KETS Office365 Operations Guide

Kentucky Department of Education

Version 2.6 *9/29/2015*

Contents

Change Log 1
1 Introduction 3
1.1 Audience 3
1.2 Technologies/Terminologies 4
1.3 Document Feedback 8
1.4 Document Updates/Location 8
2 Support/Troubleshooting 9
2.1 Downloads 9
2.2 District Level Management/Troubleshooting 10
2.2.1 District Troubleshooting Checklist 12
2.2.2 Case Workflow 13
2.3 Contacting Premier Support 13
2.3.1 Using Premier Online 14
2.4 KETS Service Desk Support 21
2.5 Responsibilities 22
2.5.1 KIDS/Microsoft 22
2.5.2 District 23
2.6 O365 Service URLs and IP Addresses 23
2.7 Reporting SPAM to Microsoft 23
2.8 Password Requirements/Procedures 24
2.8.1 Fine Grained Password Policies 24
2.8.2 Password Resets 27
2.9 Additional Support Resources 27
3 KETS Specific Components 30
3.1 OLPS 30

Table of Contents

3.1.1 OLPS User Provisioning 31

3.1.2 Synced Attributes between AD and O365 33

3.2 KETS EDU Tab 35

3.3 KETS Custom AD Attributes 37

3.4 PCNS 38

3.5 KETS Control Panel 39

3.5.1 Disable Mailbox 40

3.5.2 District Config 41

3.5.3 FIM Reports 44

3.5.4 Jobs 45

3.5.5 Logs 46

3.5.6 Viewer 47

3.6 SMTP Relay 48

4 Exchange Online 49

4.1 Exchange Online Management Accounts 49

4.2 GAL Visibility 51

4.3 User E-Mail Access 51

4.4 Group Calendars 53

4.5 Outlook Web App 53

4.5.1 Password Recovery Questions 54

4.5.2 OWA Password Security 55

4.5.3 Compromised Accounts 56

4.6 AD Specific Management 57

4.6.1 Disable User Account 58

4.6.2 Re-Attaching AD/O365 Objects 58

4.6.3 Preventing Incremented MSOIDs 59

4.6.4 User Name Changes 59

Table of Contents

4.7 Distribution Group/Contact Management 59

4.7.1 KETS State-wide Shared Distribution Group Permissioning 61

4.7.2 Renaming a Security or Distribution Group in Active Directory 63

4.7.3 Dynamic Distribution Groups 63

4.7.4 State-Created Dynamic Distribution Groups 64

4.7.5 Sending to Large Groups 65

4.7.6 Creating Contacts 66

4.8 Naming of Objects and GAL Visibility 67

4.8.1 Naming of Distribution Groups 67

4.8.2 Naming of Resource Accounts 67

4.8.3 Distribution Group and Service Account GAL Visibility 68

4.9 Exchange Admin Center 70

4.10 E-Mail Addresses and Secondary (Proxy) Addresses 72

4.11 Allowed Attachment Extensions in Exchange Online 72

4.12 Mailbox Searches in EAC 73

5 Skype for Business Online 84

5.1 Skype for Business Online Client Installer 84

6 SharePoint Online 85

6.1 OneDrive for Business 86

7 PowerShell 87

7.1 PowerShell in Exchange Online 89

7.1.1 Connecting to Exchange Online 90

7.1.2 Retrieving Mailbox Information 91

7.1.3 Retrieving Distribution Group Information 91

7.1.4 Adding Proxy Email Address 91

7.1.5 Grant Mailbox Permission to Other Users 92

7.1.6 Mailbox Searches in PowerShell 92

Table of Contents

7.1.7 Create Contacts 93

7.1.8 Create Dynamic Distribution Group 94

Change Log

Version	Date	Editor	Description
0.1 DRAFT	1/6/2013	Garrett Dutton	Initial Creation – Alpha Version (Draft)
0.2 DRAFT	1/7/2013	Garrett Dutton	Integrating changes that Richard mentioned
0.3 DRAFT	1/8/2013	Garrett Dutton	Password Policies have been added
0.4 DRAFT	1/9/2013	Garrett Dutton	Changed all references from outlook.com to login.microsoftonline.com
0.5 RC	1/10/2013	Garrett Dutton	Added additional info about whitelisting IP/URL ranges
1.0	1/11/2013	Garrett Dutton	Removed remaining references to Student processes, fixed inconsistencies with Password Complexity/FGPP section, added further explanation of licensing responsibilities for KETS/District.
1.1	1/14/2013	John Fabry	Proofreading.
1.2	1/18/2013	Garrett Dutton	Removed reference to msexchhidefromaddresslists. OLPS now writes this value back to AD.
1.3	2/28/2013	Garrett Dutton	Added remove-mailboxpermissions instructions to PowerShell section and added password reset information to the password section.
1.4	4/11/2013	Garrett Dutton	Added section on running mailbox searches from within EAC
1.5	6/19/2013	Garrett Dutton	Added callout to FGPP section about global groups
1.6	8/25/2013	Garrett Dutton	Changed instructions on creating contact objects with OLPS
1.7	9/12/2013	Garrett Dutton	Updated screenshots for DG management and removed “Staff Only” watermark.
2.0 RC	10/02/2013	Garrett Dutton	Revised for KOOG for O365 Wave 15
2.0	10/29/2013	Garrett Dutton	Finalized Wave15 Changes

Change Log

2.1	07/25/2014	Garrett Dutton	KCP changes to reflect new implementation
2.2	08/29/2014	Garrett Dutton	Formatting Changes
2.3	12/19/2014	Garrett Dutton	Updated limits on mailboxsearch DDG info update passwordreset.aspx info added
2.4	6/29/2015	Garrett Dutton	Document Audit to bring content in-line with current version/features of Office 365
2.5	9/29/2015	Garrett Dutton	Added new connectionURI for ExO powershell connection
2.6	9/29/2015	Garrett Dutton	Added Start-MailboxSearch info
2.7	9/29/2015	John Fabry	Removed Search-Mailbox instructions.

1 Introduction

Check this space throughout the document for important information or links to additional content and documentation.

Welcome to the Office 365 Operations Guide. The focus of this guide is to convey the necessary tasks for carrying out the routine operations required to administer your district's implementation of Office 365. There are other authoritative resources that this document will continually point to for guidance and will usually be included in the column to the left. District administrators should leverage these additional external resources with the understanding that some of the components outlined in this guide may not necessarily pertain to the KETS customized implementation of Office 365.

The KETS offering of Microsoft's "Office 365" suite is the next iteration of Microsoft cloud based solutions for business and education. From an end user perspective, the services/features that were offered in the previous Live@Edu environment will be continued in Office 365. However the method(s) by which those services/features are managed may differ and will be explained throughout the course of this document.

Office 365 is managed by similar methods to Live@Edu and in some cases those methods have remained unchanged. In the following sections all 'KETS specific' tasks and how they are to be accomplished are described, meaning those tasks that are designed solely for the KETS system for which no other documentation exists. Sections of operations that are not KETS specific will not be defined in this document, but rather reference an authoritative source of information on that topic. Also, there are specific discussions which may be duplicated in different areas of this guide as they may logically fall in several areas. This document is *not* intended to cover all required end user tasks, but instead attempts to outline the necessary operational procedures for districts to make use of the KETS Office 365 system.

1.1 Audience

This guide was written and is kept up-to-date for technical administrators and user managers of Kentucky school districts' directory services and messaging systems.

1.2 Technologies/Terminologies

There are acronyms and technology terms that are used when discussing Active Directory and the Office 365 implementation in KETS. It's first important to reiterate that technical administrators in this K-12 environment are the audience for this document.

- ***KETS*** - **Kentucky Education Technology System** will be referenced throughout this document, referring to all users, and technologies, which utilize enterprise services delivered to the 176 (including KSD and KSB) school districts by KIDS (the Office of Knowledge, Information and Data Services) which was formerly the Office of Education Technology, or OET. KIDS is the technology office of the Kentucky Department of Education.
- ***KIDS*** – The **KDE Office of Knowledge, Information and Data Services** was formerly the Office of Education Technology (***OET***).
- ***Premier*** - This is the Microsoft Support service for the Office 365 system.
- ***OLPS*** - The **Outlook Live Provisioning System** is the mechanism that creates Office 365 users based on data present in active directory.
- ***AD/ADDS*** - **Active Directory Domain Services** are utilized by KETS to manage directory services for the enterprise. The Active Directory Domain Controllers, the devices which run the service, utilize Windows Server 2008 Hyper-V technology. Microsoft's Windows Server 2008 Hyper-V provides virtualization of operating systems and their services. KETS also utilizes Domain Name Services (***DNS***) which resides within Active Directory as well as external to Active Directory on other platforms.
- ***O365*** - **Office 365** is Microsoft's offering for "Office" related technologies that are hosted at Microsoft's datacenters throughout the world. These technologies are accessed over the internet by various clients depending on the technology required. KETS has initially adopted only the e-mail and collaborative services (***Exchange Online*** and ***Skype for Business***) of Office 365 which are two of several offerings that reside under the Office 365 suite of services.
- ***ExO*** – Exchange Online is the Email offering component available in O365 and is almost a direct replication of the feature set that was available in in Live@Edu.

- ***SFB –*** Skype for Business Online is the component of O365 that allows instant messaging/web conferencing/distance learning between tenant users.
- ***MSOID*** - **Microsoft Online ID** is the account type that exists in the cloud for each user in the O365 system.
- ***OWA*** – The **Outlook Web App** allows access to e-mail services offered by Exchange Online through a web browser. This can be accessed through the O365 portal which is available at https://login.microsoftonline.com .
- ***Tenant*** – The tenant is the top most level of organization in the O365 environment. Tenants are how an organization is defined within O365 and can be thought of as similar in concept to an Active Directory Domain. All state users reside within one single tenant but have different accepted domains within that. Example: adair.kyschools.us, allen.kyschools.us, anchorage.kyschools.us, etc…
- ***FIM*** - **Forefront Identity Manger** is the underlying system that OLPS is built upon which reads and writes to/from Active Directory and O365. Certain components of OLPS also perform customized tasks that synchronize objects between the two systems.
- ***EAC/KCP*** – The **Exchange Admin Center** is the primary administrative interface for Exchange Online. Some administrative tasks are performed in web portals that are provided to district administrators. These are the **KETS Control Panel** (customized for our environment) and the Exchange Admin Center. The tasks that can be performed in these web interfaces as well as the other technologies discussed in this section will be expanded upon throughout this document. From a high-level there are some very specific tasks that can be accomplished through the KETS Control Panel, but there is nothing that is required for normal user management.
- ***PCNS*** - **Password Change Notification Service** allows for passwords in Active Directory and O365 to be in sync. This service is installed on all of the domain controllers in the district and typically syncs the user password within seconds.
- ***UPN*** – **User Principal Name** is the attribute that allows login to AD joined machines with a user specified naming scheme. In the KETS AD implementation the UPN is the same as the

Learn more about PowerShell at TechNet.
http://technet.microsoft.com/en-us/library/bb978526.aspx

user email address. OLPS controls the writing of this attribute to the user's AD object at the onset of the provisioning process.

