CatNet Delegated
IT Staff
Guide to UACConnect
## Table of Contents

Training Objective...........................................................................................................4

Module 1: Overview of Microsoft Active Directory, Exchange 2013 and Lync 2013 ..................4

Active Directory ..................................................................................................................4

  Overview ..........................................................................................................................4

  Terminology ....................................................................................................................5

  Management Tools .........................................................................................................5

    PowerShell Basics .......................................................................................................7

Microsoft Exchange ...........................................................................................................7

  Overview .........................................................................................................................7

Exchange Terminology: .................................................................................................... Error! Bookmark not defined.

  Server Types: ..................................................................................................................8

Exchange Management and Administration .......................................................................9

  Installing the Exchange 2013 Management tools .........................................................9

  Exchange Admin Center (EAC) .....................................................................................9

  Exchange Management Shell (EMS) .............................................................................9

Using the Exchange Management Tools .......................................................................10

Exchange Recipients: .......................................................................................................11

  Mailboxes .........................................................................................................................11

  Mail User .........................................................................................................................11

  Contacts ..........................................................................................................................12

  Room Resource .............................................................................................................12

  Equipment Resource .....................................................................................................12

  Distribution Groups .......................................................................................................12

Microsoft Lync 2013 ......................................................................................................13

  Overview ........................................................................................................................13

Lync Terminology: ..........................................................................................................13

  Server Types: ..................................................................................................................14

  The following are the Lync server roles for Microsoft Lync 2013.................................14

  Persistent Chat Rooms .................................................................................................15

Module 2: UofA Central Active Directory and Exchange Services ....................................15
Overview .................................................................................................................................................. 15
UAConnect .................................................................................................................................................. 16
Overview .................................................................................................................................................. 16
Architecture ............................................................................................................................................... 16
Policies ....................................................................................................................................................... 16
Exchange Management Tools Pre-requisites ............................................................................................... 23
Role Based Access Control (RBAC) for Delegated IT Staff ......................................................................... 23
UA Exchange Admin Center for Delegated IT Staff .................................................................................... 24
UAConnect Lync .......................................................................................................................................... 24
Overview ................................................................................................................................................... Error! Bookmark not defined.
Architecture ............................................................................................................................................... Error! Bookmark not defined.
Policies ....................................................................................................................................................... 24
Commands Available to Delegated IT Staff ................................................................................................. 25
Module 3: Practical Application and Troubleshooting .................................................................................. 26
Step-by-step Examples of Common Exchange Tasks .................................................................................. 26
Creating Mailboxes ...................................................................................................................................... 26
Departmental Accounts .................................................................................................................................. 26
Service Accounts ......................................................................................................................................... 28
Departmental Accounts .................................................................................................................................. 31
Service Accounts ......................................................................................................................................... 32
Set Mailbox Permissions .............................................................................................................................. 33
Set Full Access to a mailbox ......................................................................................................................... 33
Set Mailbox Folder Permissions .................................................................................................................... 34
Set Send-as Access to a mailbox ................................................................................................................... 35
Set Send on Behalf of Access to a Mailbox ..................................................................................................... 36
Rename Existing Accounts ............................................................................................................................ 37
Configuring Additional SMTP Addresses ................................................................................................... 38
Remove an Existing Account ........................................................................................................................ 41
Create Room Resources and Equipment Resources ..................................................................................... 43
Creating Distribution Groups ....................................................................................................................... 50
Training Objective

The material in this guide is intended to provide departmental IT staff with the basic knowledge required to administer objects within CatNet and UAConnect. The guide is divided into three modules. Module 1 delivers a general overview of Active Directory, Exchange and Lync. Module 2 provides details of the UofA central implementations of Active Directory, Exchange and Lync including policies and procedures governing use of CatNet and UAConnect. Module 3 delves into practical applications of Exchange administration, Lync Persistent Chat management and diagnostic troubleshooting within CatNet and UAConnect. After completing this training, departmental IT staff should be able to perform day to day Active Directory, Exchange and Lync Persistent Chat administrative tasks and diagnostic troubleshooting for their department and users.

Module 1: Overview of Microsoft Active Directory, Exchange 2013 and Lync 2013

Active Directory

Overview

Active Directory (AD) is a centralized system for managing identities and security permissions for users and computers in a Microsoft Windows based environment. Without AD, Windows computers must be managed individually and user accounts must be created and managed on each individual computer. AD also allows administrators to publish security and operational settings, such as password length and desktop appearance, to many computers at one time. This keeps administrators from having to make the same changes to multiple computers, effectively eliminating the need for many repetitive tasks required for desktop and server setup and administration.

- AD maintains information about users and computers as AD objects. A user will always have a user object and a computer has a computer object. Additional specialized objects include contacts, rooms, and printers.
- Objects are assigned to groups to aid in the application of permissions. Instead of granting each user permission to a file it is recommended that administrators assign permissions to a group and then add users to the group. Each user in a group will inherit the permissions granted to that group.
- Objects are also organized in Organizational Units (OUs). OUs hold all Active Directory object types in order to make them easier to find and manipulate in the Directory. OUs are also designed as points for applying policies for users and computers or granular permissions for role based administration.
- Group Policies are sets of modifications that are configured to change the way Windows computers operate and the way users that are using Windows computers view and use the OS.

*For more detailed information on Active Directory please access one of the following:

- **UACBT** course Microsoft MCTS (Exam 70-640): Creating & Maintaining AD Objects and Microsoft MCTS (Exam 70-640): Group Policy
**Terminology**

Forest: A collection of Active Directory trees that share a Configuration container and Schema and are connected through trusts. The forest acts as a security boundary for an organization and defines the scope of authority for administrators.

Tree: A collection of Active Directory hierarchical domains that share a common namespace.

Domain: An X.500-based hierarchical database of containers and objects. Microsoft domains have a DNS domain name, a security service to authenticate and authorize access to resources, and policies that dictate functionality. Domains are boundaries for administration and replication.

Active Directory Site: A site is a set of well-connected subnets. Sites differ from domains; sites represent the physical structure of your network, while domains represent the logical structure of your organization. Sites optimize bandwidth requirements for replication, make authentication quicker and more efficient and enable clients to find the nearest active directory service providers more easily.

Organizational Unit: A type of container in an Active Directory domain. It can contain objects like users, computers, contacts, groups, or other OU's or containers. OU's can also have group policies applied.

User object: Account for authenticating in AD and that can be used to grant access to resources.

Computer object: Account for authenticating a computer within a Domain.

Group objects: An object in Active Directory that can have members. Members can be users, contacts, computers, or other groups. Permissions can be granted to security groups (not distribution groups) to give all members access to resources. Distribution groups are not security enabled and can be used only for communication purpose.

Security principals: Active Directory objects, which can be used to manage access to domain resources. Each security principal is assigned a unique identifier, which it retains for its entire lifetime.

*A complete glossary of Active Directory terminology can be found on the Microsoft TechNet site:*


**Management Tools**

- **Remote Server Administration Tools**
  
  The Remote Server Administration Tools pack enables remote management of Windows Servers by allowing you to open and run management tools and snap-ins to manage roles, role services, or features on a remote computer.
You can install Remote Server Administration Tools in one of the following ways.

**Add Features Wizard**: Open Control Panel, open Programs and Features, and then click Turn Windows features on or off.

**PowerShell**: Open a Windows PowerShell session with elevated user rights. To do this, click Start, click All Programs, click Accessories, click Windows PowerShell, right-click the Windows PowerShell shortcut, and then click Run as administrator.

Import the Server Manager module into the Windows PowerShell session before working with Server Manager cmdlets. Type the following, and then press Enter.

```
Import-Module ServerManager
```

You can install remote administration tools for all roles or all features in a single command instance by choosing one of the container identifiers shown in the following list.

- RSAT for installing or removing all available Remote Server Administration Tools.
- RSAT-Role-Tools for installing or removing all available remote role administration tools.
- RSAT-Feature-Tools for installing or removing all available remote feature administration tools.

Type the following, in which name represents the command name of the remote administration tool that was obtained in the previous step, and then press Enter to install the remote administration tool.

```
Add-WindowsFeature name
```

You can install multiple tools by using commas to separate the command names, as shown in the following example.

```
Add-WindowsFeature RSAT-RDS,RSAT-Web-Server,RSAT-BitLocker
```

- **Active Directory Users and Computers**
  - Active Directory Users and Computers is a Microsoft Management Console (MMC) snap-in that you can use to administer and publish information in the directory. It is used to create new or manage existing Active Directory objects, including users, groups, computers, and organizational units.

- **Group Policy Management Console**
  - Group Policy Management Console (GPMC) is a Feature Administration Tool included in the RSAT pack. It can be installed by either the Add Features wizard or the Add-WindowsFeature PowerShell cmdlet.

- **Windows PowerShell (Active Directory Module)**
  - The Active Directory PowerShell Module is part of the Active Directory module installed with the RSAT pack. To use the cmdlets the module must be imported into a Windows PowerShell session (```
Import-Module ActiveDirectory```).

© University of Arizona, 2015
Version 2.0
PowerShell Basics

PowerShell is a task automation framework that is built on top of and integrated with the .NET framework. It provides both local and remote access to administrative tasks via COM and WMI integration. It allows users to perform simple functions by running simple commands or script complex functions with multiple commands tied together.

Running PowerShell is simple enough and can be accomplished by typing PowerShell at the command prompt or through the Run window (Windows Button + R in any version of Windows) and hitting enter. Once the PowerShell console is open you can begin performing operations with PowerShell. PowerShell is installed by default in all versions of Windows after Windows Vista. It can be installed in Windows 7 64 bit or higher by installing the Windows Management Framework tools available here: https://www.microsoft.com/en-us/download/details.aspx?id=40855.

PowerShell commands follow a verb-noun notation. For instance, get-service will show a list of services running on a computer. Set-date will allow you to change the date. Get-command will list all commands that can be used in PowerShell. It’s possible to get more information about a specific command and how to use it by typing get-help <command>. Get-help set-date will give you information on how to use the Set-date command.

Each PowerShell command includes a number of switches that can modify the way the command works. For instance, running get-service with the -include switch will limit the list of services that show. Running get-service -include “s**” will return only the services that begin with the letter S. You can also use switches to get more information from the get-help command. Running get-help set-date -full will give you all available information about using set-date, including examples.

It’s possible to tie commands together by using a function called pipelining or piping. A pipeline takes the output of one command and uses it as input for another command. This allows you to perform actions on multiple objects at once. A pipeline is initiated by using the “|” character (the pipe character, located just above the enter key on most keyboards or Shift + \\). A pipeline must be initiated after the first command you enter, so initiating a pipeline at the start of a command will do nothing. As an example, you can display all of the attributes returned by a get type command by piping the output of the command to the Format-list command. For example, running get-date | format-list will return the date and a number of other things including the number of days into the current year, day of the week, and others. As an example of what the pipeline is capable of doing, it’s possible to start all of the services on a computer by running get-service | start-service (Don’t do this, though, as it can cause a crash depending on what services are installed on the computer).

Microsoft Exchange

Overview

Microsoft Exchange is Microsoft’s enterprise messaging application. Exchange’s main function is providing email services, but also includes other features such as calendaring, task list development, collaboration, contact tracking and grouping, and several other features.
Users in Exchange are assigned Mailboxes that serve as delivery points for email and as storage for their calendar, personal contacts, and other information that they may need.

