to users in their Accounts OU. We should consider leaving this permission in place for LSA until their migration is complete. We should immediately change all other OU permissions to restrict this ability.

Permissions derived from: Accounts OU Admin

Change Mailbox Quotas for Department and Calendar Resources - Self Service Admins - Yes for now, LSA OU Admins - yes for now, but longer than other groups

Same as above:

Permissions Summary for Exchange Self Service Admins

Comments: Currently all Organizations OU Admins have the ability to change quotas on user objects and needs to be changed

Permissions derived from: Organizations OU Admin

Create Departmental Address Book - Self Service Admins - No, ITCS Exchange Admins - Yes

Each department can request one departmental address book that will appear in the Exchange Global Address List. ITCS Exchange Admins will create this address book.

Comments: Department address books are created using an LDAP search function to specify which mailboxes will appear in the address list. This LDAP search will be defined by ITCS and the requesting department when it is created. In general, we recommend that an agreed upon "Department" name be specified. The LDAP search will add any users that have this "Department" name in beginning of the user Department field or in the beginning of a group name. For example, the address book for Housing specifies "Housing" as the Department Name. Users with Department attributes of "Housing", "Housing ResNet" or Group Names such as "Housing HelpDesk" will all appear in the Housing address book.

Permissions derived from: Accounts OU Admins, Organizations OU Admin

Populate Departmental Address Book - Self Service Admins - Yes

Self service admins can add mailboxes to their department address list by editing the Department attribute for users or properly naming their groups. See above:

Comments:

Permissions derived from: Accounts OU Admins, Organizations OU Admin

The following permissions are listed on the 4 Exchange tabs of a user object:

Exchange General Tab

Mailbox Store - Anyone - No

Use this text box to view the location of the user's mailbox. Not a writeable field by anyone.

Alias - Self Service Admins - Yes

Don't change. The alias is the same as the user's logon name that you selected when you created the mailbox-enabled user.

Permissions derived from: Accounts OU Admins, Organizations OU Admin

Delivery Restrictions - Self Service Admins - Yes

You can select the maximum size for outgoing and incoming messages, and you can specify who a mailbox-enabled user can or cannot receive messages from.

Comments: Can OU Admin overwrite Exchange system message limits?

Permissions derived from: Accounts OU Admins, Organizations OU Admin (?)

Delivery Options - Self Service Admins - Yes

- Send on behalf (Add any AD user)
- Forward to: (must forward to another AD User or Contact)

Permissions Summary for Exchange Self Service Admins

- Recipient Limits

Comments: Use this dialog box to specify message delivery options for a mailbox-enabled user. You can allow one or more users to send messages on behalf of a mailbox-enabled user, you can specify a forwarding address for messages addressed to a mailbox-enabled user, and you can limit the number of recipients that a mailbox-enabled user can send a message to.

Permissions derived from: Accounts OU Admins, Organizations OU Admin (?)

Storage Limits - Self Service Admins - Yes for now, but should be changed

This includes settings to change Storage Limits (override quotas) and Deleted item retention. These should both be changed.

Email Addresses Tab - Self Service Admins - Yes, but generally should not be changed

SMTP, X400, X500, SIP, Set as Primary, etc.

Comments: Although Self Serve admins can change these setting, there are dangerous and can easily break the user's mailbox. Use with care.

Permissions derived from: Accounts OU Admins, Organizations OU Admin

Exchange Features Tab

Mobile Services - Self Service Admins - No, Exchange Full Admins - Yes

All Mobile Services are enabled by default, but can't be changed by Accounts or OU Admins

- Outlook Mobile Access - enabled
- User Initiated Synchronization - enabled
- Up-to-date Notifications - enabled

Permissions derived from: Accounts OU Admins, Organizations OU Admin, Lack of "Exchange Admin" permissions at the ITCS Admin Group level (?)

Protocols - Self Service Admins - Yes

All protocols are enabled. Can be enabled, disabled or settings changed.