- ***PowerShell*** - **PowerShell** is a command-line based scripting language that can be used to administer objects in Outlook Live and for that matter most components of the newer Windows operating systems. There are many functions that can be accomplished only with PowerShell in O365. These range from Multi-Mailbox searches to adding secondary proxy addresses to mailboxes.
- ***KE/KRE*** - The **KETS Regional Engineers** are assigned to your district and can be contacted concerning KIDS information.
- ***SMTP Relay*** - The **SMTP Relay** consists of two load balanced SMTP servers that districts can utilize to send mail from SMTP enabled devices within the districts. The server name for districts to use is ***"ketsmail.us"***. The relay requires a valid AD credential to send mail. All devices that are incapable of accepting this type of authentication should be discussed with the KETS Service Desk if that device needs to make use of the relay.
- ***DRAD*** - **Disaster Recovery Active Directory** is the Hyper-V cluster maintained by KIDS that houses the tertiary domain controller (EDXXXADDC2) for each district for disaster recovery purposes and handling OLPS system write changes.
- ***DDG*** - **Dynamic Distribution Groups** are distribution groups that exist only in the Exchange Online component of Office 365 for which membership is updated based on criteria set by the administrator and evaluated at time of message delivery.
- ***DL/DG*** - **Distribution Lists or Distribution Groups** exist in AD and O365 for message delivery to groups of multiple users.
- ***SG*** - **Security Groups** exist in O365 for granting rights to resources in SpO. All groups provisioned from AD to O365 are SGs that can be used for mail delivery as well.
- ***ADUC*** – **Active Directory Users and Computers** is the client snap-in for AD administration. This can be installed via the RSAT (Remote Server Administration Tools) on a Windows Vista/7/8 workstation to manage the Server 2008 implementation of AD that is in operation in the KETS environment. The installer for the current RSAT is available at the following URL: http://www.microsoft.com/en-us/download/details.aspx?id=7887 . There

is also an updater that will need to be installed after adding the ADUC snap-in to an administrator workstation that extends the application for O365 support in the KETS environment. You can obtain the installer by contacting the KETS helpdesk.

Note – All users in the state O365 implementation will be visible to all other users unless explicitly hidden.

- ***GAL –*** The **global address list** is the combined set of information that is leveraged by the O365 components to allow collaboration, messaging, etc. This includes contact lists of all state users.
- ***GUI*** – A **graphical user interface** is the point and click front end method of interaction for a user to control applications rather than by using a command-line interface (***CLI***).
- ***Cloud*** - This is a generic term for any hosted services that do not exist in the on premises network. For purposes of this document it refers to data or features that exist in O365.
- ***EWS*** – **Exchange Web Services** is one of the methods by which programs can be created that can access content from Exchange Online. More information is available at the following link: Exchange Web Services
- ***FGPP –*** A **Fine Grained Password Policy** is the method by which different groups of users can have different password policies in the same Active Directory domain.
- ***PSO –*** A **Password Settings Object** is the actual object that is created in AD to specify the password settings.
- ***CMDLET -*** A **cmdlet** (Pronounced: "Command-let") is a lightweight command that is used in the Windows PowerShell environment. They are used to perform application-like functionality.
- ***AQS –*** **Advanced Query Syntax** is used for defining parameters to filter objects by. It is used in the context of this document for mailbox searching in PowerShell.
- ***IAAS –*** **Infrasturcture as a Service** in the KETS environment refers to VMs ran in Microsoft Azure.

Again, these technologies and terms will be explained in more detail in later sections.

1.3 Document Feedback

If you have ideas for improving this document, such as adding additional information or clarifying existing content, please send them to your KETS Engineer so they can be considered for future versions.

1.4 Document Updates/Location

This document will be updated and enhanced over time. Please check for new versions periodically at http://education.ky.gov/districts/tech/Pages/Administration-and-Install-Guides.aspx

2 Support/Troubleshooting

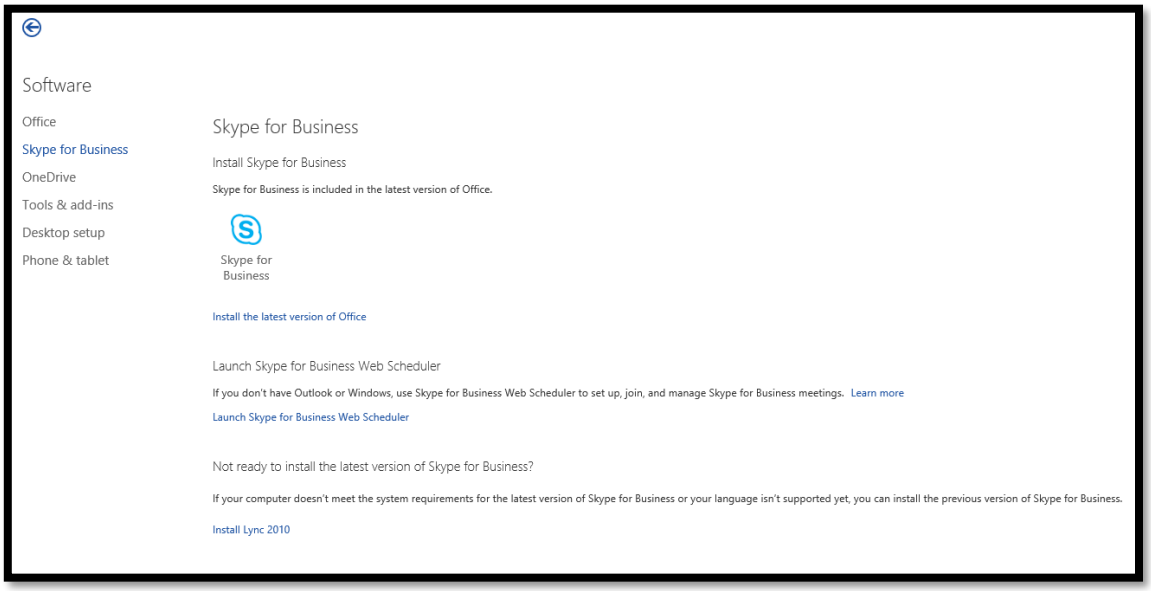
Completing all applicable troubleshooting notes below can greatly decrease the time to resolve O365 issues that may arise.

The purpose of this section is to provide KY Department of Education (KDE) Office of Knowledge, Information & Data Services (KIDS) support staff guidance on how to properly obtain support on O365 related support issues and basic troubleshooting processes. This is a guide only and cannot address every possible scenario. Where content exists in another source that document is referenced. If you are not sure whether vendor documentation is correct, Microsoft or otherwise, for a particular task please contact the KETS Service Desk. The KDE implementation of O365 is designed in such a way that initial triage and problem resolution should be handled at the level closest to the end-user. In the case of KDE this should be at the District IT level. District IT staff should be fully encouraged to not adopt a "quick trigger" on escalations to Premier Support or KIDS. District IT should follow this guidance to ensure issues are properly examined and attempts are made to resolve prior to escalation.

2.1 Downloads

You can obtain the O365 specific installers from the ***"Software"*** section of the O365 Portal. It is accessible at https://portal.microsoftonline.com/OLS/MySoftware.aspx . This includes software such as the ***"O365 Desktop Setup"*** application and the office product installers if your district has a valid EES agreement with Microsoft.

O365 SOFTWARE



2.2 District Level Management/Troubleshooting

At a high-level there are four major management avenues that can be utilized by an IT admin for O365 administration. These areas are:

I. Active Directory management tools
   a. Active Directory Users and Computers
   b. CSVDE, LDIFDE, DSADD, DSMOD, DSQUERY, etc.
   c.
   d. Other 3rd party tools
II. KETS Control Panel
III. Exchange Admin Center
IV. PowerShell
V. EWS/Graph/REST

2 Support/Troubleshooting

The first two areas (AD tools, and KETS Control Panel) are leveraged with those Active Directory credentials that were used in the past that have membership in privileged Security Groups such as DIST Support Admins, DIST Staff User Admins, etc. The third area () is used specifically for management of the messaging infrastructure. To summarize, you will login with your administrative Active Directory credentials to do AD and KETS Control Panel tasks. Anything in Exchange Admin Center will be a MSOID that does not exist in Active Directory.

Exchange Admin Center is primarily used for O365 mailbox creation and Exchange Online Management. More specifically, it is mostly used for Distribution Group (aka Distribution List) creation and management. So you will use O365 administrative accounts that do not exist in Active Directory to perform tasks against Outlook Live (Exchange Admin Center, PowerShell or scripting to the mail system). All administrative credentials are outlined in the following section.

2.2.1 District Troubleshooting Checklist

Please use the following checklist to troubleshoot issues with the O365 system before engaging the KETS helpdesk.

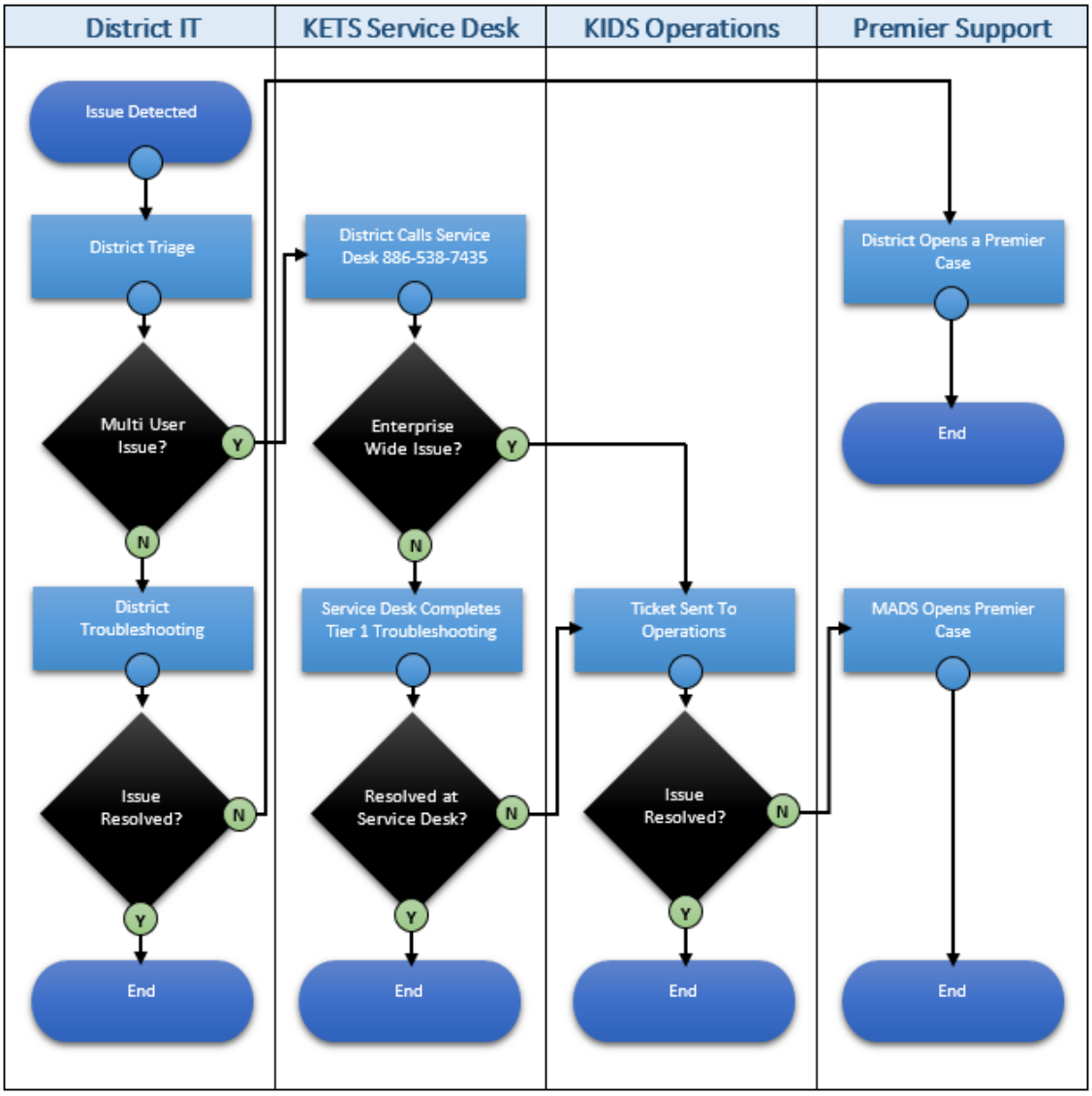
- ☐ Ensure AD account is created in an appropriate OU and is not stamped with NOMAIL on the KETS EDU tab.
- ☐ Ensure enough time has elapsed for the account to be provisioned. Typically provisioning can take up to 2 1/2 hours.
- ☐ Review the Active Directory object for potential issues.
- ☐ Access the "Viewer" section of the KETS Control Panel and ensure that all checkboxes are green. Review any red "X's" to help determine the problem.
- ☐ Review the "Logs" section of the KETS Control Panel for errors on the account.
- ☐ Ensure that a password reset has occurred for the user through AD if this is a new or rarely used account.
- ☐ Review the related account in the Exchange Admin Center for potential issues.
- ☐ Can the account be accessed using https://login.microsoftonline.com ?
- ☐ If the issue is related to use of the browser based components of O365 then contact Microsoft Premier Support (i.e. OWA and EAC).
- ☐ Use the Microsoft Remote Connectivity Analyzer to determine if this is a local network issue.