- Exchange allows the use of Distribution Lists. Distribution Lists allow multiple users to be grouped together with a single email address. Emails sent to a distribution list are sent to all members of the Distribution List. This allows for easy email distribution to multiple people without needing to type in multiple email addresses.
- Exchange Calendars can be shared between users or groups of users. Users can grant specific or broad permissions to their calendars to allow other users to see their appointments or add additional appointments depending on the level of permissions granted.

**Server Types:**

Exchange 2013 utilizes only two main server types, Client Access, and Mailbox. Each server type performs a specific role. Unlike with previous versions of Exchange, the 2013 approach is **NOT** to split up roles to different servers, it’s considered good practice to deploy all roles on **all** Exchange servers.

**Client Access Server (CAS)**

The Client Access Server is used to provide users with access to their mailboxes in a variety of ways (e.g. Outlook, Outlook Web App, ActiveSync). The primary methods of access are Outlook and Outlook Web Access (OWA). Outlook is the mail client developed by Microsoft that provides full integration with the Exchange server to allow users to view and modify their email, calendar, tasks, and contacts with ease. Outlook Web Access is a Web Based version of Outlook that allows users to have the same functionality through a web browser without having to install additional software on their computer.

There are two main components:

- **Client Access service** - handles the client connections to the mailboxes
- **Front End Transport service** - performs various email filtering functions as well as email routing between the Exchange servers and the outside World.

**Mailbox server**

The Mailbox Server holds one or more large databases that contain all the information stored in each user’s mailbox. Users that connect to Exchange will read the data stored in the database by communicating first with a Client Access Server.

This server also runs two Transport services:

- **Hub Transport service** - provides email routing within the organization and connectivity between the Front End transport service and the Mailbox Transport service.
- **Mailbox Transport service** - passes email messages between the Hub Transport service and the mailbox database
Outlook Web Application (OWA)

Outlook Web Application is included in Exchange server to allow all users to access their mailboxes no matter where they are (as long as they have an Internet connection), what web browser or what Operating System they are using to access it.

Exchange Management and Administration

Exchange 2013 allows administrators to configure and manage Exchange remotely through a selection of management tools.

Installing the Exchange 2013 Management tools


The Exchange 2013 management tools can be installed using the current service pack installer or CU installer, rather than the full Exchange 2013 installation media. If you have a previous version of the management tools installed, you will need to use the service pack installer or CU installer to upgrade them to the appropriate level. It is important to keep your installation of the management tools up to date; outdated software might fail to connect to the Exchange environment, contain deprecated cmdlets or be missing current cmdlets.

The Exchange 2013 management tools installation will add the following items to your local computer:

- Exchange Administrative Center (Internet shortcut to the web-based management console)
  - Note that the shortcut defaults to https://localhost/ecp/?ExchClientVer=15. Localhost in this URL will need to be replaced with a valid mail server host name.
- Exchange Management Shell (locally installed command shell)
- Exchange Server Help (Internet shortcut to Microsoft on-line help for Exchange)
- Exchange Toolbox (MCC for managing configuration and mail flow)

Exchange Admin Center (EAC)

The Exchange Admin Center (EAC) is the web-based management console in Microsoft Exchange Server 2013. It is optimized for on-premises, online, and hybrid Exchange deployments. The EAC replaces the Exchange Management Console (EMC) and the Exchange Control Panel (ECP), which were the two graphical interfaces used to manage Exchange Server 2010.

Because the EAC is now a web-based management console it can be accessed from any browser using the ECP virtual directory URL (i.e. https://mail.catnet.arizona.edu/ecp).

Exchange Management Shell (EMS)

The Exchange Management Shell is a Command Line Interface (CLI) for Exchange 2013. It allows administrative users to read, manipulate, and modify settings and properties for all aspects of Exchange using PowerShell. When managing Exchange through the EMS it is possible to perform all actions without the constraints of the
limitations of a Graphical Interface. However, the EMS is more difficult to learn than the EAC. It also provides a robust and flexible scripting platform that can reduce the complexity of current Microsoft Visual Basic scripts.

### Using the Exchange Management Tools

**Using Exchange Administrative Center (EAC)**

Most basic administrative tasks, such as creating, deleting, and disabling mailboxes, can be performed easily through the Exchange Administrative Center.

![Exchange Administrative Center](image)

The EAC is navigated with the use of a topic list view in the left pane of the console. This list view is separated into twelve topics: Recipients, Permissions, Compliance Management, Organization, Protection, Mail Flow, Mobile, Public Folders, Unified Messaging, Servers, Hybrid, and Tools. Depending on the permissions granted to the user logged into the EAC, fewer topics may be visible.

One of the more important things to note about the EAC is that settings are not changed until the user presses the **Save** button. Closing the settings window with the Cancel button or the X in the upper right corner of the window will result in all changes being lost.

Note that not all functions can be accomplished through the Exchange Admin Center. The EAC only provides a graphical method for passing PowerShell Commands to the Exchange Servers. The EAC is aimed at providing a simplified interface for day to day administration tasks, as a result, most of the more advanced or complex management of Exchange objects must be done through the Exchange Management Shell (EMS).
Using the Exchange Management Shell

The EMS is accessed via the “Exchange Management Shell” shortcut on the Start Menu (Windows 7) or Apps list (Windows 8). Launching the EMS automatically provides access to the specialized PowerShell cmdlets available for Exchange management. These cmdlets would not be available by default in a standard Windows PowerShell console.

The EMS is fairly straightforward once you have a basic understanding of PowerShell. Like the Windows PowerShell and Active Directory PowerShell cmdlets, the Exchange cmdlets follow the standard verb-noun syntax (i.e. get-mailbox). Most of the available cmdlets accept pipeline input allowing you to pass information gathered using a get-command to another command such as a set- or enable-command. Exchange cmdlets can be grouped together in PowerShell scripts to facilitate automation of common tasks.

Exchange Recipients

Recipients in Exchange 2013 are separated into several categories; Mailboxes, Groups, Resources, Contacts, Shared and Migration. Each type differs in purpose and implementation.

Mailboxes

Mailboxes are Recipients that have an Active Directory Account with an Exchange Mailbox assigned to it. These users can receive and send mail by connecting to the Exchange server with a Mail client (Outlook, OWA, etc.).

For details on creating mailboxes see “Creating Mailboxes”

Mail User

Mail users are Active Directory user objects that have external e-mail addresses (users that have access to resources via Active Directory login credentials, but do not have a mailbox in Exchange).
Contacts

Contacts are meant to give External Email recipients an Email Address within the local Exchange Environment. Emails addressed to an email address that belongs to a Contact are redirected to the external email address assigned to the contact. Contacts can also be applied to user’s mailboxes as a way to forward emails to an external email address.

For details on creating contacts see “Creating Contacts”

Room Resource

A room mailbox is a resource mailbox assigned to a meeting location, such as a conference room, auditorium, or training room. Only one room resource can be associated with a meeting at a time.

For details on creating room resources see “Creating Room Resources and Equipment Resources”

Equipment Resource

An equipment mailbox is a resource mailbox assigned to a resource that's not location specific, such as a portable computer, projector, microphone, or a company car. Multiple equipment resources may be assigned to a single meeting.

For details on creating equipment resources see “Creating Room Resources and Equipment Resources”

Distribution Groups


Distribution Groups in Exchange 2013 serve a dual purpose. First, they are meant to allow users to send emails to multiple recipients by using a single email address. They can also be used to assign permissions for shared resources like Calendars. There are two types of Distribution Groups in Exchange 2013, Standard and Dynamic.

Standard Distribution Groups

Distribution groups operate similarly to normal Active Directory groups. After the group is created an administrator or group owner must manually add and remove members. Distribution groups can hold as few or as many users as needed and may be assigned multiple owners for the purposes of membership management. Every member of a distribution group will receive a copy of each message that is sent to the distribution group. Distribution groups cannot be used to assign permissions to mailboxes or mailbox folders such as calendars. By default, new distribution groups are configured to only allow delivery of messages from senders within the organization.

To ease the support burden of managing membership, distribution groups can be configured to allow for open membership, meaning that anyone that wants to join the group may join it without administrator or owner
intervention. Alternatively, they can be configured to allow owners to approve or reject requests for group membership which could also reduce the support burden on IT staff.

**Security Groups**

Exchange security groups combine the functionality of a distribution group with the ability to assign permission to shared resources. Like distribution groups, an administrator or group owner must manually add and remove members. Unlike distribution groups, security groups can be added to the access lists for mailboxes and mailbox folders. In addition, a security group may be used to add multiple contacts at a time to a user’s Lync contact list.

**Dynamic Distribution Groups**

Dynamic Distribution Groups allow administrators to automate membership in the distribution group. There are a number of attributes that can be used to define membership in these groups and only users that match all of the requirements set during the group’s creation will receive emails sent to a Dynamic Distribution Group.

**Distribution Group Moderation**

It is possible to configure Distribution Groups so that only emails that are approved by an assigned moderator are sent to the members of the group. Once this is configured, an Arbitration email is sent to the configured moderator. If the moderator approves the message it is sent to recipients. If not, the email is not transmitted. This helps to prevent unauthorized use of Distribution Groups.

Moderation can be configured for all group types through the EAC or through the EMS.

For details on creating distribution groups see “Creating Distribution Groups”

**Microsoft Lync 2013**

**Overview**

Microsoft Lync Server 2013 is a communications suite that offers instant messaging (IM), presence, conferencing, and telephony solutions that can support enterprise-level collaboration requirements.

**Lync Terminology:**

Contacts list - A list of people, groups, or organizations with whom you communicate.

Conversation History - The folder in Outlook where instant messages and phone conversations are stored.

Edge pool - A single computer pool or a multiple computer pool that, by default, supports remote users in your organization who sign in to Lync Server from outside the firewall by using a virtual private network (VPN).

Front End pool - A set of Front End Servers, configured identically, that work together to provide services for a common group of users.

Lync Meeting - Denotes the experience with Lync that can be scheduled, or ad-hoc. A Lync Meeting provides the ability to interact with people through video, audio, instant messaging, and content sharing.
Lync Meeting window - Denotes the Conversation window that handles escalations (peer-to-peer to conference) and scalable views that display people and content together inside a Lync Meeting.

Lync Server Management Shell - The management command line interface built on Windows PowerShell technology that includes a set of cmdlets to help control administration and automation.

Lync Web Scheduler - A web-based meeting scheduling and management tool for users who don’t have access to Microsoft Outlook, or are on an operating system not based on Windows. With Lync Web Scheduler, you can create new meetings, change your existing meetings, and send invitations using your favorite email program.

Microsoft Lync Server Mobility Service - This service supports Lync functionality, such as instant messaging (IM), presence, and contacts on the following mobile devices: iPhone, iPad, Android, Windows Phone, and Nokia.

Microsoft Push Notification Service - A notification service that sends new events, such as an instant messaging invitation or a missed call, to the Windows Phone mobile device.

Office Web Apps Server - A server role used with Office Web Applications in Lync Server to handle the sharing and rendering of PowerPoint presentations.

presence status - One of the attributes that makes up presence and that indicates a person’s availability and willingness to communicate.

A glossary of Lync/Skype terminology can be found on Microsoft Technet: https://technet.microsoft.com/en-us/library/hh393341(v=ocs.15).aspx

Server Types:
Each server running Lync has one or more server roles. Each role defines the functionality of the server. There is no need to have all the server roles in the network, only the ones required by the feature(s) you plan to use. Microsoft provides a Planning Tool to assist in designing your Lync implementation to include the server roles you need.