- Outlook Web Access -enabled
- POP3 - enabled (service is turned off on server, so this does nothing)
- IMAP4 - enabled

Permissions derived from: Accounts OU Admins, Organizations OU Admin

Exchange Advanced Tab

Simple Display Name - Self Service Admins - Yes

Use this text box to specify a simple display name for a mailbox-enabled user. The simple display name is used by systems that cannot interpret all of the characters in a normal display name. For this reason, you should specify a simple display name that uses non-ANSI characters, such as Kanji.

Permissions derived from: Accounts OU Admins, Organizations OU Admin

Hide from address list - Self Service Admins - Yes

Permissions Summary for Exchange Self Service Admins

Use this option to prevent a mailbox-enabled user from appearing in address lists. If you select this option, the mailbox-enabled user will be hidden from all address lists.

Permissions derived from: Accounts OU Admins, Organizations OU Admin

Downgrade high priority mail for X400 - Self Service Admins - Yes

Use this check box to downgrade e-mail that is set for high priority delivery to an X.400-type e-mail address. The downgrade causes the outbound e-mail to conform to original 1984 X.400 conventions.

Permissions derived from: Accounts OU Admins, Organizations OU Admin

Custom Attributes - Self Service Admins - Yes

Click [Custom Attributes](#) to specify Exchange custom attributes. Exchange provides 15 custom attributes. Assigning values to the custom attributes enables you to select the mailbox-enabled user's information you want to track. For example, if your company uses an employee identification numbering system, you can type the user's identification number in a custom attribute.

One of these may be used for shortcodes in the future.

Permissions derived from: Accounts OU Admins, Organizations OU Admin

ILS Settings - Self Service Admins - Yes

Click [ILS Settings](#) to specify an ILS server. ILS gives Internet service providers and Web site managers the ability to increase communication between users visiting a Web site. ILS stores information about each user, including their Internet Protocol (IP) address. This enables your online users to find each other.

Permissions derived from: Accounts OU Admins, Organizations OU Admin

Mailbox Rights - Self Service Admins - Yes,

Click **Mailbox Rights** to grant and deny mailbox permissions for a mailbox-enabled user. You can view and change mailbox permissions for a mailbox-enabled user, assign mailbox permissions to another user or group, and change inherited permissions.

Comments: You can assign the following permissions to any user:

- Full mailbox access
- Delete Mailbox Storage
- Read Permissions
- Change Permissions
- Take Ownership
- Associated external account
- Special permissions
- Advanced

Permissions derived from: Accounts OU Admins, Organizations OU Admin, Exchange Self Service Admin

Mailbox "Send As" Delegation for Uniqname users - Self Service Admins - No, ITCS Exchange Admins, Yes

The "Send As" delegation allows the assigned user to send email that appears to come from the user who you apply this permission to. This is in contrast to the "send on behalf" delegation that is

Permissions Summary for Exchange Self Service Admins

set in the Delivery options of the Exchange General tab. "Send on behalf" adds the words "sent on behalf of" to the from address and isn't always acceptable.

This is set by changing the permissions on the user object you want to send mail as. Since the permissions on users in the Accounts OU are very restricted, we don't give the ability for OU Admins to change permissions and therefore cannot set the "Send As" delegation".

Permissions derived from: Accounts OU Admins and lack of ability to change permissions.
Domain Admin access to all user objects in People OU and Accounts OU.

Mailbox "Send As" Delegation for Department and Calendar users- Self Service Admins - Yes

See above. Because an Organizations OU Admin has full control over all the objects in their OU, they have the ability to change the necessary permissions for all the objects and the "Send As" permission.

To assign the "Send As" permission to a user:

1. Make sure ADUC is in Advanced Mode (View->Advanced)
2. Open the Security tab in the User Properties of the user you want to be able to Send As.
3. Click Add, and add the user who you want to be able to send the message as the other person
4. Scroll through the permissions and check "Allow" for the "Send As" permission.

Permissions derived from: Organizations OU Admin which have full control of object including changing permissions.

View Exchange System Manager - Self Service Admins - Yes

View Mailboxes and sizes

View Logons

Mailbox and other delegation

See Kelly's paper

Create Contacts?

Calendar Auto accept

Calendar on the web

Maryb's list from the web

<http://www.itd.umich.edu/~lannos/exchange/service.html>

Attributes available and blocked

<http://www.umich.edu/~lannos/windows/central-accounts-attributes.html>