You can access the Remote Connectivity Analyzer at the following link: https://www.testexchangeconnectivity.com/

The following should be provided when opening a ticket with the KETS Service Desk:

- ☐ Detailed description of the problem, including any specific symptoms experienced.
- ☐ Example account(s) that are currently experiencing the issue. If multiple users are experiencing this issue, be prepared to provide at least a few examples.
- ☐ Any errors that were noted on the account in the KETS Control Panel Logs or Viewer.
- ☐ Detailed description of any troubleshooting that has been performed at the district level.
- ☐ Frequency of the problem: intermittent or 100% of the time.
- ☐ Is the problem currently occurring? If not, when was the last occurrence?

2.2.2 Case Workflow



If you want to access premier services through the web using premier online, you will need to follow the instructions in the following section.

2.3 Contacting Premier Support

Microsoft Premier offers technical support to address issues districts may experience related to Office 365 via the phone or web. Examples of issues technical support can assist you with include difficulty with Microsoft ID issues, Exchange Online delays, users cannot log in, etc.

Phone Support: (800) 936-3100
Web Support: https://premier.microsoft.com

Districts with their own Premier Support Agreements should use the Access IDs they already have. Your O365 Access ID should be kept PRIVATE and CONFIDENTIAL with a very limited number of people in a district. Reporting is keyed off this Access ID and it is critical that districts protect the integrity of their Access ID.

Support entitlement/authentication for access to support is by Access ID. District Technology Coordinators should contact their KE to receive their appropriate Access ID and Password. When working with a support engineer during troubleshooting make sure that you let the technician know that you do not have "**Tenant Admin**" privileges. If the support technician needs you to perform certain tasks which you do not have access to, you will need to contact the KETS Service Desk to escalate those procedures to the operations division of KIDS.

District IT Support requests submitted with your supplied O365 Access ID for products other than Office 365 will be closed. Currently there is not a programmatic method to prevent cases from getting opened for any non-Office 365 products**. ANY DISTRICT THAT OPENS A PREMIER CALL FOR A PRODUCT OTHER THAN OFFICE 365 USING THEIR OFFICE 365 SUPPLIED ACCESS ID MAY BE SUBJECT TO FINANCIAL CHARGES APPLIED BY MICROSOFT.**

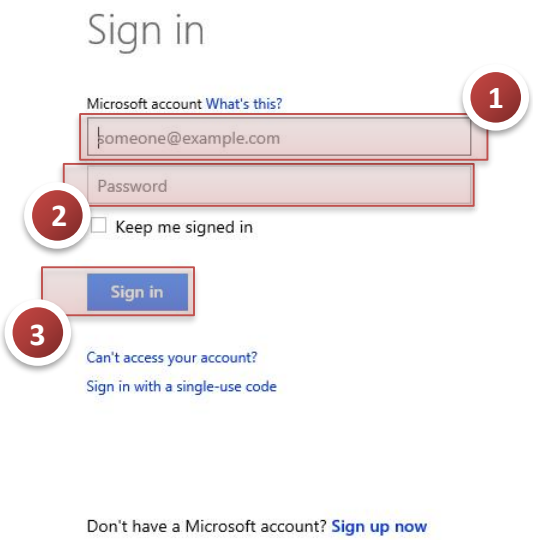
For district opened cases that experience a service delivery issue, the district IT staff should contact KIDS via the KETS Service Desk. A representative from KIDS will contact the Technical Account Manager for escalation support. For KIDS and districts with Premier Support, contact the district's Technical Account Manager for escalation support.

2.3.1 Using Premier Online

To access premier online (https://premier.microsoft.com), you will first need to setup the account. **THIS IS VERY IMPORTANT!! MAKE SURE TO FOLLOW THESE STEPS EXACTLY, AS YOU WILL ONLY HAVE THE OPPORTUNITY TO CORRECTLY SET THIS UP ONCE!!**

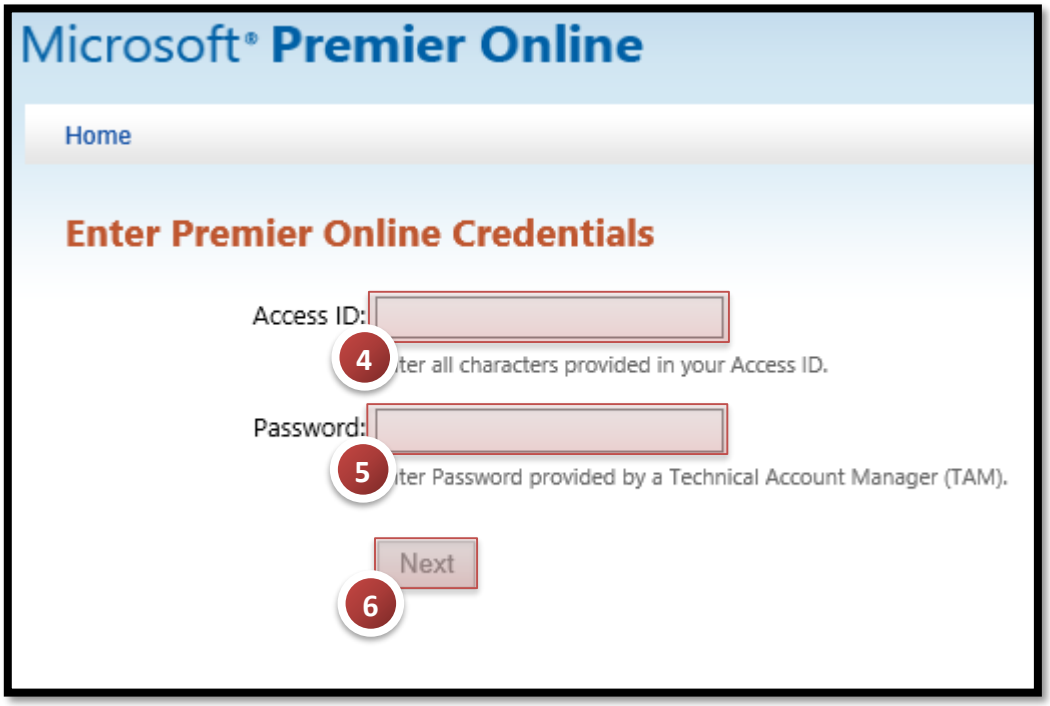
First you need to obtain the Access ID and Password for your district. If you do not have this you can obtain it by contacting your KE. Once you have the ID you need to go to the Premier Online website (https://premier.microsoft.com) and sign in as the outlookadmin account for your district (outlookadmin@***DISTRICT***.kyschools.us).

PREMIER ONLINE



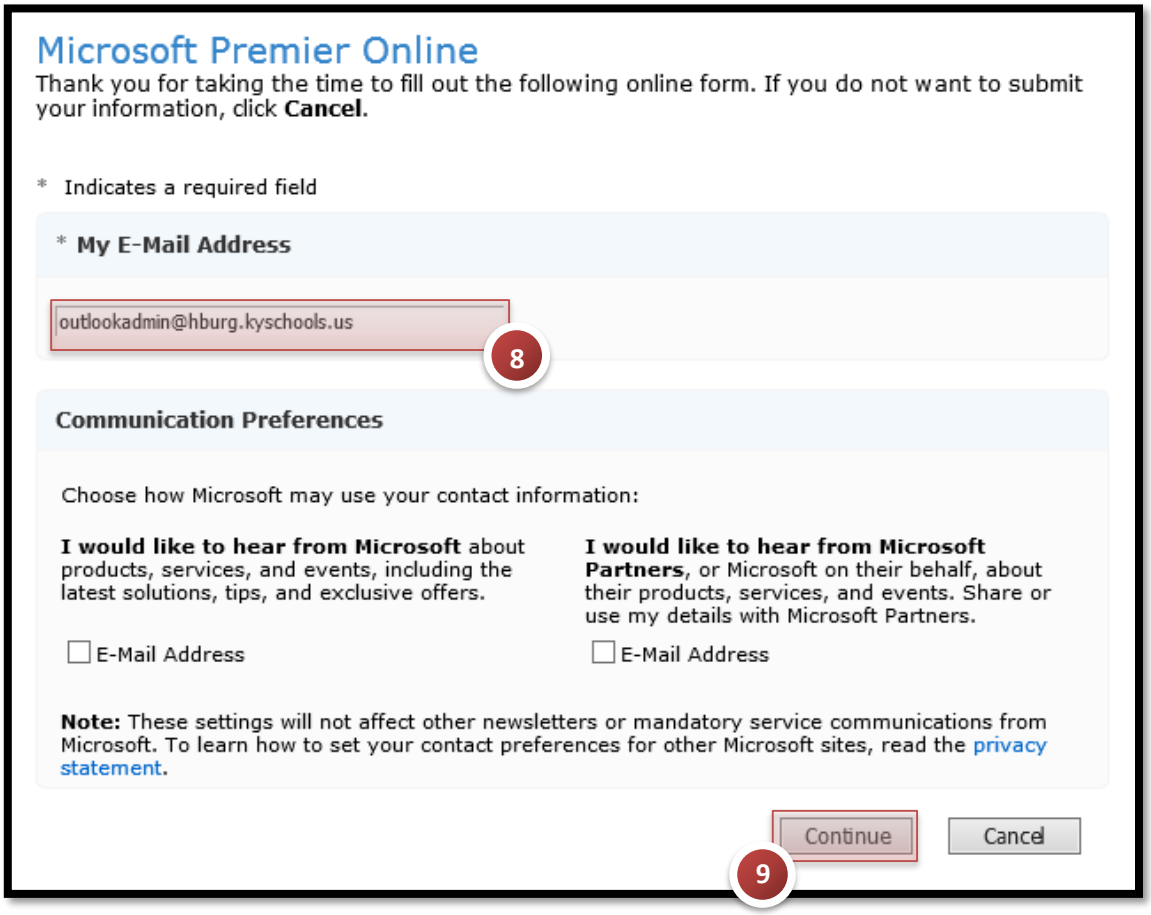
You may be prompted that your "password isn't enough" and need to include additional password recovery information. If so please refer to the steps in the following section for more information.

At this point you will be prompted to enter the Access ID and password for your district to pair to your outlookadmin MSOID to the associated Premier account.