Lync 2013 Planning Tool guide download page:

Microsoft Lync 2013 Server Roles
- Front End Server (web front end)
- Back End Server (MS SQL)
- Edge Server
- Mediation Server
- Director
- Persistent Chat Front End Server
- Persistent Chat Store (MS SQL)
Persistent Chat Compliance Store (MS SQL)

On most server roles you can build pools of servers running the same role for scalability and availability. You must use a load balancer (DNS or hardware balancers are supported) to balance the load among the servers in the pool.

Persistent Chat Rooms

Persistent chat lets you create topic-based discussion rooms that persist over time. Persistent chat rooms are organized by Categories and allow communication and collaboration with a group of people who have a common area of interest. You can share ideas and information by posting messages in real time and find ideas and information by browsing or searching the chat history. Messages are saved over time, so new and old chat room participants can see all the chat history at any time.

With persistent chat, you can search for content within and across rooms, and create alerts (notifications) and filters (topic feeds) to track conversations in particular rooms and about specific topics. And, you can create and manage your own chat rooms, if you’ve been authorized by your Lync administrator.

IMPORTANT: Conversational style in a chat room is typically casual, but remember whatever you write in a chat room is permanent. Anyone with access to the room can see what you’ve written for as long as the chat room is enabled.

Module 2: UofA Central Active Directory and Exchange Services

CatNet

Overview

CatNet is the University of Arizona central Active Directory. It provides a mirror of NetID for Windows and LDAP authentication purposes as well as a delegated administration roles allowing Campus IT to leverage the benefits of Active Directory without having to manage and maintain AD infrastructure.

Architecture

CatNet Infrastructure Diagram

- CatNet follows a single forest, single domain model. Forest and domain functional levels are at Windows Server 2012. There are three Active Directory sites configured in CatNet; two in Tucson (UA, Biosphere2) and one in Phoenix. Exchange is only deployed in the U of A Tucson site.
  - CatNet contains a mirror of NetID usernames and passwords. Each NetID is tied to an Active Directory user account and is granted permission based on job role and the organization to which they belong. NetID changes are synced in real time to CatNet. This is a one-way sync from NetID; changes cannot be made to NetID accounts directly in CatNet. All NetID accounts are located in the NetID OU in the CatNet Active Directory. Only Enterprise Administrators have direct access to the NetID OU.
CatNet also has a departmental OU assigned for each organization with objects that are managed in CatNet. These OUs are controlled by departmental IT staff and can hold all necessary accounts needed for operation. Delegated IT staff are granted permission to fully control their Department OU.

Users with departmental administrative permissions in Active Directory can perform most or all administrative actions against objects that are in their departmental OU. This includes, but is not limited to, adding and removing computers, changing and creating new Group Policies that are assigned to the department OU, and creating additional OUs.

Important Notes:

- All objects created within department OUs must follow the CatNet naming conventions. This ensures that each object has a unique name within the directory and prevents objects from being overwritten by automated processes.
- Departmental accounts and service accounts are the only types of user accounts supported within department OUs. All other users must be assigned accounts via NetID.
- Group Policies that modify password requirements must not be applied to any OUs. Doing so can cause the policy to apply to the entire Active Directory. Department delegated IT staff should coordinate with UITS to create granular (fine-grained) password policies for objects in Department OUs.
- Group Policies normally apply to the OU they are linked to and all OUs below it. This means that linking OUs in the wrong location can impact more objects than intended, and may affect the entire departmental OU.

*For more information on CatNet please access the CatNet entry on the UITS services site.

**UAConnect**

**Overview**

UAConnect is the University of Arizona central email, calendaring and messaging service for faculty and staff. It includes Exchange 2013 for email and calendaring and Lync 2013 for messaging.

**Architecture**

UAConnect Mail flow Diagram

Lync Infrastructure Diagram

**UAConnect Exchange Overview**

Exchange 2013 provides email, calendaring, task management, contact management and resource (room and equipment) management for U of A faculty, staff, retirees, student employees and DCCs. Exchange 2013 has been implemented in a fully redundant and highly available architecture spanning two physical data centers with 4 complete copies (1 active, 2 passive, 1 lagged) of the mailbox data to ensure email continuity through planned maintenance and unexpected disruptions.
Policies

Exchange Recipients in UAConnect

Mailbox

Users’ affiliation with the university determines whether or not they will have a mailbox in CatNet. All faculty and staff receive Exchange mailboxes by default at the time of NetID creation. Student employees and designated campus colleagues (DCC) can receive an Exchange mailbox upon request.

Mailbox requests are built into the DCC request process which allows for DCC mailboxes to be created at the time of NetID creation in a similar manner to faculty and staff mailboxes.

Student Employee requests must be sponsored by a faculty or staff member; requests can be made via a web interface which allows for individual or bulk requests: https://netid.arizona.edu/UaconnectStudentTemp.

Departmental/Service accounts are created and managed by delegated IT staff within their delegated OU(s). All departmental and service accounts must follow either UAConnect (<dept>-xxxx) or base CatNet (__xxxx) naming conventions. For security reasons, all departmental accounts must be created as “shared” accounts in Exchange with access to the mailboxes delegated to the appropriate individuals. Service accounts are intended to be used by applications and should have strong passwords enforced by fine grained password policies.

Mail Users

This primarily includes students that are not employees and DCC accounts that did not request an Exchange mailbox.

All mail users in UAConnect are created via the automated account creation processes.

Contacts

All contacts in CatNet are explicitly excluded from the Global Address List (GAL) but may be included in other Exchange address lists, including custom address lists.

Room Resource

Like any other object created in CatNet, room resources must follow the CatNet naming conventions. Room names should begin with the department abbreviation, followed by a dash, then “Room”, another dash and finally the room number (i.e. UITS-Room-101)

Equipment Resource

Equipment resources are also expected to follow CatNet naming conventions. Equipment names should begin with the department abbreviation, followed by a dash, and end with a descriptive name of the resource (i.e. UITS-Projector1).
Distribution Groups

UAConnect policies require that all groups follow a specific naming convention. This prevents multiple groups with the same name being created and causing errors. The naming convention for UAConnect is the Department abbreviation followed by a dash and then the group name. For example, UITS-Administrators would be the group name for the Administrator’s group in the UITS department. In addition, it is recommended to add “distgroup” to the Custom Attribute 1 property of the distribution group. Once the custom attribute is added, the distribution group should be assigned an email address of groupname@distribution.arizona.edu which does not require additional route information for external email delivery.

Mailbox Quotas

The default mailbox quota is in CatNet is 12GB.

The following quota related actions are configured by default on user mailboxes:

- Warn: 11.5 GB
- Prohibit send: 11.75 GB
- Prohibit send/receive: 12 GB
- Quota messages will be generated once a day at 1:00 AM

Message Limits

The following are the message limit settings in UAconnect:

- Maximum receive size (internal): 100MB
- Maximum send size (internal): 100MB
- Maximum number of recipients: 5000

Recoverable Items

In Exchange 2010 Microsoft introduced the Recoverable Items folder which is used in a number of Exchange processes including Deleted Item Recovery and Single Item Recovery. This feature helps protect users’ mailboxes from accidental or malicious deletion of items. The Recoverable Items folder (and its subfolders: Deletions, Versions, Purges, and Audits) is not visible to the user in their email clients.

Deleted Item Retention

When a user soft deletes any item from their mailbox it is moved to the Deletions folder in the Recoverable items subtree. Items are retained in this folder for 14 days and can be recovered by the end user without administrator intervention.

An item is soft deleted when a user empties their deleted items folder or when a user presses SHIFT+DELETE to delete an item from any other folder.

To recover items using the Recover Deleted Items feature a user must be logged into either Microsoft Outlook or Outlook Web App (OWA).
In Outlook, users can navigate to the Folder tab and select “Recover Deleted Items.” This will open a new window displaying items deleted within the last 14 days. From here users can select items to restore or they can choose to purge items.

In OWA, users can right click on their deleted items and select “Recover Deleted Items.” This will open a new browser window displaying items deleted within the last 14 days. From here users can select items to restore or they can choose to purge items.

**Single Item Recovery**

Single item recovery provides a relatively simple mechanism for administrators to recover items for users if the items are no longer available in the Deleted Item Recovery interface. This feature is not enabled by default, but it has been enabled in UAConnect.

When items are removed from the Deletions folder, either directly by the end user or via an automated process, they are moved to the Purges folder and are no longer visible to the end user in the Recover Deleted Items interface. Normally items in the Purges folder are purged from the mailbox database when the mailbox is processed by the Managed Folder Assistant. However, with Single Item recovery enabled items will not be purged from the Purges folder until the deleted item retention period has elapsed for that item. It should be noted that this does not add an additional 14 days to the retention period of an item so items still must be recovered within 2 weeks of the original deletion.

OU Exchange Admins do not have the permissions required to recover items via single item recovery. To recover items using Single Item Recovery a user must contact the 24/7 Support Center to initiate a new ticket.

**E-mail Address Policies**

Mailboxes in UAConnect are assigned at least two SMTP addresses. All mailboxes receive an alias of netid@uaconnect.arizona.edu which is used for routing purposes (the only time this alias will ever be visible to the user is if the Exchange server generates an NDR). In addition to the routing alias, all faculty and staff mailboxes have netid@email.arizona.edu as the primary SMTP address and all student employees have netid@catworks.arizona.edu as the primary SMTP address. The SMTP addresses are assigned to the mailboxes based on email address policies that examine the value of Custom Attribute 1. The following values are programmatically written to Custom Attribute 1 based on EDS data:

- Employee
- Employeeandstudent
- Student-employee
- Student
- Retiree
- RetireeandStudent

All values except for Student-employee and Student result in an @email.arizona.edu address assigned in addition to the @uaconnect.arizona.edu routing address. A value of student-employee results in an
@catworks.arizona.edu address being assigned in addition to the @uaconnect.arizona.edu routing address. A value of student is not linked to any of the base email address policies, but does impact visibility in custom address lists.

The following values can be manually written to Custom Attribute 1 by delegated IT staff in order to take advantage of the default email policies for departmental/service accounts and distribution groups:

- deptacct – results in an @email.arizona.edu primary SMTP, a route request is still required for accounts with this Custom Attribute 1 value
- Distgroup – results in an @distribution.arizona.edu primary SMTP address, a route request is NOT required for groups with this Custom Attribute 1 value

There are additional email address policies that have been customized to provide departmental email addresses to users, departmental/service accounts, resources accounts and/or distribution groups. These email address policies add to the total number of SMTP addresses assigned to an account and may configure the departmental email address to be the primary SMTP address, but in all cases the @email.arizona.edu (or @catworks.arizona.edu) and @uaconnect.arizona.edu email addresses are retained on the account.

**ActiveSync Mailbox Policy**

The following are the default Exchange ActiveSync Mailbox policies for mobile devices:

- Allow non-provisionable devices
- Include all past calendar items and past e-mail items
- Allow Direct Push when roaming
- Allow HTML-formatted e-mail
- Allow attachments to be downloaded to device
- The following are allowed: removable storage, camera, Wi-Fi, infrared, Internet sharing from device, remote desktop from device, desktop synchronization
- Allow Bluetooth
- Allowed: browser, consumer mail, unsigned applications, unsigned installation packages

**Outlook Web App (OWA) Policy**

OWA mailbox policies determine the features and functionality available to the end user in OWA.