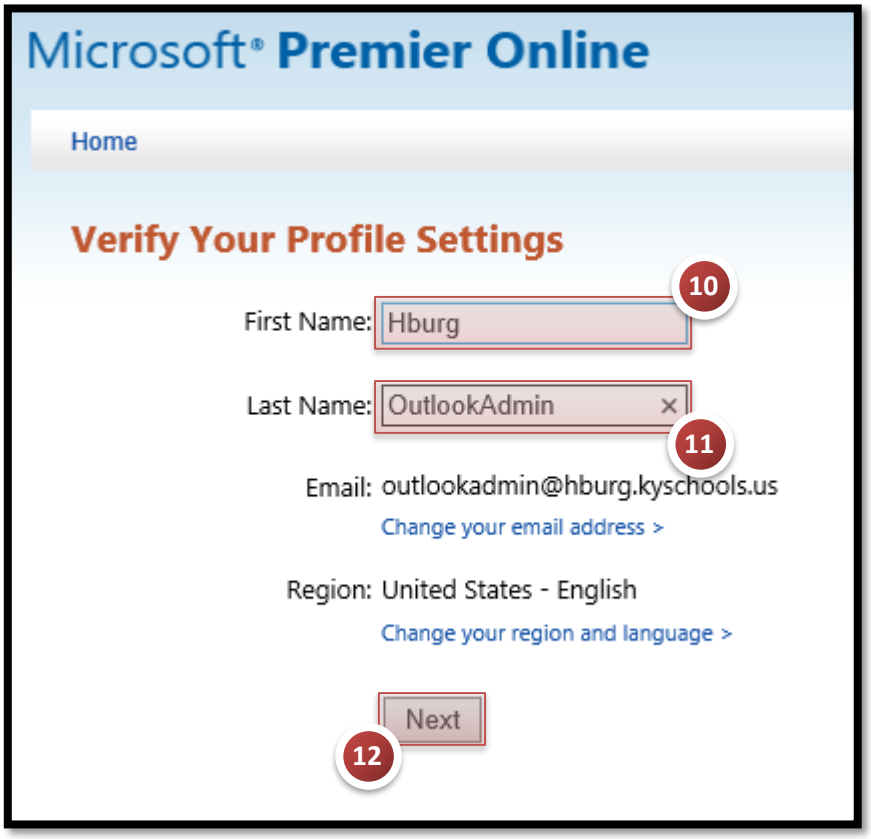


Next you will need to verify some profile settings. To keep these as standardized as possible, please follow the format specified below. First make sure the email address for the account is correct by clicking the ***"Add you email address"*** link.

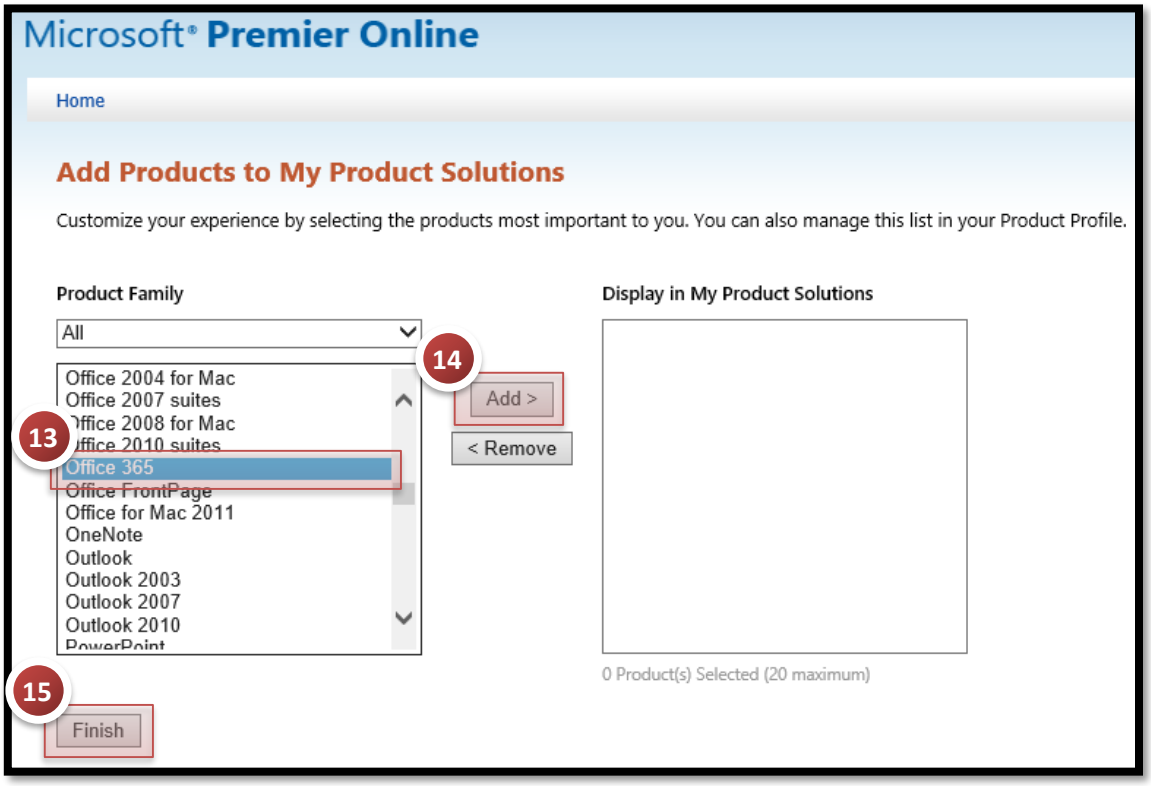
In the screen that opens confirm that the email address is the correct one for your outlookadmin account and deselect any email newsletter options. Then click the ***"Continue"*** button.



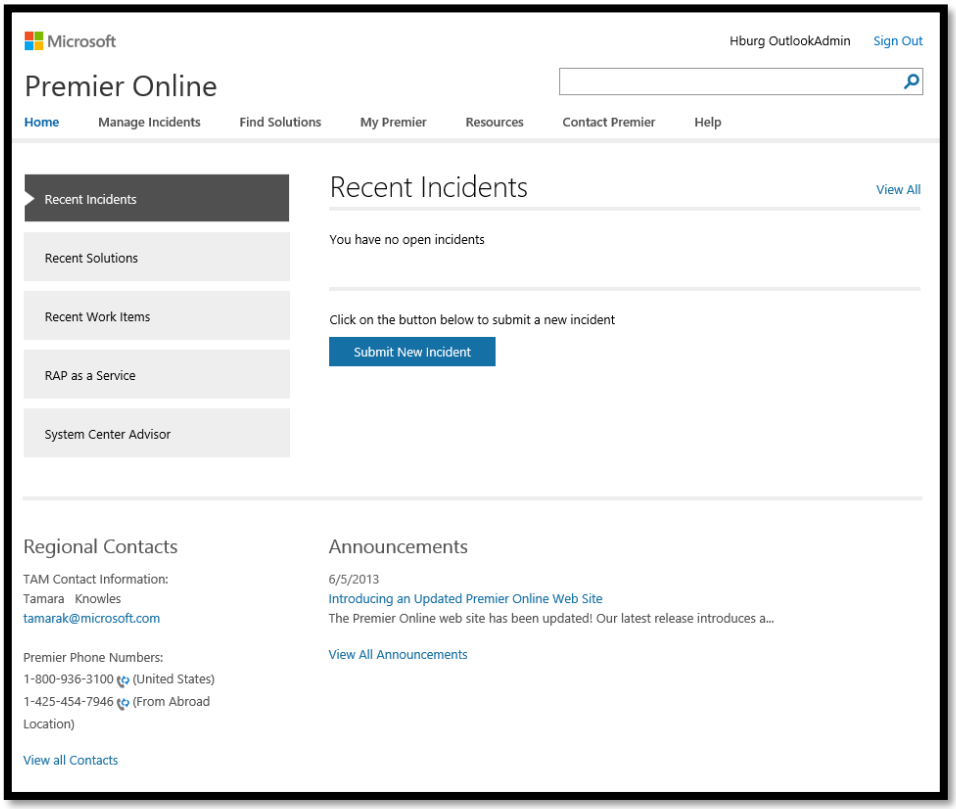
Now fill in the first and last name fields as shown below with your districts SMTP suffix (***XXXXX***.kyschools.us) in first name field and click the ***"Next"*** button.



On the next screen select ***"Office 365"*** from the left hand side product list and click the ***"Add"*** button to make it a default product solution. Then click the ***"Finish"*** button to apply the settings.



Your district's premier account is now setup and configured. You should see a screen similar to the one shown below.



If you wish to create a new premier ticket for O365 services you can click on the ***"Submit New Incident"*** button and fill out the forms that appear.

2.4 KETS Service Desk Support

For assistance with the following issues, please contact the KETS Service Desk:

I. Active Directory Issues Related to O365
   a. User Attributes

b. Password Sync (PCNS)

II. Office 365 Issues
   a. Skype for Business
   b. Exchange Online
      i. Account Provisioning
      ii. MSOID Issues

III. KETS Control Panel

IV. If you're not sure whether vendor documentation is correct, Microsoft or otherwise, for a particular task

KETS Service Desk:
(502) 564-2002 (local) (866) 538-7435 (toll free)
E-mail: ketshelp@education.ky.gov

2.5 Responsibilities

Below are defined the responsibilities in regard to what falls to the District to maintain as opposed to KETS.

2.5.1 KIDS/Microsoft

KIDS is responsible for most technical maintenance and support of systems in the KETS Active Directory/O365 environment. This includes providing the licenses required for base O365 functionality within Exchange Online and Skype for Business Online (Plan E1). KIDS is responsible for OLPS which delivers the provisioning between AD and O365. KIDS is also responsible for SMTP relaying services for secondary applications which require 'send mail' capabilities.

There are several things in the O365 environment that districts do not have admin rights to do within the tenant. These things require a ticket request be created with the KETS Service Desk or through the KE for that district and in some cases be accompanied by a justification document. While this list may change over time, below are some of the known actions that require a request to your KE or a ticket with the KETS service desk.

1) **ActiveSync Device Removal**
   - When a user reaches the ActiveSync device limit (currently 10), the district must request devices be removed from the account before the user can add

any more devices to their account. This typically occurs when district's use 1 account for device testing. To keep this from happening, we recommend that district's not use an actual user account to test with. Instead create a temporary account that can accrue devices and be deleted when the limit is reached. You may call the KETS service desk to create a ticket for this action.

2) **Resetting the outlookadmin account for a district**
3) **Transport Rules**
   - Requests for a transport rule in ExO must be accompanied with a justification document for the rule and be submitted through the district's KE.
4) **Site Collection Creation in Sharepoint**
   - Districts may get a site collection created in SharePoint Online by following the process outlined in the following section.

2.5.2 District

Districts are responsible for the physical environment which houses the Active Directory servers. This area should stay physically secure and temperature controlled. The district is also responsible for all user/object administration that's required for O365. Any additional licensing that the district requires to extend the base functionality of O365 is also incumbent upon the district.

2.6 O365 Service URLs and IP Addresses

These ranges are subject to change at Microsoft's discretion. It is recommended that you subscribe to the RSS feed for page changes so districts can be notified when changes occurs.

Access to Office 365 requires that your network devices have unrestricted access to the following set of URLs and IP addresses. You must whitelist the following ranges on any networking hardware running in-district that would potentially restrict access.

Office 365 URLs and IP Addresses

2.7 Reporting SPAM to Microsoft

In the event that users are receiving SPAM emails, a report can be filed with Microsoft which will help in deterring those types of messages. Two options are available to districts:

1. Users that access email using the Outlook client can use the Outlook Junk Mail Reporting Add-in. With this add-in users have a one-click interface for submitting SPAM to the FOPE SPAM Team for analysis.
   - This tool can be downloaded from Microsoft at the following link: Outlook Junk Mail Reporting Add-In
2. Send an email to abuse@messaging.microsoft.com with the SPAM messages as attachments for analysis. It is important to attach the SPAM messages to a new email rather than just forwarding or copying and pasting so that the full headers can be examined.

2.8 Password Requirements/Procedures

It is recommended that districts use one of the FGPPs that have been created per domain to enforce an 8 character or greater password even though currently 7 will function if provisioned from Active Directory.

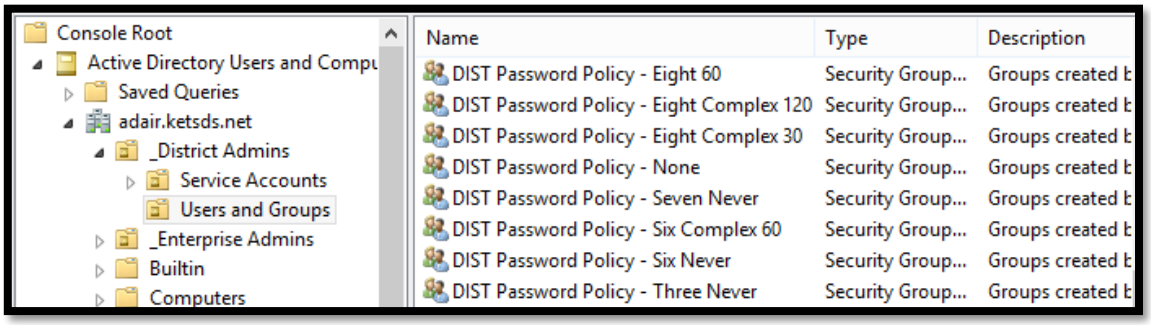
In the KETS implementation of O365 the only requirement for user passwords to be valid in the cloud is that they contain at least 7 characters. Normally the defaults would be stricter, but they have been modified at the request of KETS. Documentation from other sources will report that the minimum password policy is more than what KETS has specified. Districts must either inform users that wish to utilize O365 services to specify at least a 7 character password, or use the set FGPP security groups within Active Directory which force at least this minimum requirement. **It is possible to have a user password that is less than the O365 minimum password policy in Active Directory, but that user will not be able to use O365 services.** If you would like to know more about FGPPs they are explained in following section. The requirements for O365 accounts are listed in the following Microsoft Document: Office 365 Password Policy.

2.8.1 Fine Grained Password Policies

*FGPP Groups can only contain individual users or **global** groups. Universal and Domain local groups will not have FGPP applied to them if they are added to one of the FGPP security groups.*

Districts have the ability to utilize any of eight password policies for different groups of users. A district can choose to utilize only the default domain policy but will also have the option to take certain groups of users and apply different password policies beyond that. These new policies are not implemented on an OU basis; they are assigned to security groups and/or users.

FINE GRAINED PASSWORD POLICIES



Fine-Grained Password Policies work with the Default Domain Password Policy through "precedence" or weighting. The Default Domain Password Policy has the lowest weight, meaning if a user is placed in any of the password policy groups the FGPP will be applied instead of the Default Domain Password Policy. The groups have weighting as well, so users can be in multiple groups but only the group policy with the highest weighting will be applied to that user.

Eight Global Security Groups exist which reside in the ***"_District Admins"*** OU. Each of these groups maps to a corresponding Fine-Grained Password Policy. For a given policy to be applied, users must be placed in the corresponding group. The groups and explanation of each follow.

- **DIST Password Policy - None**
  - This policy requires no minimum password length, no complexity, forces no change and has a zero password history.
- **DIST Password Policy - Three Never**
  - This policy requires a three character password length minimum, no complexity, forces no change and has three passwords remembered (meaning you cannot reuse the last three passwords).
- **DIST Password Policy - Six Never**
  - This policy requires a six character password length minimum, no complexity, forces no change and has a zero password history.

- **DIST Password Policy - Six Complex 60**
  - This policy requires a six character password length minimum, forces complexity*, forces a change at 60 days and has five passwords remembered (meaning you cannot reuse the last five passwords).
- **DIST Password Policy - Seven Never**
  - This password policy matches the minimum requirements to received mailbox access. This policy requires a seven character password length minimum, no complexity, forces no change and has a zero password history.
- **DIST Password Policy - Eight 60**
  - This policy requires an eight character password length minimum, no complexity, forces a change at 60 days and has three passwords remembered (meaning you cannot reuse the last three passwords).
- **DIST Password Policy - Eight Complex 30**
  - This policy requires an eight character password length minimum, forces complexity*, forces a change at 30 days and has twelve passwords remembered (meaning you cannot reuse the last twelve passwords).
- **DIST Password Policy – Eight Complex 120**
  - This policy requires an eight character password length minimum, forces complexity*, forces a change at 120 days and has three passwords remembered (meaning you cannot reuse the last three passwords).

FGPP Security Groups written in Blue above are acceptable for use with O365.

For those policies above which require complexity the user must meet at least three of the following four complexity requirements within the password:

- Uppercase characters (A through Z)
- Lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Special symbols or non-alphabetic/non-numeric characters (for example: !, $, #, %, etc.)

The precedence of these groups goes from the lowest precedence ***"DIST Password Policy – None"*** to the highest precedence ***"DIST Password Policy - Eight Complex 30"***. This is with the understanding that the Default Domain Password Policy ultimately has the lowest precedence. If there are settings defined on the actual user object (**"Password Never Expires"**, etc.) those settings will apply no matter what policy the user is associated with; local user settings take precedence over policy. For example, if a user is in both the ***"DIST Password Policy - Three Never"*** group and the ***"DIST Password Policy - Eight 60"*** group the user would have to meet the requirements of the ***"DIST Password Policy – Eight 60"*** group.

When a user is placed in a Fine-Grained Password Policy group, or if the Default Domain Password Policy is modified, the affected users will **NOT** be required to immediately change their password to match the minimum requirements. The next time the user is made to change their password, the new policy will be evaluated and applied. If a user currently has no password policy that requires them to change their password the user would either have to be instructed to change their password manually or the user object would need to be set to ***"User must change password at next logon"***. This can be accomplished either in Active Directory Users and Computers on a per user basis or through a script (VB, LDIFDE, PowerShell, etc.) which would modify the ***pwdLastSet*** attribute to 0 on each user object.

2.8.2 Password Resets

*When a user goes to login to their account at login.microsoftonline.com there is a "Can't Access Your Account" link. Users **SHOULD NOT USE THIS.** This does not reset a user's password. It only submits an email requesting it to the tenant admin and **will not be acted upon.***

If for any reason a user forgets their password or there is reason to reset a service account's password you must do so through Active Directory via PCNS. Resetting passwords via the cloud if you do not already know the password for logon is not possible through EAC at this time. You must use Active Directory. **If a user needs their password reset they should contact their district IT support staff.**

2.9 Additional Support Resources

Below are some resources for support of O365. It is important to note that while the below links are normally authoritative, the KETS implementation of Office 365 is unique in many aspects so it's important to consult this document before utilizing any of the below links.

http://technet.microsoft.com	**Microsoft resources for IT Professionals**
http://community.office365.com/en-us/default.aspx	Office 365 community help
http://onlinehelp.microsoft.com/en-us/office365-smallbusinesses/ff637557.aspx	Skype for Business Online administration help
http://community.office365.com/en-us/tools/troubleshooting.aspx	Troubleshooting tool for Office 365
http://onlinehelp.microsoft.com/en-us/office365-enterprises	Office 365 enterprise help and how-to
http://community.office365.com/en-us/blogs/default.aspx	Office 365 official blogs
http://community.office365.com/en-us/forums/default.aspx	Office 365 forums
http://community.office365.com/en-us/wikis/default.aspx	Office 365 wikis
https://support.office.com/en-us/article/Office-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2?ui=en-US&rs=en-US&ad=US	Office 365 URLs and IP Address Ranges
https://technet.microsoft.com/en-us/library/jj943764.aspx	Office 365 Password Policy

http://onlinehelp.microsoft.com/en-us/office365-enterprises/hh125002.aspx	Available cmdlets in O365
https://portal.microsoftonline.com/OLS/MySoftware.aspx	O365 Software Download

3 KETS Specific Components

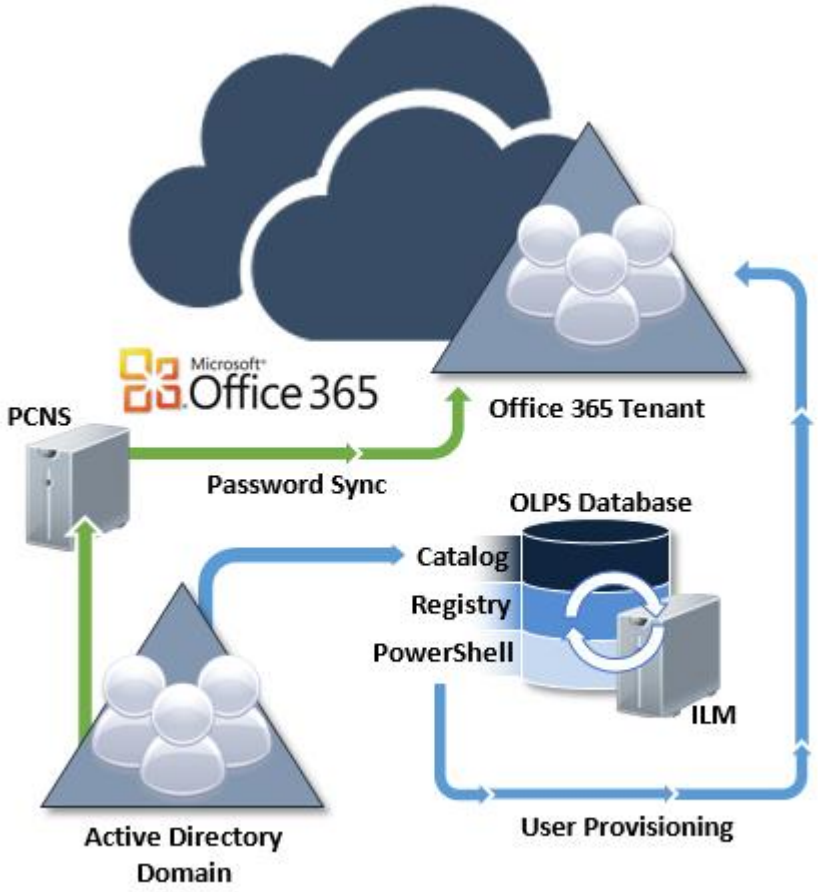
In the KETS implementation of O365 there are many components that are not "out-of-the-box" solutions that have been customized for KETS to achieve the business requirements specified. This section will cover those components that are specific to the KETS implementation of O365 services.

3.1 OLPS

The provisioning system which synchronizes information between KETS Active Directory and O365 is OLPS. It is comprised of multiple server instances running FIM and other system services. This system is responsible for keeping users, Distribution Groups, Security Groups (if desired) and mail-enabled contacts with certain attributes synchronized with the cloud. Another component of the solution is PCNS which keeps passwords in sync between AD and O365.

The OLPS services exist in an Azure IAAS services which also contains a tertiary domain controller for each district domain (EDXXXADDC3). This allows OLPS to read from and write to Active Directory at local switch backplane speeds.

There are some administrative tasks which cannot be accomplished with conventional methods so a customized KETS Control Panel exists for those special tasks. These will be explained in greater detail in later sections. The following image is a high-level depiction of the OLPS system.



3.1.1 OLPS User Provisioning

Active Directory objects (users, groups, etc.) can be created using the ADUC Management Console. To properly do this you need to be using the RSAT tools available at the following link for Windows (RSAT Tools). On top of this, to manage certain aspects of the O365 system on user objects you will need the ADUC extension for the KETSEDU tab that can be requested from the KETS service desk. This is an excellent method for most management tasks. OU placement can impact how objects are provisioned in O365 for mailbox access. If users are created under the ***"Leadership", "Students",*** or ***"Staff"*** top-level OUs (or their sub-OUs other than ***"_Groups'"***) these objects will be provisioned for O365 services. They will be placed in the State Tenant and more specifically in the accepted domain for the district

(***dist***.kyschools.us or stu.***dist***.kyschools.us). This means they will be a visible member of a single, statewide shared Global Address List. Distribution Group management, on the other hand, can be handled differently than other objects. This is described in following sections. When a new user object is created in AD and set to provision, that object must complete provisioning through the OLPS system and THEN the password must be changed/reset in AD to allow the password to be synced to O365. This is because PCNS is what sets the initial password on the O365 account and so both the AD and O365 account must exist for this to occur. Districts should delay giving the user their credentials up to 2 hours as it could take that long for OLPS to write the SMTP address to the AD object for the user. When the ***"E-mail"*** attribute is populated on the General tab for a user in ADUC the object has been provisioned and it is safe to give the user their login credentials and have them change their password.