In CatNet the following are enabled:

- Instant Messaging
- Text Messaging
- Unified Messaging
- Exchange ActiveSync
- Contacts
- Mobile device contact sync
- All address lists
- Journaling
- Notes
- Inbox Rules
• Recover Deleted Items
• Change password
• Junk E-Mail Filtering
• Themes
• Premium client
• Calendar
• Tasks
• Reminders and Notifications
• Direct File access
• WebReady Document viewing

• Offline access
• Search Folders
• Assign Archive/Retention Policies
• Permissions
• Public Folders
• S/MIME
• Spelling Checker
• Instant Messaging
• Text Messaging

**Address Book Policies and Custom Address Lists in CatNet**

Address lists are a collection of recipient and other Active Directory objects. Each address list can contain one or more types of objects (for example, users, contacts, groups, public folders, conferencing, and other resources). Address lists also provide a mechanism to partition mail-enabled objects in Active Directory for the benefit of specific groups of users. In CatNet we have created the following base custom address lists:

• Faculty and Staff
• Student Employees
• Students
• AZPM
• CALS
• CMI
• College of Nursing
• LBRY
• Retirees

These address lists are being populated using the same custom attribute values that are used to apply email address policies.

Address lists are made available to users via Address Book Policies. The default address book policy makes the Faculty and Staff, Student Employees, Students and Retirees custom address lists available to all users. Departmental address book policies make the departmental custom address list available to users in addition to the default list.

It is important to note that the GAL has been customized to exclude student employees. Within 48 hours of a student gaining Student employee status they will be removed from the GAL and will only be displayed in the Student Employees address list.

Additional custom address lists have been created for departments participating in UAConnect. Custom Attribute 2 values are used to apply Address Book Policies making custom departmental address lists available to users.
Delegated IT staff can view the current address book policies and associated address lists using EMS:

```bash
get-addressbookpolicy | select Name,AddressLists | ft -auto
```

**Accepted Domains**

Accepted domains are the SMTP namespaces for which Exchange is able to send and receive mail. In CatNet, accepted domains have been configured for the default central email domains:

- `Email.arizona.edu` – this is the default email domain for faculty/staff/DCCs/Retirees
- `Catworks.arizona.edu` – this is the default email domain for student employees
- `Distribution.arizona.edu` – this is the default email domain for distribution lists

Additional accepted domains have been configured for departments as they have migrated into UAConnect. In some cases, these domains are referenced by email address policies to assign primary SMTP address for the users in the associated departments. In other cases the domains are used in support of “legacy” email addresses, or email addresses that users received mail at prior to migration and need to continue receiving email at those addresses but do not have a need to send as the email address.

Delegated IT staff can view a complete list of accepted domains in either the EAC or EMS.

EAC: Navigate to the “Mail Flow” topic in the left pane, then to the “Accepted Domain” tab.

EMS: `get-accepteddomain`

**Spam Filter Rule**

IronPort provides virus and spam filtering for UAConnect, preventing delivery of viruses and most spam to the end users’ mailboxes (for more information on UA implementation of IronPort, see Appendix B). However, some potential spam messages are still delivered to the users’ mailboxes with additional information in the message header. In an effort to reduce the amount of spam that users see in their inbox there is a default spam filtering rule configured on each mailbox.

The rule is named "UA Email Security Spam Relocation Rule." It inspects the subject of arriving mail messages for the [SPAM?] tag. If the tag exists, the message is moved to the user’s Junk E-Mail folder.

**Calendar Sharing Policy**

By default, any authenticated user can view another user’s free/busy calendar information.

Based on the configured sharing policy users have the option to share additional calendar information which can include details such as the meeting/appointment subject, location and body. The same sharing policy also permits users to share contacts.
Internet Calendar Sharing (ICS) is also enabled. ICS provides increased flexibility allowing users a mechanism for sharing their calendar outside of the Exchange organization. Users can publish a copy of their calendar ranging from 1 day to 1 year before and/or after the current date at one of three available detail levels to the internet with either restricted (difficult to guess, unsearchable URL) or public (easily searchable and available to everyone) access.

For step by step instructions on configuring ICS see “Configuring Internet Calendar Sharing”

Federation

UAConnect supports Exchange federation trusts with external entities that are partnered with the University or a University department where sharing calendar and contact information is a requirement for business needs. Requests for Exchange federation trusts require a support request including detailed descriptions of the business requirements and are handled on a case by case basis.

Exchange Management Tools Pre-requisites

The following prerequisites must be met before it is possible to install the Exchange 2013 Management tools: http://technet.microsoft.com/en-us/library/bb691354(v=exchg.150).aspx

1. Computer must be a member of the CatNet Domain
2. The Operating System must meet the following minimum requirements
   a. Windows 7 64 bit.
      i. IIS 6 Management Console
      ii. .Net Framework 4.5.2
      iii. Management Framework 4.0
      iv. Windows Identity Foundation
   b. Windows 8 or later
      i. .Net Framework 4.5.2
3. The version of the Management Tools installed must match the version of Exchange in use (Currently Exchange 2013 Cumulative Update 12)
4. User should be logged in with a CatNet domain account that has local administrator rights on the computer and delegated Exchange administration rights (typically __a<netid>)

Role Based Access Control (RBAC) for Delegated IT Staff

Delegated IT staff have been granted access to a subset of PowerShell commands to administer Exchange objects. The commands are divided into specific roles and organized into role groups intended to facilitate management of objects in the Departmental OUs and the NetID accounts of users. Delegated IT staff are responsible for supporting.

The roles specified for delegated IT staff are designed to provide them with full control over Exchange objects located within their delegated OU.
The roles specified for NetID administration are designed to provide delegated IT staff with visibility into the settings of NetID accounts in Exchange as well as the ability to perform some common tasks on behalf of the users they support such as setting folder permissions or granting send-as rights.

A full list of the PowerShell cmdlets that have been delegated to delegated IT staff can be found at: http://uits.arizona.edu/sites/default/files/DepartmentalITStaffPowerShellAccessstoExchange2013.pdf

Additional information about these commands is available by running get-help <command> in EMS or visiting Microsoft Technet.

**UA Exchange Admin Center for Delegated IT Staff**

Due to the Role Based Access Control (RBAC) configuration for delegated IT staff, the EAC will only display 8 possible topics when a delegated IT staff member is logged in. The tabs available within each topic will also be limited by the RBAC configuration.

Delegated IT staff are granted full read access to many areas of Exchange, but should keep in mind that they will only be able to apply changes to users, contacts, and resources that are in their own scope (their assigned delegated OU and their <DEPT>-NetIDRecipients group). Objects outside a delegated IT staff member’s delegated scope will appear in the interface and all attributes can be viewed, but attempts to apply changes to these objects will fail.

**UAConnect Lync Overview**

Lync 2013 provides Instant Messaging (IM), presence, audio/video chat, web conferencing and persistent chat functionality for UAConnect users. The UAConnect implementation of Lync 2013 features highly available edge, front end and persistent chat pools with a geographically dispersed MS SQL fail over cluster for the backend. The highly available and physical site redundancy enables IM continuity through most schedule maintenance and unexpected disruptions.

**Policies**

**Account Provisioning**

Lync account provisioning is managed via automated processes included in the NetIDSync and EDSSync scripts. All employees are enabled for Lync access at the time of NetID creation, as are DCCs that have requested and are eligible for a mailbox. Retiree’s retain their Lync access in conjunction with their mailbox access.

Student Employees are eligible for Lync access, but requests must be sponsored by a faculty or staff member via a web interface which allows for individual or bulk requests: https://netid.arizona.edu/UaconnectStudentTemp.
**Persistent Chat Rooms**

Delegated IT staff are provided with a Persistent Chat Room category (category names match the associated Delegated OU name) where they are permitted to create and manage Persistent Chat Rooms. Persistent Chat Rooms should follow the UAConnect naming conventions, and when publically visible, should include a description indicating the intended use of the room. This is to improve the end user experience when searching for available Chat Rooms in their Lync Client.

Persistent Chat Rooms are created and managed via the My Rooms web interface:  
https://lync2013fep1.catnet.arizona.edu/PersistentChat/RM?clientlang=en-US

**Federation**

UAConnect supports the configuration of Lync federation with external entities that are partnered with the University or a University department where sharing IM and presence capabilities is a requirement for business needs. Requests for Lync federation requires a support request including detailed descriptions of the business requirements and are handled on a case by case basis.

Lync 2013 federation with Personal Skype is configured and supported. This allows UAConnect Lync users to add Personal Skype users as contacts within their Lync client. It also allows Personal Skype users to add UAConnect Lync users to their contact list. In both cases, the add contact request must be accepted before IM functionality between the two is available. The Personal Skype user must have their Personal Skype account linked to a Microsoft account in order for this federation to work. This allows for IM, presence and audio/video functionality.

**Lync RBAC for Delegated IT Staff**

In addition to the Persistent Chat Categories, delegated IT staff have been granted access to a subset of Lync PowerShell commands that allow them visibility into all Persistent Chat information. This includes being able to retrieve persistent chat policies and configurations as well as retrieve category and specific room information. PowerShell cannot be used for creating new rooms or modifying existing rooms, the My Rooms web interface is required for room creation and modification.

The complete list of PowerShell commands available to delegated IT staff can be found here:  
Module 3: Practical Application and Troubleshooting

Step-by-step Examples of Common Exchange Tasks

Creating Mailboxes

In CatNet you have the ability to create departmental accounts and service accounts.

- Departmental accounts are shared mailboxes to which multiple users have been delegated access such as send-as or full control. All delegates should access departmental accounts via Outlook or OWA. You cannot assign a password to a shared mailbox.
- Service accounts are mailboxes that are used in configuring applications that need to send and/or receive email, such as help desk or monitoring software. Like departmental accounts, access to service accounts may be delegated. Passwords assigned to service accounts should only be shared with the individual who will be configuring the application. Any delegates should access service accounts using their own credentials via Outlook or OWA.

It is important to note that newly created departmental accounts and services accounts in the email.arizona.edu domain will only work internal to UAConnect until an external route is created for them. To request an external route for your departmental or service account complete the Route Requests Form.

Via Exchange Admin Center

Departmental Accounts

1. In the console tree, click Recipient, Shared
2. In the action pane, click the + sign
3. This will create a new user in Active Directory and mail-enable the user; you’ll need to provide the required user account information on the User Information page of this wizard
4. Complete the following fields on the User Information page:

- **Display name:** Use this box to type a display name for the user. This is the name that's listed in Active Directory and the GAL. You will need to manually populate the field with a value beginning with your Department abbreviation followed by a dash and then a descriptive name (i.e. UITS-SupportDesk). The name can't exceed 64 characters
  - **Alias** This is the unique identifier for the account and is not related to additional/alias SMTP addresses.
  - **Specify the organizational unit rather than using a default one:** You will need to set this to your delegated OU in CatNet. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**.

5. On the **Mailbox Settings** page, you will see the following options:

- **Mailbox database:** Do **not** select this option. Because all of the mailboxes in CatNet are treated equally it is best to allow Exchange to select the database automatically.

- **Address book policy:** Do not select this option. The only custom address book policies currently used in UAConnect are for training purposes and applying them will interfere with accessing the default and custom address lists in UAConnect.

6. On the **Archive Settings** page, you will see the following options:
• **Create an on-premises mailbox for this user:** *(This is not available in UAConnect)* Check this box to create a personal (also known as a local or on-premises archive) for the mailbox. Click the browse button to manually select an archive database. If you create a personal archive, mailbox items will be moved automatically from the primary mailbox to the archive, based on the default retention policy settings or those you define.

On the **New Shard Mailbox** page, review your configuration settings. To create the new shared mailbox, click Save.

7. If you intend to take advantage of the default email address policy for departmental and service accounts, once the mailbox is created you will need to set the value of Custom Attribute 1 to “deptacct”. Select the mailbox in the list of shared mailboxes, click the pencil icon and then click the “More options...” link. Under “Custom Attributes” click the pencil icon and enter the value in the first field.

![Shared Mailbox - Internet Explorer](https://mail.kittennet.arizona.edu/kcp/UserGroups/SharedMailbox.aspx?pmcId=188/ReturnObjectType=1&sid=605658)

![Custom Attributes -- Webpage Dialog](https://mail.kittennet.arizona.edu/kcp/UserGroups/EditCustomAttributes.aspx)

**Service Accounts**

7. In the console tree, click **Recipient, Mailboxes**
8. **In the action pane, click the + sign**

On the dialog box, select **User Mailbox**.

9. **This will create a new user in Active Directory and mail-enable the user; you'll need to provide the required user account information on the User Information page of this wizard**
10. Complete the following fields on the User Information page:

- **Alias**: This is the unique identifier for the account and is not related to additional/alias SMTP addresses.
- **Specify the organizational unit rather than using a default one**: You will need to set this to your delegated OU in CatNet. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**.
- **First name**: Use this box to type the first name of the user. This field is optional and should be left blank for departmental and service accounts.
- **Initials**: Use this box to type the initials of the user. This field is optional and should be left blank for departmental and service accounts.
- **Last name**: Use this box to type the last name of the user. This field is optional and should be left blank for departmental and service accounts.
- **Name**: Use this box to type a name for the user. This is the name that’s listed in Active Directory and the GAL. If you use the first name, initials and last name fields this box is automatically populated. Since we are not using those fields for departmental or services accounts you will need to manually populate the field with a value beginning with your Department abbreviation followed by a dash and then a descriptive name (i.e. UITS-SupportDesk). The name can’t exceed 64 characters.
- **User logon name (User Principal Name)**: To complete this field, copy the value you used in the Name. The suffix is the domain name in which the user account resides and should be left as @catnet.arizona.edu (this is NOT the email address for the account).
- **Password**: Use this box to type the password that the user must use to log on to his or her mailbox. It is recommended that the passwords are at least 13 characters long and include upper, lower, numeric and special characters.
- **Confirm password**: Use this box to confirm the password that you typed in the Password box.
- **User must change password at next logon**: This option is selected if you want the user to reset the password when they first logon to the mailbox. This option should **not** be selected for departmental or service accounts.

11. On the **Mailbox Settings** page, you will see the following options:

- **Mailbox database**: Do **not** select this option. Because all of the mailboxes in CatNet are treated equally it is best to allow Exchange to select the database automatically.
- **Address book policy**: Do not select this option. The only custom address book policies currently used in UAConnect are for training purposes and applying them will interfere with accessing the default and custom address lists in UAConnect.

12. On the **Archive Settings** page, you will see the following options:

- **Don't create an archive**: *(this is selected by default and should not be changed)* Click this button if you don't want to create an archive for the mailbox.
• **Create a local archive**: *(This is not available in UAConnect)* Click this button to create a personal (also known as a local or on-premises archive) for the mailbox. If you create a personal archive, mailbox items will be moved automatically from the primary mailbox to the archive, based on the default retention policy settings or those you define.

• **Create a remote hosted archive**: *(This is not available in UAConnect)* Click this button to create a cloud-based archive. To create a cloud-based archive, you must first configure Exchange Online Archiving.

On the New Mailbox page, review your configuration settings. To make any configuration changes, click Back. To create the new mailbox, click Save.

8. If you intend to take advantage of the default email address policy for departmental and service accounts, once the mailbox is created you will need to set the value of Custom Attribute 1 to “deptacct”. Select the mailbox in the list of mailboxes, right click and select properties. On the general tab select “Custom Attributes” and enter the value in the first field.

![Image of Custom Attributes in Exchange Management Shell]

**Via the Exchange Management Shell**

**Departmental Accounts**

1. Open the Exchange Management Shell
2. Enter the following command (Make sure the entire command is on one line):

```
New-Mailbox -UserPrincipalName uits-test@catnet.arizona.edu -Alias uits-test1 -Name "UITS-Test" -DisplayName "UITS-Test" -shared -OrganizationalUnit "catnet.arizona.edu/Delegation/Delegated OUs/UITS/ExchangeTraining/TrainingOU"
```

This command will create a new mailbox named “UITS-Test1” in the TrainingOU. The -shared parameter will disable the active directory account. The mailbox will be active and any user that has been delegated permissions will be able to access the account. This eliminates the security risk of having an account that could be logged into but never is. This parameter should be used only for departmental accounts, not service accounts. You can modify the values for the –UserPrincipalName, -Name, and -DisplayName parameters to create an account with a different name.

3. Enter the following command (Make sure the entire command is on one line):

```
set-Mailbox -Identity uits-test@catnet.arizona.edu -CustomAttribute1 "deptacct"
```

This command will set the CustomAttribute1 value to deptacct which will allow the default email address policy for departmental and service accounts to be applied.

If your departmental account uses an email domain other than email.arizona.edu, do not use this command.

**Service Accounts**

1. Open the Exchange Management Shell
2. Enter the following command (Make sure the entire command is on one line):

```
$Password = Read-Host "Enter password" -AsSecureString
```

This command creates a variable ($Password) that will hold the password information as a secure string to be used in the next command. You will be prompted to enter a value for the password – type it in and press enter. Creating the password variable this way will allow you to include characters that would ordinarily be interpreted as new variables or new parameters in a PowerShell command (i.e. $ or -)

3. Enter the following command (Make sure the entire command is on one line):

```
New-Mailbox -UserPrincipalName uits-test@catnet.arizona.edu -Alias uits-test1 -Name "UITS-Test" -DisplayName "UITS-Test" -OrganizationalUnit "catnet.arizona.edu/Delegation/Delegated OUs/UITS/ExchangeTraining/TrainingOU" -Password $Password
```

This command will create a new mailbox named “UITS-Test1” in the TrainingOU with the password you entered in the previous command. The -shared parameter will effectively disable
the active directory account. The mailbox will be active and any user that has been delegated permissions will be able to access the account. This eliminates the security risk of having an account that could be logged into but never is. This parameter should be used only for departmental accounts, not service accounts. You can modify the values for the -UserPrincipalName, -Name, and -DisplayName parameters to create an account with a different name.

4. Enter the following command (Make sure the entire command is on one line):

   ```
   set-Mailbox -Identity uits-test@catnet.arizona.edu -CustomAttribute1 "deptacct"
   ```

   This command will set the CustomAttribute1 value to deptacct which will allow the default email address policy for departmental and service accounts to be applied.

   If your departmental account uses an email domain other than email.arizona.edu, do not use this command.

**Set Mailbox Permissions**

When you create a new mailbox, Exchange Server uses information from the mailbox store to create the default permissions for the new mailbox. The default folders in the new mailbox inherit permissions from the mailbox itself. Users can modify the permissions on folders in their mailbox using Outlook. Outlook uses MAPI permissions, which Exchange Server automatically converts to Windows Server permissions when it is storing the changes.

Delegated IT Staff have the ability to modify mailbox permissions for departmental and service accounts they have created and for NetID accounts they are responsible for supporting. For more information on how Delegated IT Staff are delegated permissions in UAConnect see “Exchange 2013 PowerShell Access and Commands for Departmental IT Staff (CatNet OU Admins)”

Permissions can be modified via the EAC or the EMS.

**Via Exchange Admin Center (EAC)**

**Set Full Access to a mailbox**

1. In the EAC select the **Recipients** topic and the **Mailboxes** (or **Shared**) tab.
2. In the result pane, select the mailbox or use the Search option above the results to search for the mailbox for which you want to grant “Full Access” permission.
3. Double click the mailbox and in the dialog box select “mailbox delegation”
4. On the Full Access Permission section, click Add (+ symbol on top)
5. In the Select Full Access dialog box search for the user to which you want to grant Full Access permission, and then click Add and OK. On the dialog box it will state “Use this permission to allow anyone other than the mailbox owner to send email from this mailbox
6. Click “save”
7. On the Completion page, the dialog states: Use this permission to allow a delegate to open and view the contents of this mailbox. To allow this delegate to send email from this mailbox you have to assign the delegate the Send As or Send on Behalf Of Permission.
8. Click Save.

Via Exchange Management Shell (EMS)

1. Open the Exchange Management Shell
2. Enter the following command (Make sure the entire command is on one line):

   ```powershell
   Add-MailboxPermission "Anna Nicole" -User "James DeBarge" -AccessRights FullAccess
   ```

   This example grants the user James DeBarge Full Access permission to Anna Nicole’s mailbox. In the TrainingNetID OU you will find other users you can practice setting permissions on.

Set Mailbox Folder Permissions

End users have the ability to set permissions to individual folders within their mailbox via the Outlook client. Delegated IT Staff have also been delegated the ability to set permissions on folders within mailboxes that they either created (departmental or service accounts) or are responsible for supporting. For more information on how Delegated IT Staff are delegated permissions in UAConnect see “Exchange 2013 PowerShell Access and Commands for Departmental IT Staff (CatNet OU Admins)”

Folder level permissions can only be administratively set via the EMS.

Via Exchange Management Shell

1. Open the Exchange Management Shell
2. Enter the following command (Make sure the entire command is on one line):

   ```powershell
   Add-MailboxFolderPermission -Identity "trn-annanicole:\calendar" -User "trn-sherlinejoans" -AccessRights Owner
   ```

   This example grants the user Sherline Joans Owner rights to Anna Nicole’s calendar.

   ```powershell
   Set-MailboxFolderPermission -Identity "trn-annanicole:\calendar" -User "trn-sherlinejoans" -AccessRights Reviewer
   ```

   This example changes Sherline Joans’ rights on Anna Nicole’s calendar to Reviewer

   ```powershell
   Remove-MailboxFolderPermission -Identity "trn-annanicole:\calendar" -User "trn-sherlinejoans"
   ```

   This example removes Sherline Joans’ rights on Anna Nicole’s calendar.
Set Send-as Access to a mailbox

Send-as permissions allow users other than the mailbox owner to send messages that appear as if they were sent by the mailbox owner. This is useful when working with departmental accounts and it can also be useful for admin assistants who directly manage another user’s mailbox. Users cannot set send-as permissions on their own mailbox via their client, but an administrator can set send-as permissions via both the EMC and the EMS.

Via Exchange Admin Center

1. In the EAC select the **Recipients** topic and the **Mailboxes** (or **Shared**) tab.
2. In the result pane, select the mailbox or use the Search option above the results to search for the mailbox for which you want to grant **Send as Permission** (you can also set the Send on Behalf and Full access). You can manage Send As permission for the following recipient types:
   - Discovery mailboxes
   - User mailboxes
   - Resource mailboxes
3. Double click the mailbox and in the dialog box select “mailbox delegation”
4. On the **Send As Permission** dialog, select the users or groups to which you want to grant the Send As permission or from which you want to remove the permission.
   - **Add (+)**: Click this button to open the **Select User or Group** dialog box. Use this dialog box to select the users or groups to which you want to grant the Send As permission.
   - **Remove (-)**: Select a user or group, and then click this button to remove the Send As permission from that user or group.
5. On the **Completion** page, the dialog states: Use this permission to allow anyone other than the mailbox owner to send email from this mailbox.
6. Click Save.