Two of the suggested methods District administrators can utilize for initial password sync are as follows:

1. ***User Generated (Preferred)*** - Create the account with a predefined temporary password and set the AD account to ***"force the user to change the password on next login"***. This can be done through ADUC or by setting the Active Directory ***"pwdLastSet"*** attribute to 0 if being done programmatically. This way after the account has provisioned you may give the user the temporary credentials you used and upon login they will be prompted to set their own password which will accomplish the initial sync to O365.
2. ***Admin Generated -*** Create accounts with the desired password, allow provisioning to run, and then from KETS Control Panel set the password in O365 to match the Active Directory password. If the user ever changes their AD password in the future PCNS will sync the change to O365.

OLPS is configured to run every 15 minutes for staff mailboxes (mailboxes contained within the ***"Staff"*** OU) and 6 hours for students (mailboxes contained within the ***"Student"*** OU). After factoring in replication latency and the point in the provisioning cycle that the account was created total provisioning time for a staff user can be up to two hours. This also

applies to any modification of users between AD and O365. Provisioning of group creation and modification are processed once nightly, so the changes you make in AD regarding group membership will be active the next day in O365. Group and Contact deletions occur once per week.

A member of DIST Support Admins can disable the scheduled run of provisioning through the KETS Control Panel as described in the KCP section. This might be useful if districts are going to perform a bulk amount of changes in Active Directory and wanted to hold all the changes until they are ready to be processed.

Mass user creations/modifications should be performed at the end of the day so that the potential impact of increased user provisioning workload will occur after hours. OLPS is a sequential process shared amongst all the districts in the state. Mass creations will be put in queue the same as a single user account creation. It is for this reason that off hours is the best time to do mass creations.

When deleting an Active Directory user object that has a corresponding O365 account it's important to consider the behavior of access to mail for the given user. If a user object is deleted in ADUC, the corresponding mailbox would still receive mail until the tombstone days have expired as set in the ***"District Config"*** section of the KCP. After the tombstone days have expired the O365 account and all associated content will be deleted. By default users will not have access to their mailboxes when the AD account is deleted but the mailbox will still be able to receive mail and show in the GAL until the tombstone days have expired.

Districts may choose to set the AD user object to ***"Hidden"*** before deletion so that it does not show in the state GAL after the O365 account is put into tombstone status.

3.1.2 Synced Attributes between AD and O365

The list below contains the AD attributes that are being synchronized to the corresponding O365 objects. These can be leveraged by the district for Exchange Web Services programming, Remote PowerShell, Dynamic Distribution Group creation, etc.

- Active Directory="ketsSystemID" Office 365="Name"
- Active Directory="ObjectID" Office 365="DirSyncId"

- Active Directory="ketsEduDisable" Office 365="AccountDisabled"
- Active Directory="ketsEduHidden" Office 365="AccountHidden"
- Active Directory="mail" Office 365="EmailAddress"
- Active Directory="l" Office 365="City"
- Active Directory="ketsDistrictCode" Office 365="CustomAttribute1"
- Active Directory="ketsLocationCode" Office 365="CustomAttribute2"
- Active Directory="department" Office 365="Department"
- Active Directory="displayName" Office 365="DisplayName"
- Active Directory="facsimileTelephoneNumber" Office 365="Fax"
- Active Directory="givenName" Office 365="FirstName"
- Active Directory="homePhone" Office 365="HomePhone"
- Active Directory="initials" Office 365="Initials"
- Active Directory="sn" Office 365="LastName"
- Active Directory="mobile" Office 365="MobilePhone"
- Active Directory="info" Office 365="Notes"
- Active Directory="physicalDeliveryOfficeName" Office 365="Office"
- Active Directory="pager" Office 365="Pager"
- Active Directory="telephoneNumber" Office 365="Phone"
- Active Directory="postalCode" Office 365="PostalCode"
- Active Directory="st" Office 365="StateOrProvince"
- Active Directory="streetAddress" Office 365="StreetAddress"
- Active Directory="title" Office 365="Title"

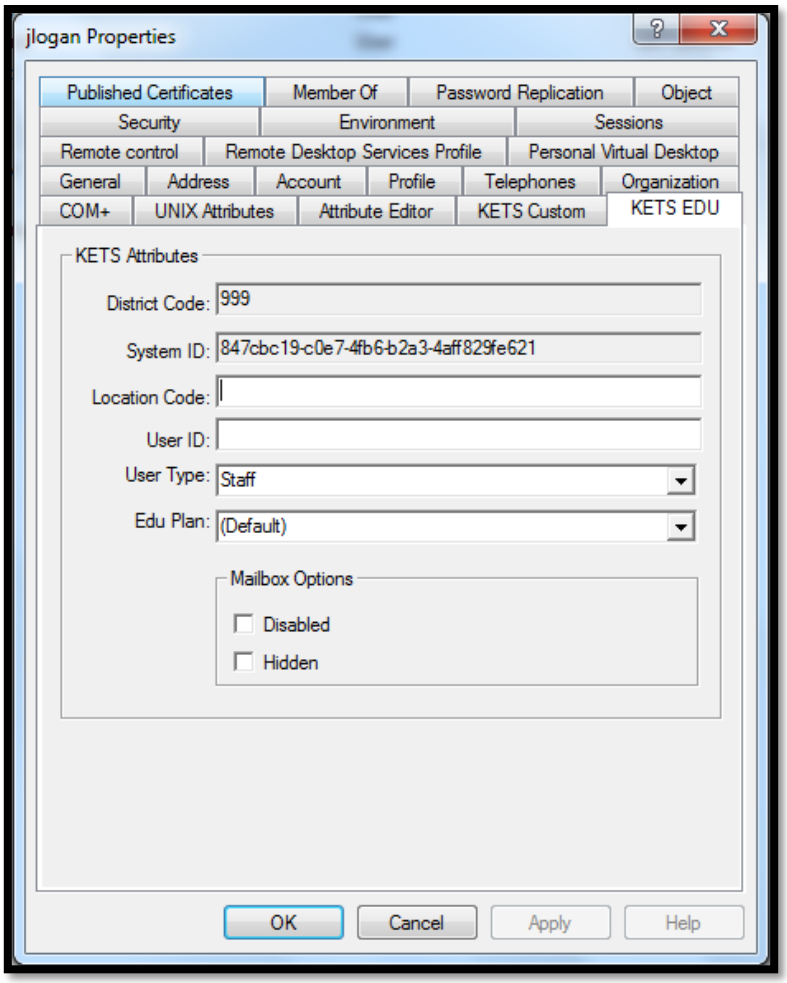
There are also other attributes that do not directly flow from AD but are set on the user's cloud object because of placement in the AD structure.

- CustomAttribute4 = Staff/Student based on provisioning
- CustomAttribute1 = District Number
- CustomAttribute3 = Provisioned Status

3.2 KETS EDU Tab

Below is an explanation of the features available on the KETS EDU tab that the downloadable ADUC extension adds.

KETS EDU



- **District Code**
  - This is reserved by OLPS and should not be changed or added. It will populate with the district's 3 digit ID code.
  - Also flows to extensionAttribute14 in AD and CustomAttribute1 in O365.

- **System ID**
  - This is reserved by OLPS and should not be changed or added
  - This value is used to give each user a unique identifier in the O365 system and is the main link between AD objects and the corresponding O365 object.
  - The O365 attribute ***"CN"*** *is populated with this value.*
- **Location Code**
  - Value that can be up to 255 characters at the discretion of the district. This attribute is not used by the system. It exists for the district to standardize if they so choose.
- **User ID**
  - This value is also reserved by OLPS and has no use in O365 at present. This should be left blank.
- **User Type**
  - The user type is automatically calculated by OLPS based on the AD user account parent OU. Any user created in the Leadership or Staff top-level OUs (or sub-OUs other than _Groups) will be assigned a KETS User Type of ***"Staff"*** and placed in the state tenant and will be viable in the shared GAL.
  - You may manually select the ***"Resource"*** option here to keep OLPS from performing any action on the AD account.
- **Edu Plan**
  - **Default** - Leaving this field as ***"Default"*** will result in a user account being created in O365 and activated for all services therein. At present this includes Exchange Online and Skype for Business Online. This is the default setting and does not need to be stamped on every user account. It will automatically be filled when the AD object is created.
  - **NoMail** - A choice of ***"NoMail"*** will result in an AD account that has no corresponding user account in O365. The AD account will get the UPN written back to the AD object allowing for login to domain resources only with that value. Also, the SMTP email address will be reserved in the OLPS system so that no other user account can use that UPN as well.

Be very careful when setting this value. "NoMail-ing" an account will not obey tombstone policies and immediately delete the account.

- If an already existing O365 user gets the ***"Edu Plan"*** attribute changed on their AD account from ***"Default"*** to ***"NoMail"*** this will completely delete the user in O365 the next time that provisioning runs. This includes any data that may be associated with that account.

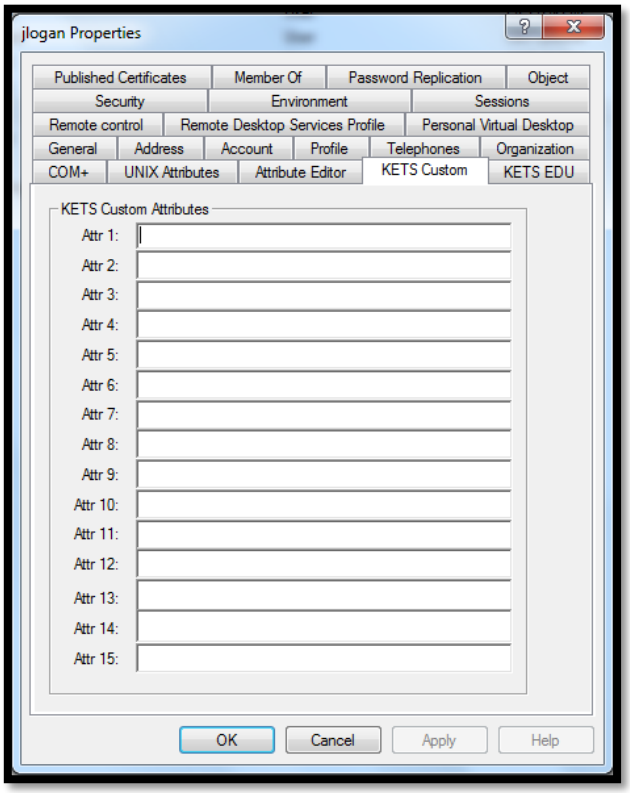
- **Mailbox Options**
  - **Hidden –** Checking ***"Hidden"*** will result in O365 user account being hidden from the state tenant GAL. This is an attribute in O365 that can be set to TRUE or FALSE. Checking the ***"Hidden"*** checkbox will hide a user across all O365 services, not just Exchange Online. If you have created an Exchange Online account solely in the cloud, you must use PowerShell to change the user attribute ***"HiddenFromAddressListsEnabled"*** that controls Gal visibility.
  - **Disabled –** Checking ***"Disabled"*** will result in the O365 account being disabled upon the next run of OLPS provisioning. This option prevents end-user access to their mailbox and Skype for Business, but preserves mail-flow into the mailbox and does NOT disable the AD object. Also, if the user object itself is disabled in ADUC the effect will be the same.

In Live@Edu this was achieved by setting CASMailbox attributes to FALSE. In O365 it is a true user disable that spans across all associated O365 services.

3.3 KETS Custom AD Attributes

Districts have access to 15 additional attributes in AD (ketsCustom1 – ketsCustom15) that can be used as the district sees fit. These are displayed on the ***"KETS Custom"*** tab after installing the KETS ADUC Extension.

KETS CUSTOM TAB



When adding information to these or other AD attribute fields, districts should take note that any information added to an active directory user account is visible to any other user account in the AD Forest. In short, all the info from an account can be read by every other account, whether in the same district or not. This makes AD a poor place to store sensitive user info and districts should refrain from doing so.

These new attributes need to be discussed as district administrators should understand what each is used for. Administrators also can leverage these values for programming, LDAP queries, etc. against Active Directory. Custom Attributes 1, 3, and 4 are already in use by OLPS and should not be used.

3.4 PCNS

There can be latency between the time a user changes their Active Directory password and completion of the sync to Outlook Live. This should be negligible (seconds), but you can check the KCP logs to make sure the password has synced.

Passwords between Active Directory and O365 (through MSOID) are kept in sync through the OLPS system which leverages PCNS configured on all Domain Controllers in the forest. When a user changes his/her password, that password is synced through the OLPS system to the user's MSOID. This allows for the same password to be used between Active Directory and O365 services. If, for any reason, a user changes their password and it doesn't get synced to their MSOID, they can log into https://login.microsoftonline.com or

https://portal.microsoftonline.com with their previous password and change it to mirror Active Directory.

3.5 KETS Control Panel

You can configure a registry key to disable sharing creds between browser sessions in IE by following the instructions found here.

The KETS Control Panel is a customized web interface for administrative control and utilities that are specific to KETS needs. This is not to be confused with the Exchange Admin Center which is the Microsoft default portal for management of Exchange Online and its components. The KCP can be accessed at https://live.kyschools.us/admin/.

While ADUC and EAC will continue to be administrative tools for most tasks there are a few administrative functions that can only be performed in the KETS Control Panel. There are two different views to the KETS Control Panel, one for administrators and one for users. This means that a user with admin rights in the system will see a slightly different version of the KCP than other users. The differences between these different portal views are discussed in the following sections.

Different object types (user, group, contact) that are created in Active Directory are provisioned to O365 and Exchange Online on different schedules. Those schedules are listed below.

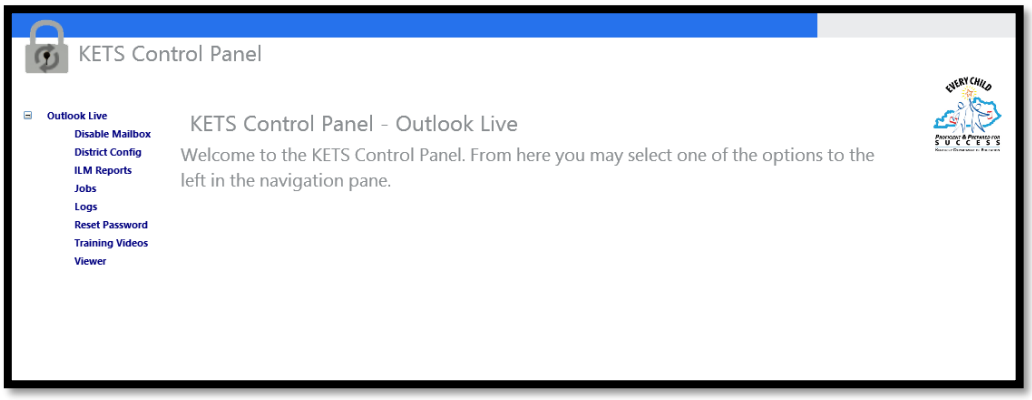
Staff Objects	Jobs run every 15 minutes, with replication latency could be up to 2 hours to fully provision
Student Objects	Jobs run every 6 hours, but manual provisioning jobs can be ran through KCP to provision new students ahead of scheduled runs
Groups	Jobs run nightly
Contacts	Jobs run nightly

Districts can run manual provisioning jobs using the KETS Control Panel (explained below) for user objects. This will not affect groups or contacts which run once during the

night. This means that groups and contacts created in AD will not show in the Global Address List until the following day.

Members of the ***DIST Support Admins*** or ***DIST Staff User Admins*** AD security groups will have authority in the admin section of the KETS Control Panel to modify settings. These areas of the control panel will be described below.

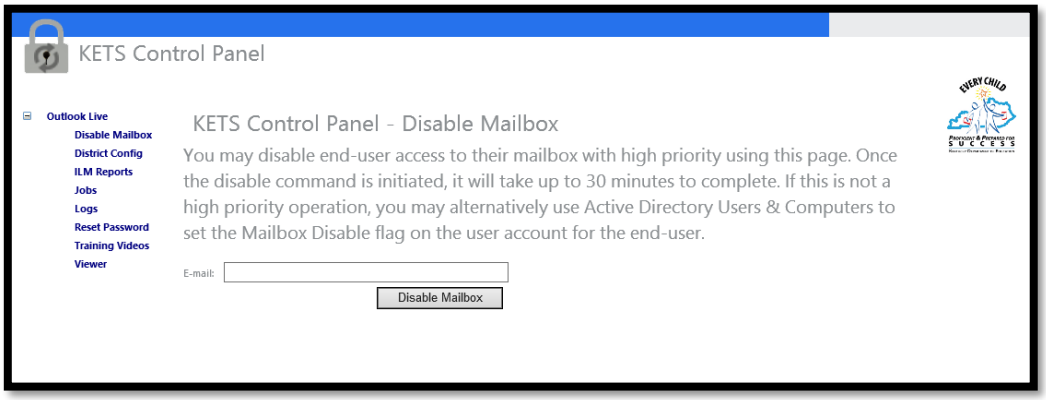
KETS CONTROL PANEL



3.5.1 Disable Mailbox

Members of DIST Support Admins and DIST Staff User Admins groups are able to disable end-user access to their mailbox using this page. DIST Support Admins can disable any mailbox. Once the disable command is initiated it may take a few minutes to complete. If this is not a high priority operation you may alternatively use Active Directory Users and Computers to set the Mailbox Disable flag on the user account for the end-user.

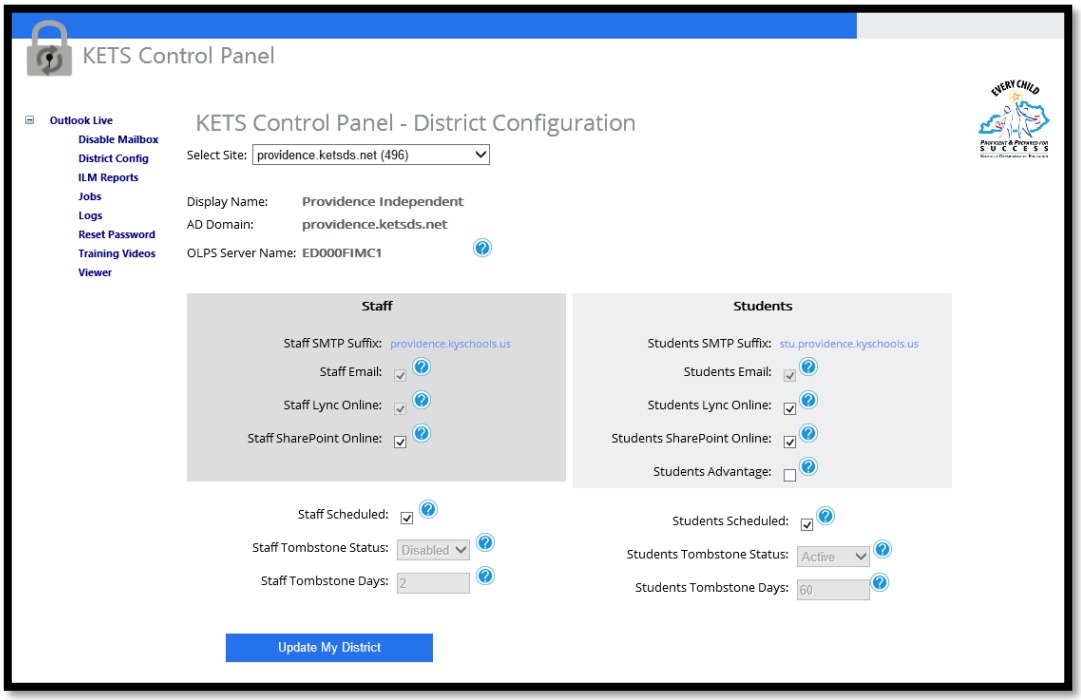
DISABLE MAILBOX



3.5.2 District Config

The District Config area of the KETS Control Panel is where members of the DIST Support Admins group have access to modify certain settings of provisioning. Districts can only manage their own configuration so the ***"Select Site"*** dropdown will automatically populate based on the account used to access KCP. Some of the settings are unavailable and will show as greyed out because they require higher levels of access or are not enabled for use at present. These options are set this way as they can cause ***dramatic*** ill-effects if not handled properly. A change to any of these values will only be applied on the weekend, so the expectation should be that modifications will be implemented by the following Monday. The default settings for the ***"District Config"*** section are shown below.

DIST CONFIG



The options in the ***"District Config"*** screen are described below.

*!!! There is **NO** recovery option for content that may be removed from SpO/OneDrive spaces as a result of unlicensing SpO. Be **very** sure you want to do this on behalf of your district users before unchecking the SharePoint Online options !!!*

- **Staff/Student Licensing Section**

  In the licensing sections for staff and students you will see the various components of O365 listed with a checkbox. Some components such as email (Exchange Online) are not currently optional to disable and will appear greyed out. However, components such as Skype for Business Online for students can be unlicensed and will be available for district admins to uncheck. These settings are for ***ALL*** students and ***ALL*** staff. Changing these settings will cause the selected component changes to be applied to the entire staff or student population respectively on the weekend following the change to the district configuration settings.

  - **Email**: Licensing for Exchange Online
  - **Skype for Business Online**: Licensing for Skype for Business Online

        - **SharePoint Online**: Licensing for SharePoint Online / OneDrive for Business. **Unlicensing SharePoint Online will also remove OneDrive for Business!**
        - **Student Advantage**: Licensing for Student Advantage Office Pro Pus Student Advantage Info
- **Staff/Student Scheduled**
    - Checked: Sets provisioning to run on a schedule for district users
        - Staff provisioning is set to run every 15 minutes, though it could take up to 2 hours to complete depending on the AD replication interval and OLPS internal processes. Students run every 6 hours.
    - Unchecked: Disable automatic runs of provisioning for district users
        - This would allow for a district to make mass modifications/etc. and/or run provisioning manually (utilizing the ***"Jobs"*** option explained below)
- **Staff/Student Tombstone**

    If the **ketseduplan** attribute has not previously been set to "NoMail" on an AD user object and provisioning allowed to run, user mailboxes will ***always*** go into a "tombstoned" state once the user object is deleted from AD. This means that the mailbox will continue to exist in O365 for a period defined by OLPS before it is finally removed entirely. The duration and the accessibility of the mailbox while in a tombstoned state is not modifiable and is a standardized value across districts. Currently staff mailboxes cannot be accessed by the end user once they enter a tombstoned state and will continue to exist in O365 for a period of 60 days before being removed. Student mailboxes can still be accessed by the end user once they enter a tombstoned state and will continue to exist in O365 for a period of 90 days before being removed.