Via Exchange Management Shell

Use the **Add-ADPermission** cmdlet to manage Send As permissions for a mailbox. When you use the **Add-ADPermission** cmdlet, you must specify the name of the mailbox on which the Send As permission should be added and the mailbox that should be granted the permission. Because the **Add-ADPermission** cmdlet controls many permissions, you must also specify the Send As permission with the **ExtendedRights** parameter.

1. Open the Exchange Management Shell
2. Enter the following command (Make sure the entire command is on one line):

```
Add-ADPermission "Rachel Norton" -User "catnet\trn-samanthakenwald" -ExtendedRights "Send As"
```

This command will allow the user Samantha Kenwald to send as the user Rachel Norton. Note that this command will only accept the DisplayName value when specifying the mailbox on which send-as rights will be added.
Set Send on Behalf of Access to a Mailbox

Send on behalf of access is similar to send-as access in that it permits users to send messages from a mailbox for which they are not the owner. However, when a user sends a message using send on behalf of rights the recipient of the message will clearly see that the message was sent from one user on behalf of another user. The end user can use delegation options within Outlook to configure send on behalf of rights, or an administrator can use either EAC or EMS to configure a user to send on behalf of another user.

Via Exchange Admin Center

1. In the EAC select the Recipients topic and the Mailboxes (or Shared) tab.
2. In the result pane, select the mailbox or use the Search option above the results to search for the mailbox for which you want to grant Send on Behalf.
3. Double click on the mailbox and choose Mailbox Delegation.
4. On the Send on Behalf dialog, select the users or groups to which you want to grant the Send on Behalf permission or from which you want to remove the permission.
   - Add (+): Click this button to open the Select User or Group dialog box. Use this dialog box to select the users or groups to which you want to grant the Send As permission.
   - Remove (-): Click this button to open the Select Usr or Group dialog box to remove the send on Behalf permission from that user or group.
5. Click the Add button (+)
6. Select the user(s) you wish to grant access to and click Ok
7. On the completion page it states: If you use this permission the From address in any message sent by the delegate indicates that the message was sent by the delegate on behalf of the mailbox owner
8. Click Save.

Via Exchange Management Shell

3. Open the Exchange Management Shell
4. Enter the following command (Make sure the entire command is on one line):

   ```powershell
   Set-Mailbox “trn-JasonShay” -GrantSendOnBehalfTo “trn-JennaGreen”
   ```

   This command will allow Jenna Green to send on behalf of Jason Shay. Note that using this command will replace any users that currently have send on behalf of rights with only Jenna Green.

   If one or more users have already been granted send on behalf of rights to an account, use the following command to grant send on behalf of rights to additional users:

   ```powershell
   Set-Mailbox “trn-JasonShay” -GrantSendOnBehalfTo @{add=”trn-JennaGreen”}
   ```
This command will also allow Jenna Green to send on behalf of Jason Shay, but it will not replace any existing users that already have send on behalf of rights to Jason Shay’s mailbox.

**Rename Existing Accounts**

Changing business needs in a dynamic environment can make it necessary to rename an account to better reflect current operations. Delegated IT staff have the ability to rename the departmental or service accounts they have created.

*Via Exchange Admin Center*

1. In the EAC select the **Recipients** topic and the **Mailboxes** (or **Shared**) tab.
2. In the result pane, select the mailbox or use the Search option above the results to search for the mailbox for which you want to rename. Double click on the mailbox or select the edit on the top icons menu.
3. On the dialog box you may need to change the: First Name, Initial, Last Name, Display Name, the Alias and the User logon name.

4. After the name has been changed in all the appropriate fields you can hit save and the e-mail address policy should pick up the new Alias and modify the default smtp address.
5. You will still have the old SMTP address and can leave it on the account for whatever period of time is deemed necessary before removing it.

*Note: E-mail to the previous address will continue to come into the renamed account until the old SMTP Address is removed. New email.arizona.edu addresses require a request for a new route before external senders can send to them ([Route Requests Form](#)).

**Via Exchange Management Shell**

1. Open the Exchange Management Shell.
2. Enter the following command (Make sure the entire command is on one line):

   ```
   set-Mailbox -Identity uits-test1@catnet.arizona.edu -Alias uits-dev1 -Name "UITS Dev1" -UserPrincipalName "uits-dev1@catnet.arizona.edu" -DisplayName "UITS Dev1"
   ```

   This command will rename the UITS Test1 account to UITS Dev1. As long as an email address policy is applied to the account the email addresses will be automatically updated to include aliases with the new name (the aliases with the old name will still be on the account).

   *Note: E-mail to the previous address will continue to come into the renamed account until the old SMTP Address is removed. New email.arizona.edu addresses require a request for a new route before external senders can send to them ([Route Requests Form](#)).

**Configuring Additional SMTP Addresses**

In some cases it is necessary to configure a mailbox with additional SMTP addresses that are not automated by the Exchange e-mail address policies. For example, this may be required for a single account that has multiple @email.arizona.edu addresses or when merging two or more accounts for
business reasons. In these cases the additional SMTP addresses can be manually added to the account via EAC or EMS.

Via Exchange Admin Center

1. In the EAC select the Recipients topic and the Mailboxes (or Shared) tab.
2. In the result pane, select the mailbox or use the Search option above the results to search for the mailbox for which you want to configure additional SMTP addresses for. Double click on the mailbox and select “email address”.
3. On the Email Addresses dialog box click the “Add (+)...” icon
4. A new window will be displayed prompting you to enter the additional SMTP address

5. After clicking “OK” you will be returned to the E-Mail Addresses Tab where the additional address is displayed in the list of SMTP addresses. This can be repeated as many times as necessary
Note that the “Set as Reply” option is not available as long as the “Automatically update e-mail addresses based on the-mail address policy applied to this recipient” option is selected. If you need one of the additional SMTP addresses to be the reply to address for the account you need to double click the SMTP address that you want to be the reply address and select in the dialog box: “Make this the reply address”. Be aware that if any central changes to e-mail address policy are made they will NOT apply to your account.

Via Exchange Management Shell

1. Open the Exchange Management Shell
2. Enter the following command (Make sure the entire command is on one line):

   ```
   Set-mailbox UITS-Test1 -EmailAddresses @{add="test1@email.arizona.edu"}
   ```

   This command will add `test1@email.arizona.edu` to the list of SMTP addresses on the UITS-Test1 mailbox. It does not modify the “Set as Reply” or “Automatically update e-mail addresses based on e-mail address policy” options.

3. If you need to add an address and set it as the reply address use the following commands instead (Make sure the entire command is on one line):

   ```
   Set-mailbox UITS-Test1 -EmailAddresses @{add="test1@email.arizona.edu"} -EmailAddressPolicyEnabled $false
   Set-mailbox UITS-Test1 -PrimarySmtpAddress test1@email.arizona.edu
   ```

   The first command adds `test1@email.arizona.edu` to the list of SMTP addresses on the UITS-Test1 mailbox and disables the “Automatically update e-mail addresses based on e-mail address policy” options. The second command sets the new `test1@email.arizona.edu` address as the reply to address for the account.
Remove an Existing Account

If a mailbox is no longer in use, it should be removed from Exchange in order to make best use of the storage resources available. You can remove an existing user’s mailbox only, leaving the Active Directory account or delete both the Active Directory account and mailbox. Delegated IT staff have been delegated the ability to do both for departmental or service accounts they have created.

Remove mailbox via Exchange Admin Center

The following will remove the Exchange mailbox leaving the Active Directory account intact:

1. In the EAC select the **Recipients** topic and the **Mailboxes** (or **Shared**) tab.
2. In the result pane, select the mailbox or use the Search option above the results to search for the mailbox you want to remove. Click on the account,

   ![Exchange Admin Center](image)

   Click the top icon “**More**” ⋯ and then click **Disable**. (In this More ⋯ selection you have also menu items to export the mailbox to a file, connect a disconnected mailbox, and also to run and advanced search)

3. Click yes on the dialog box telling you that the Exchange mailbox will be disabled.

   ![Warning](image)

4. The mailbox is now removed from the Active Directory account

Remove mailbox via Exchange Management Shell

1. Open the EMS and type the following command:
Disable-Mailbox -Identity catnet\uits-test1

Type y at the prompt if you are sure

This command will remove all Exchange attributes from the account UITS test1 and mark the mailbox for deletion. It will leave the Active Directory account intact.

**Remove Exchange mailbox and delete the Active Directory account via Exchange Admin Center**

1. In the EAC select the **Recipients** topic and the **Mailboxes** (or **Shared**, or **Resources**) tab.
2. In the result pane, select the mailbox or use the Search option above the results to search for the mailbox you want to remove. Select the account, select the trash bin icon on the top icon selection

![Exchange admin center](image)

and select Delete on the dialog box

3. Click Yes on the dialog box telling you that the Active Directory account will be removed and the Exchange mailbox deleted
4. The Exchange mailbox and Active Directory accounts are now removed

**Remove Exchange mailbox and delete the Active Directory account via Exchange Management Shell**

1. Open the EMS and type the following command:

```
Remove-Mailbox -Identity catnet\uits-test1
```
Type y at the prompt if you are sure

This command will remove all Exchange attributes from the account UITS Test1, mark the mailbox for deletion and remove the Active Directory account.

Create Room Resources and Equipment Resources

A room mailbox is a resource mailbox assigned to a meeting location, such as a conference room, auditorium, or training room. An equipment mailbox is a resource mailbox assigned to a resource that's not location specific, such as a portable computer, projector, microphone, or a company car. Only one room resource can be included in a meeting request; however multiple equipment resources can be included. You can use the Exchange Admin Center (EAC) and the Exchange Management Shell to create a room or equipment mailbox.

Via Exchange Admin Center

1. Click on Recipients, Resources, Add (+) and select Room Mailbox

2. Select Room Mailbox or Equipment Mailbox and click Next

3. On the Mailbox Information page, complete the following fields:
   - **Specify the organizational unit rather than using a default one**: You will need to set this to your delegated OU in CatNet. To select a different OU, click **Browse** to open the Select Organizational Unit dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**.
   - **Room Name** Use this box to type a name for the user. This is the name that's listed in Active Directory. By default, this box is populated with the names you enter in the First name, Initials, and Last name boxes – since we are not using those fields type in a value beginning with your Department abbreviation, followed by a dash (-) and then a descriptive name (i.e. UITS-Room555, UITS-ConfPhone1). The name can't exceed 64 characters
4. On the **Mailbox Settings** page, complete the following fields:

- **Alias**  The alias will be populated with the value from the Name field on the previous screen by default. The alias can't exceed 64 characters and must be unique in the forest.
- **Specify the mailbox database rather than using a database automatically selected**: You should not select this option. Because all of the mailboxes in CatNet are treated equally it is best to allow Exchange to select the database automatically.
- **Exchange ActiveSync mailbox policy**  Leave this box un-checked and allow the default ActiveSync policy to be applied.
- **Address book policy**  Leave this box un-checked and allow the default address book policy to be applied.

5. On the **New Mailbox** page, review your configuration settings. Click **Save** to create the mailbox.

6. After is created open it with the edit icon on top resembling a pencil (see pic below) to add or change functionality on the mailbox (hide from address list, attributes, booking delegates, booking options, contact information, email address, MailTips and Mailbox Delegation)
To create a Room Mailbox:

```
new-mailbox -alias "UITS-Room-555" -Name "UITS-Room-555" -OrganizationalUnit "catnet.arizona.edu/Delegation/Delegated OUs/UITS/ExchangeTraining/TrainingOU" -UserPrincipalName "UITS-Room-555@catnet.arizona.edu" -room -ResourceCapacity 10
```

This command creates the room resource UITS-Room-555 in the TrainingOU and sets the capacity of the room to 10.

To create an Equipment Mailbox:

```
new-mailbox -alias "UITS-ConfPhone1" -Name "UITS-ConfPhone1" -OrganizationalUnit "catnet.arizona.edu/Delegation/Delegated OUs/UITS/ExchangeTraining/TrainingOU" -UserPrincipalName "UITS-ConfPhone1@catnet.arizona.edu" -equipment
```

This command creates the equipment resource UITS-ConfPhone1 in the TrainingOU.

**Resource Mailbox Properties**

There are a number of settings that are configurable for resource mailboxes. Room and Equipment mailboxes share the same configuration setting. The settings can be modified via either the EAC or the EMS.

**Via Exchange Admin Center**

Here is a brief description of the different settings you can configure on the properties tabs of a resource mailbox.
- **Resource General** - This tab allows you to configure resource custom properties as well as the resource capacity value. Additionally, it is on this tab that you configure whether you enable the Resource Booking Attendant for this mailbox or not.

![Resource General Tab](image)

- **Booking Delegates** – Use this section to change or view the reservation and who can accept or decline requests if it isn’t done automatically.

![Booking Delegates Tab](image)

- **Booking Options** – Use this section to specify when this room can be scheduled and maximum booking lead dates, maximum duration in hrs., a message to the organizer if a reply is needed, and how far in advance the room can be reserved.

![Booking Options Tab](image)
- **Contact Information** – Contact information for the room.

- **Email Address** – Default reply email address and policy update.
- **MailTip** – Displays when sending email to this user to warn of potential issues. i.e response delay.

- **Mailbox Delegation** – Permissions for Send As, Send on Behalf and Full Access. Tip: Full access allows a delegate to open and view the contents of the mailbox. To allow the delegate to send email from this mailbox, you have to assign the Send As or the Send on Behalf Of permission
See scheduling permissions for a room mailbox: http://technet.microsoft.com/en-US/library/ms.exch.eac.EditRoomMailbox_ResourceDelegates(EXCHG.150).aspx?v=15.0.847.30&l=0. In the EAC on the “Me tile” upper right corner where your login name is, change it to select the Room mailbox (i.e. UITS-Room-555) and all the Options for the room mailbox will be displayed, where you can change the behavior of the mailbox. (account, organize email, groups, site mailboxes, settings, phone, block or allow and apps.)
Via Exchange Management Shell

1. Open the Exchange Management Shell
2. Enter the following command (Make sure the entire command is on one line):

   ```
   Set-CalendarProcessing -Identity "UITS-Room-555" -AutomateProcessing AutoAccept -DeleteComments $true -AddOrganizerToSubject $true -AllowConflicts $false -AllowRecurringMeetings $true -BookingWindowInDays 1080 -DeleteNonCalendarItems $true -TentativePendingApproval $true
   ```

   This command will set the calendar for the room named “UITS-Room-555” to auto-accept invitations, to remove all details in the body of the invitation, add the meeting organizer to the subject line of the meeting, to disallow conflicting appointments, to allow recurring meetings, to allow the resource to be reserved for up to 1080 days in the future, to delete all non-calendar items from the resource mailbox and to mark pending items as tentative on the calendar.

   ```
   Set-CalendarProcessing -Identity "UITS-Room-555" -ResourceDelegates "UITS-Group1"
   ```

   This command will set all members of the group “UITS-Group1” as delegates for the room “UITS-Room-555”

   ```
   Set-CalendarProcessing -Identity "UITS-Room-555" -ResourceDelegates "trn-Robertlowry"
   ```

   This command will set the user Robert Lowry as the only delegate for the room “UITS-Room-555”

   ```
   Add-MailboxFolderPermission 'UITS-Room-555:\non_ipm_subtree\freebusy data' -User trn-Robertlowry -AccessRights PublishingEditor
   ```

   This command provides Robert Lowry with sufficient rights to access and modify the free/busy data for the room “UITS-Room-555”

Creating Distribution Groups

There are two types of groups that can be used to distribute messages:

- **Mail-enabled universal distribution groups** (also called distribution groups) can be used only to distribute messages.
- **Mail-enabled universal security groups** (also called security groups) can be used to distribute messages as well as to grant access permissions to resources in Active Directory. For more information, see Manage Mail-Enabled Security Groups.

It’s important to note the differences between Active Directory and Exchange. In Active Directory, a distribution group refers to any group that doesn’t have a security context, whether it’s mail-enabled or
In contrast, in Exchange, all mail-enabled groups are referred to as distribution groups, whether they have a security context or not.

Distribution groups can be created in either the EAC or EMS, however, it is recommended that they be created in the EMS as this method is generally quicker. Techniques for creating Standard and Dynamic groups in EAC and EMS are below:

Creating Standard Distribution Groups in EAC

1. Open EAC and navigate to Recipients\Groups
2. Click the plus sign (+) and select “Distribution Group”
3. Select Distribution group as the Group Type if you intend to use this group only to send/receive email messages. Select Security as the Group Type if you intend to use this group to configure permissions on Exchange objects (i.e. mailboxes, calendars, or rooms) as well as to send/receive email messages. Select Dynamic Distribution group if the recipients are modified dynamically every time according to filters set (custom attributes), instead of a defined set of recipients.
4. Specify an Organization Unit rather than using a default one. Click browse.
5. Select the Departmental OU this Group should be placed in, then click OK
6. Enter a Name for the group under Display Name, this should be in the format <dept>-<group> (i.e. UITS-Testing). This is the name that will appear in the Address Book.
7. Enter the Name again under Alias.
8. Ensure that all the fields are properly filled.
9. Click Next, and then Save. This will create the Distribution Group.
10. Click the Email Options tab and click on the “+” button and select any Email Addresses other than groupname@distribution.arizona.edu. Click the “–“ button to remove them. Then hit save.
11. Once the group is created, users can be added on the “Membership” selection of the Group Properties
12. To set the custom attribute’s value (distgroup) for the group you need to set it using PowerShell since is no longer available in the GUI for Standard Distribution groups.
Creating Standard Distribution Groups in EMS

1. Open the Exchange Management Shell
2. Enter the following command (Make sure the entire command is on one line):

   ```bash
   New-distributiongroup "UITS-Group1" -organizationalunit "catnet.arizona.edu/Delegation/Delegated OUs/UITS/ExchangeTraining/TrainingOU" -primarysmtpaddress uits-group1@distribution.arizona.edu
   ```
3. Once the command has completed, enter the following command to set the Custom Attribute:

   ```bash
   Set-distributiongroup UITS-Group1 -customattribute1 'distgroup'
   ```
4. Users can be added to the group in EMS using the following command

   ```bash
   add-distributiongroupmember UITS-Group1 -member trn-jasondaniels, trn-kennywald, trn-lesyaannson
   ```

Creating Dynamic Distribution Groups in EAC

Dynamic Distribution Groups can be created in both the EAC and EMS, however, EMS allows much greater flexibility when building conditions for dynamic groups. To create a Dynamic Distribution Group in EAC, do the following:

1. Open EAC and navigate to Recipients\Groups
2. Click the “+” and select “Dynamic Distribution Group”
3. Enter the group name under Display Name and Alias in the format <dept>-<group> (i.e. UITS-Group1) and click Next
4. If the users that should belong to the group are in a single OU, click Browse to select the OU where the users are located.
5. Select All Recipient Types,
6. The Membership section allows you to set specific conditions (rules) that determine the members of the group if they are not all grouped by OU. In order for the Conditional Group Member system to work, the users must have the attributes selected as part of their user account. For instance, if the group will hold all members with a Custom Attribute of User, all users that are to belong to the group should have the Custom Attribute setting on their mailbox set to equal User. Enter “distgroup” without quotes into the field labeled Custom Attribute 1 and hit “Save”
7. Once the group is created, select it (double click) in the list of Distribution groups, and then you can review/modify all settings on the Dynamic Distribution Group created if needed.
Creating Dynamic Distribution Groups in EMS

Creation of Dynamic Distribution Groups in EMS is significantly more complex than creating them in EAC, but is much more flexible since any Active Directory Attribute can be used as a part of the filter to limit the users in the group. For instance, you can create a Distribution Group that only includes users that have the First Name of Sam. This is referred to as Recipient Filtering. Because of the complexity of this topic, this guide will not cover it, but will focus instead on using the EMS to create a dynamic group that uses an OU or Custom Attribute to limit membership. It is possible to learn more about using recipient filtering here: [http://technet.microsoft.com/en-us/library/bb124268.aspx](http://technet.microsoft.com/en-us/library/bb124268.aspx)

1. Open the EMS and enter the following Command to create a Dynamic Distribution Group (All commands should be entered on the same line):

To limit Membership with an OU:

```
New-dynamicdistributiongroup UITS-DynGroup1 –includedrecipients allrecipients –organizationalunit “catnet.arizona.edu/Delegation/Delegated OUs/UITS/ExchangeTraining/TrainingOU” –recipientcontainer “catnet.arizona.edu/Delegation/Delegated OUs/UITS/ExchangeTraining/TrainingNetID” –primarysmtpaddress UITS-DynGroup1@distribution.arizona.edu
```

To limit Membership with a Custom Attribute:

```
New-dynamicdistributiongroup UITS-DynGroup2 –includedrecipients allrecipients –organizationalunit “catnet.arizona.edu/Delegation/Delegated OUs/UITS/ExchangeTraining/TrainingOU” –conditionalcustomattribute1 ‘deptacct’ –primarysmtpaddress UITS-DynGroup2@distribution.arizona.edu
```

2. Once the group is created, run the following command to add the necessary custom Attribute to it:

```
Set-distributiongroup UITS-DynGroup2 –customattribute1 ‘distgroup’
```

Remove Distribution Groups

Via Exchange Admin Center

1. In the console tree, navigate to Recipients/Groups.
2. In the result pane, select the distribution group that you want to remove.
3. In the action pane, under the name of the distribution group, click on the “garbage can“ icon.
4. A warning appears confirming that you want to remove the distribution group. Click Yes.
Via Exchange Management Shell

1. Open the Exchange Management Shell
2. Enter the following command (Make sure the entire command is on one line):

   `Remove-DistributionGroup -Identity "UITS-Test"`

   This example removes the distribution group UITS-Test.

Creating Contacts

Contacts essentially provide a pointer to an external email address. Contacts are the only way you can include external email addresses in an Exchange distribution group. Delegated IT staff are free to create contact objects within their OU, however, it is required that all contact objects created in CatNet have a unique alias containing a character invalid in NetID (i.e. dash (-), underscore (_), or period (.) and be hidden from Exchange address lists.

Via Exchange Admin Center

1. In the console tree, click Recipients/Contacts.
2. In the action pane, click the “+” icon and select “Mail Contact”
3. Complete the following fields on the Contact Information page:
   - **Specify the organizational unit rather than using the default one:** You will need to set this to your delegated OU in CatNet. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**.
   - **First name** Use this box to type the contact’s first name. This field is optional.
   - **Initials** Use this box to type the contact’s initials. This field is optional.
   - **Last name** Use this box to type the contact’s last name. This field is optional.
   - **Display Name** Use this box to type a name for the contact. This is the name that’s listed in Active Directory. By default, this box is populated with the names you enter in the **First name, Initials, and Last name** boxes. If you didn’t use those boxes, you must still type a name in this field. The name can’t exceed 64 characters.
• **Alias** Use this box to type a unique alias (64 characters or less) for the contact. This field is required and should contain at least 1 character that is illegal in UA NetID (i.e. dash (-), underscore (_), period (.)).

• **External email address** Type the external email address

4. Click **Save** to close the wizard.
5. Find the contact you just created, double click on it and choose the various menu items to change the properties (General, Contact Information, Organization, email options and MailTip.
6. Note: “Hide from Exchange address list” has to be done using the EMS

**Via Exchange Management Shell**

1. Open the Exchange Management Shell
2. Enter the following command (Make sure the entire command is on one line):

   ```powershell
   New-MailContact -Name "Ted.Bremer" -ExternalEmailAddress ted@tailspintoy.com -OrganizationalUnit "catnet.arizona.edu/Delegation/Delegated OUs/UIITS/ExchangeTraining/TrainingOU"
   ```

   This command creates a mail contact for Ted Bremer.

   ```powershell
   Set-MailContact -identity "Ted.Bremer" –HiddenFromAddressListsEnabled $true
   ```

   This command hides Ted Bremer’s contact object from Exchange address lists.

**Configuring Internet Calendar Sharing**

Internet calendar sharing is available on a user’s calendar in Outlook Web App (OWA) or Outlook. A user logged in OWA right clicks on the Calendar, and chooses Share Calendar:

![Internet Calendar Sharing](image)

Start typing the email of any person and the “Search contacts & directory” opens up where you can select your desired contacts. If it’s an external contact you can start typing the external address. On the
right hand of the email address of each contact there is a selection box where you can select: Availability only, Limited details, Full details, Editor and Delegate.

The internal user will receive an invitation in his mailbox to see your calendar. You can click on the “add calendar” link sent to add it to your mailbox.

An external user will open the links received in an email to see the calendar. Publishing the calendar generates two URLs - one to view the Calendar in a web browser and one to subscribe to the calendar (a link to the calendar.ics file that can be added to most email programs or webmail clients like Gmail). Internet Calendar Sharing can be disabled anytime by clicking on the calendar and selecting the permissions option where it will show you the list of users that you share the calendar with. Remove the user or change the options on the sharing permissions. In the public calendar you can select “Not shared” to stop publishing the calendar.
Calendar sharing in OWA link:
Calendar added as an .ics calendar in Outlook:

External users who have been provided the link to view a published calendar in a web browser are completely anonymous and have no direct access to the publishing users’ calendar or other mailbox data. They don’t require an access to a calendar reader, only access via HTTP to the Internet and the recipient’s Exchange Server.

It should be noted that users cannot configure this option for a mailbox other than their own, even if they have been granted full control of the other mailbox. For example, if there is a requirement to internet publish the calendar for a resource account, delegates on the resource account will NOT be able to access the options to publish the calendar in OWA. Instead, a delegated admin will need to run the following PowerShell commands:

```
Set-MailboxCalendarFolder <mailbox name>:\Calendar -PublishEnabled $true
Get-MailboxCalendarFolder <mailbox name>:\calendar |fl
```

The first command enables internet publishing for the calendar while the second command returns (among other information) the HTML and ICS URLs for internet viewing and subscription respectively.

You’ll notice the default result of this command is to publish “AvailabilityOnly”. If a different level of detail visibility is required, use the -DetailLevel parameter on the set-mailboxcalendarfolder command with one of the following options:

- AvailabilityOnly, LimitedDetails, FullDetails, Editor
Advanced PowerShell Examples

In the previous step by step examples you had the opportunity to practice basic Exchange PowerShell commands. The basic commands allow you granular control over creation, manipulation and deletion of individual Exchange objects. More advanced PowerShell commands will allow you to administer objects based on output from other commands, search criteria, and file content among other things. This section provides some examples of more advanced PowerShell commands.

Bulk Set Custom Attribute

1. Open the Exchange Management Shell
2. Enter the following command (Make sure the entire command is on one line):

```powershell
get-distributiongroup -OrganizationalUnit "catnet.arizona.edu/Delegation/DelegatedOUs/UITs/ExchangeTraining/TrainingOU" -filter {alias -like 'UITs-*'} | set-distributiongroup -customattribute1 'distgroup'
```

This example searches the TrainingOU for all distribution groups that begin with “UITs-“ then sends the results of the search to another command which sets the custom attribute 1 value to “distgroup”. This will enable you to quickly configure your distribution groups to get the default email address policy for distribution groups.

Bulk Create Room Accounts

1. Create a CSV file in the root of c:\ with the following column format: Dept, No, Capacity, Phone
2. Enter several rows of data in the CSV where Dept=department abbreviation, No=room number, Capacity=total number of people the room can hold, Phone=phone number for the room.
3. Open the Exchange Management Shell
4. Enter the following command (Make sure the entire command is on one line):

```powershell
import-csv c:\rooms.csv | foreach {new-mailbox -alias "$(__Dept)-Room-$(__No)" -Name "$(__Dept)-Room-$(__No)" -OrganizationalUnit "catnet.arizona.edu/Delegation/DelegatedOUs/UITs/ExchangeTraining/TrainingOU" -UserPrincipalName "$(__Dept)-room-$(__No)@catnet.arizona.edu" -room -ResourceCapacity $_.Capacity -phone $_.Phone}
```

This command imports the data from the CSV file you created and sends it to a command that will create a new room resource in the TrainingOU for each line in the CSV. It will set all the required parameters for the room resources as well as populating the optional capacity and phone number attributes for each room.

Bulk Configure Calendar Processing

1. You can use the same CSV created for “Bulk Create Room Accounts, or create a new one that contains the column format: Dept, No
2. Open the Exchange Management Shell
3. Enter the following command (Make sure the entire command is on one line):

```
import-csv c:\rooms.csv | foreach {Set-CalendarProcessing -Identity "${_._Dept}-Room-${_._No}" -AutomateProcessing AutoAccept -DeleteComments $true -AddOrganizerToSubject $true -AllowConflicts $false -AllowRecurringMeetings $true -BookingWindowInDays 0 - DeleteNonCalendarItems $true -TentativePendingApproval $true}
```

This command imports the data from the CSV file you created and attempts to set calendar processing parameters for the rooms on each line of the CSV file. This command can be used if you have standard calendar processing requirements you’d like to set for a large number of rooms.

**Step-by-step Examples of Lync Persistent Chat Room Management**

**Creating a new chat room**

1. Browse to the “My Rooms” web URL: https://lync2013fep1.catnet.arizona.edu/PersistentChat/RM?clientlang=en-US
2. When the Web interface launches, you will be prompted for credentials. Use your Delegated IT staff credentials to login
3. Click the "Create a new room" button
   - In the ‘Room name’ field enter a room name following naming conventions (i.e. UITS-PCRM-Test1)
   - Under ‘Privacy’ select the radio button for “closed”
   - If you see a ‘Category’ option, select the appropriate category for your department (note: you will only see a Category option if your account is authorized to create persistent chat rooms in multiple categories)
   - Under ‘Managers’ enter the delegated IT staff account(s) that should be permitted to manage the chat room (note: this field should already be populated with your delegated IT staff account. When searching for an account you can use first name, last name, or login name but be aware that the information entered must be specific enough to return only 1 match)
   - Under ‘Members’ enter the NetIDs of the users who will be allowed to participate in the chat room
   - Click the ‘Create’ button to complete the creation of your new room

**Managing an existing chat room**

1. Browse to the “My Rooms” web URL: https://lync2013fep1.catnet.arizona.edu/PersistentChat/RM?clientlang=en-US
2. When the Web interface launches, you will be prompted for credentials. Use your delegated IT staff credentials to login
3. Under ‘My Rooms’ you should see any rooms you created as well as any rooms you have been added as a manager to.
4. Hover over the room you want to manage and click the "edit" icon
5. Modify any of the field you would like to change and click the “commit changes” button
Appendix A: Infrastructure Diagrams

CatNet Infrastructure Diagram

UAConnect Mail flow Diagram
NetID Sync to CatNet Data Flow Diagram

- NetID to Active Directory synchronizations are near real time.
- New NetID creation by users is managed by the NetID process. The data is then sent to a web service that is polled by a Windows task to retrieve the information used to populate the user accounts in Active Directory.
- No Bio/Demo data is included. The records consist of NetID, Name, Password, and basic affiliation (Student or Employee).
- The service is also used to propagate password changes, NetID changes, and NetID deletions.
- Initial email routes are added/updated for employees and students.
- Processes approved student-employee UAConnect account creations.
**EDS Sync to CatNet Data Flow Diagram**

- EDS is updated nightly from Uaccess Student and Uaccess Employee (12 am – 6 am).
- Active Directory pulls data from EDS starting at 7 am.
- Active Directory checks/updates every NetID based off the EDS data. This process:
  - Has a 12-15 hour run time.
  - Writes current bio/demographic data to NetID based AD user accounts.
  - Checks existing mail routes and updates/removes as needed.
  - Creates/deletes ULDAP account as needed.
  - Creates Exchange mailbox/sync account if needed with proper EDU attributes.
  - Disables AD accounts and removes mailboxes.
Appendix B: IronPort

Overview

The University of Arizona has 6 Cisco IronPort appliances providing e-mail edge services for UACconnect as well as a Security Management Appliance.

The 6 appliances are configured in a DNS round robin for load balancing purposes. It is important to understand that this will not balance load based on any performance metrics of the individual appliances; mail will simply be routed to the next available appliance which may lead to delays on one appliance that are not experienced on others.

Mailgator.email.arizona.edu: this DNS name includes all inbound interfaces on the IronPort appliances

Smtpgate.email.arizona.edu: this DNS name includes all outbound interfaces on the IronPort appliances

The IronPort appliances provide SPAM and virus filtering for both inbound and outbound email. SPAM filtering is based on email sender reputation, web reputation and the Cisco Context Adaptive Scanning Engine (CASE). Messages that are positively identified as SPAM are quarantined while messages that are suspected of being SPAM are marked with a [SPAM?] tag in the subject line and delivered as usual. Virus filtering is done using Sophos Anti-Virus. Repaired messages, encrypted messages and unscannable messages are all delivered as usual with anti-virus scan results appended to the headers. Virus infected messages are dropped entirely.

In addition to providing SPAM and virus filtering for UACconnect, the IronPorts are also configured to provide Encryption and Data Loss Prevention services.

Encryption

Cisco provides email encryption via their Cisco Registered Envelope Service. This is an external service that requires an additional set of credentials in order for users to access encrypted mail messages they have received. Encryption is enabled for UACconnect and may be triggered by adding any one of the following tags to an outgoing message subject (note that the brackets must be included and the tags are case sensitive):

- [encrypt]
- [Encrypt]
- [ENCRYPT]
- [secure]
- [Secure]
- [SECURE]

Because this encryption method relies on a content filter on the IronPort appliances, it cannot be used to encrypt mail messages sent from one UACconnect mailbox to another UACconnect mailbox.
Data Loss Prevention (DLP)

Data Loss Prevention (DLP) allows policies to be applied that will prevent sensitive data from leaving the organization. Cisco provides a wide range of templates spanning a number of categories to include Regulatory Compliance, Acceptable Use, Privacy Protection and several others. Each template requires customization in the form of regular expression filters in order to correctly identify the sensitive data it is meant to protect. DLP is currently enabled in UAConnect, but there are no DLP policies defined at this time.