To reattach a deleted user object to a mailbox:

If during the ***"Staff Tombstone Days"*** period the desire was to recreate the AD user object and reattach it to the mailbox the district would have to create the user object and assign the ***"E-mail"*** attribute the value of the SMTP address. **This MUST be done immediately after user creation.** This means that the desired user's AD object would need to be recreated in ADUC; then, immediately after the creation, double-click on the user object and add the user's original SMTP address in the ***"E-mail"*** field on the ***"General"*** tab. This will trigger the provisioning system to find the ***"Tombstoned"*** MSOID and link it to the new user.

3.5.3 FIM Reports

This section displays the statistics for each of the OLPS provisioning runs. You can click on each run name to get more information. This information is most helpful when troubleshooting an issue.

FIM REPORTS

ILM Run Reports

Run Name	Adds	Updates	Renames	Deletes	Start Time	End Time
ED000FIMC6 - Routine - Delta - 7/25/2014	0	1	0	0	7/25/2014 3:30:03 PM	7/25/2014 3:31:13 PM
ED000FIMC1 - Routine - Delta - 7/25/2014	0	1	0	0	7/25/2014 3:17:41 PM	7/25/2014 3:32:12 PM
ED000FIMC6 - Routine - Delta - 7/25/2014	0	0	0	0	7/25/2014 3:16:08 PM	7/25/2014 3:16:41 PM
ED000FIMC2 - Routine - Delta - 7/25/2014	1	1	0	0	7/25/2014 3:15:38 PM	7/25/2014 3:22:51 PM
ED000FIMC5 - Routine - Delta - 7/25/2014	1	0	0	0	7/25/2014 3:15:31 PM	7/25/2014 3:23:56 PM
ED000FIMC3 - Routine - Delta - 7/25/2014	0	3	0	0	7/25/2014 3:08:10 PM	7/25/2014 3:26:41 PM
ED000FIMC4 - Routine - Delta - 7/25/2014	3	2	0	0	7/25/2014 3:02:51 PM	7/25/2014 3:16:51 PM
ED000FIMC6 - Routine - Delta - 7/25/2014	0	1	0	0	7/25/2014 3:01:39 PM	7/25/2014 3:02:46 PM
ED000FIMC2 - Routine - Delta - 7/25/2014	0	0	0	0	7/25/2014 3:01:30 PM	7/25/2014 3:05:36 PM
ED000FIMC5 - Routine - Delta - 7/25/2014	0	0	0	0	7/25/2014 3:00:51 PM	7/25/2014 3:02:08 PM
ED000FIMC1 - Routine - Delta - 7/25/2014	3	0	0	0	7/25/2014 3:00:17 PM	7/25/2014 3:14:20 PM
ED000FIMC3 - Routine - Delta - 7/25/2014	3	7	0	0	7/25/2014 2:50:59 PM	7/25/2014 3:08:09 PM
ED000FIMC6 - Routine - Delta - 7/25/2014	0	1	0	0	7/25/2014 2:48:12 PM	7/25/2014 2:51:38 PM
ED000FIMC1 - Routine - Delta - 7/25/2014	1	0	0	0	7/25/2014 2:48:07 PM	7/25/2014 2:53:36 PM
ED000FIMC5 - Routine - Delta - 7/25/2014	0	1	0	0	7/25/2014 2:46:12 PM	7/25/2014 2:54:10 PM
ED000FIMC2 - Routine - Delta - 7/25/2014	0	0	0	0	7/25/2014 2:45:39 PM	7/25/2014 2:48:08 PM
ED000FIMC4 - Routine - Delta - 7/25/2014	0	4	0	0	7/25/2014 2:45:03 PM	7/25/2014 2:52:49 PM
ED000FIMC3 - Routine - Delta - 7/25/2014	5	4	0	0	7/25/2014 2:32:52 PM	7/25/2014 2:50:59 PM
ED000FIMC6 - Routine - Delta - 7/25/2014	0	1	0	0	7/25/2014 2:32:17 PM	7/25/2014 2:34:50 PM
ED000FIMC2 - Routine - Delta - 7/25/2014	0	0	0	0	7/25/2014 2:31:17 PM	7/25/2014 2:35:38 PM

ILM Run Report

ED000FIMC6 - Routine - Delta - 7/25/2014

Registry Added:	0
Registry Updated:	0
Registry Renamed:	0
Registry Deleted:	0

Detailed Report

Expand All

Name	Profile	Result	Start Time	End Time
Active Directory	Delta Import	success	7/25/2014 3:30 PM	7/25/2014 3:30 PM
OLPS Registry Service	Delta Import	success	7/25/2014 3:30 PM	7/25/2014 3:30 PM
OLPS Registry Service	Delta Synchronization	success	7/25/2014 3:30 PM	7/25/2014 3:30 PM
Active Directory	Delta Synchronization	success	7/25/2014 3:30 PM	7/25/2014 3:31 PM
OLPS PowerShell Service	Delta Synchronization	success	7/25/2014 3:31 PM	7/25/2014 3:31 PM

3.5.4 Jobs

The ***"Jobs"*** section allows for a manual run of OLPS provisioning, meaning you can force a run of ***"User mailbox provisioning"*** for users. Selecting either ***"Add Staff import Job"*** or the "***Add Students Import Job"*** will notify that OLPS should queue up a job to run through the selected district for either staff or student changes.

Realize that an import job runs every 15 minutes on a schedule by default for staff users and 6 hours for student users. This can work in conjunction with ***"Staff Scheduled"*** and ***"Student Scheduled"*** under the District Config option explained above. If there are multiple bulk changes that need to be made to all users, disabling the ***"Scheduled"*** options for staff or students would give admins time to make all the necessary changes before OLPS started to provision them to the cloud. It's important to note that groups and contacts from Active Directory do not adhere to the manual job runs, meaning that if ***"Add Staff Import Job"*** or ***"Add Students Import Job"*** is chosen this only affects user objects in AD which require mailbox access. Contacts and Groups will only provision changes on the weekends.

To kick off a run of OLPS provisioning admins can click ***"Add Staff Import Job"*** or ***"Add Students Import Job"***.

OLPS JOBS

Select District: providence.ketsds.net (496) | Add Staff Import Job | Add Students Import Job | Refresh

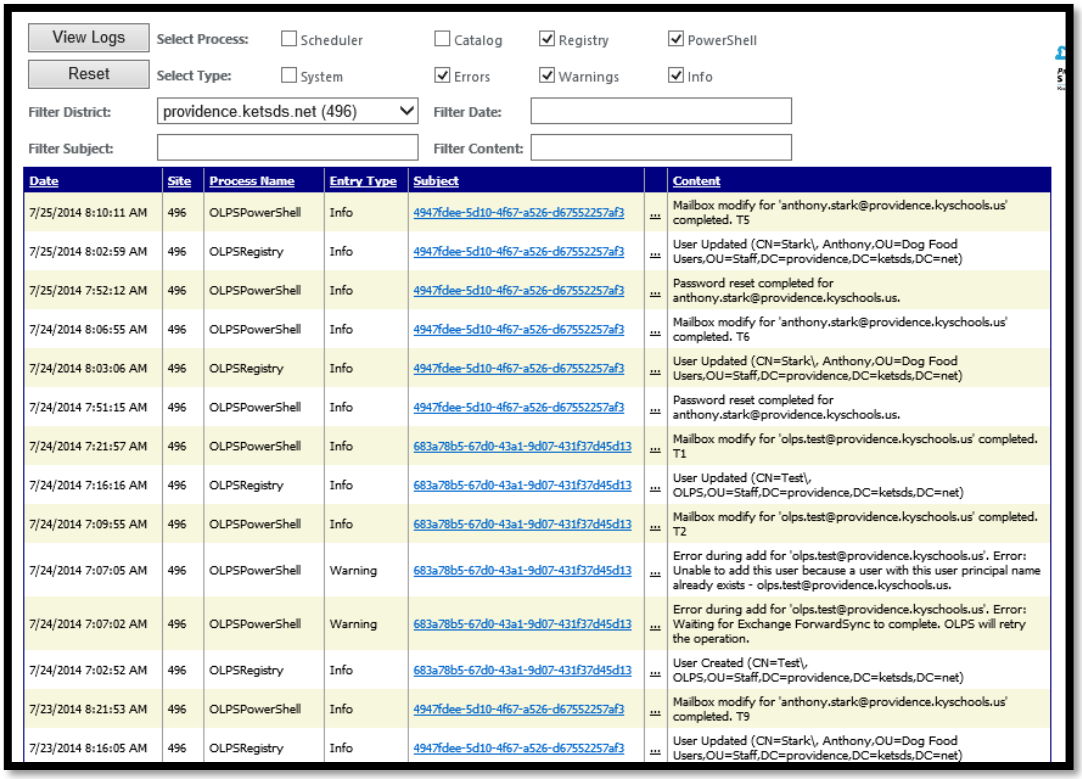
Date	Subject	Content
7/25/2014 3:31:12 PM	Server=ED000FIMC1 Site=496 Role=1	Finished Delta job for 'User'.
7/25/2014 3:31:11 PM	Server=ED000FIMC1 Site=496 Role=1	Running Delta job for 'User'.
7/25/2014 3:17:49 PM	Server=ED000FIMC1 Site=496 Role=1	Finished Delta job for 'User'.
7/25/2014 3:17:49 PM	Server=ED000FIMC1 Site=496 Role=1	Running Delta job for 'User'.
7/25/2014 3:01:05 PM	Server=ED000FIMC1 Site=496 Role=1	Finished Delta job for 'User'.
7/25/2014 3:01:05 PM	Server=ED000FIMC1 Site=496 Role=1	Running Delta job for 'User'.
7/25/2014 2:47:42 PM	Server=ED000FIMC1 Site=496 Role=1	Finished Delta job for 'User'.
7/25/2014 2:47:42 PM	Server=ED000FIMC1 Site=496 Role=1	Running Delta job for 'User'.
7/25/2014 2:30:59 PM	Server=ED000FIMC1 Site=496 Role=1	Finished Delta job for 'User'.
7/25/2014 2:30:59 PM	Server=ED000FIMC1 Site=496 Role=1	Running Delta job for 'User'.
7/25/2014 2:17:37 PM	Server=ED000FIMC1 Site=496 Role=1	Finished Delta job for 'User'.
7/25/2014 2:17:36 PM	Server=ED000FIMC1 Site=496 Role=1	Running Delta job for 'User'.
7/25/2014 2:00:53 PM	Server=ED000FIMC1 Site=496 Role=1	Finished Delta job for 'User'.
7/25/2014 2:00:53 PM	Server=ED000FIMC1 Site=496 Role=1	Running Delta job for 'User'.
7/25/2014 1:47:30 PM	Server=ED000FIMC1 Site=496 Role=1	Finished Delta job for 'User'.
7/25/2014 1:47:30 PM	Server=ED000FIMC1 Site=496 Role=1	Running Delta job for 'User'.
7/25/2014 1:30:47 PM	Server=ED000FIMC1 Site=496 Role=1	Finished Delta job for 'User'.
7/25/2014 1:30:47 PM	Server=ED000FIMC1 Site=496 Role=1	Running Delta job for 'User'.
7/25/2014 1:17:24 PM	Server=ED000FIMC1 Site=496 Role=1	Finished Delta job for 'User'.
7/25/2014 1:17:24 PM	Server=ED000FIMC1 Site=496 Role=1	Running Delta job for 'User'.
7/25/2014 1:00:40 PM	Server=ED000FIMC1 Site=496 Role=1	Finished Delta job for 'User'.
7/25/2014 1:00:40 PM	Server=ED000FIMC1 Site=496 Role=1	Running Delta job for 'User'.
7/25/2014 12:47:18 PM	Server=ED000FIMC1 Site=496 Role=1	Finished Delta job for 'User'.
7/25/2014 12:47:17 PM	Server=ED000FIMC1 Site=496 Role=1	Running Delta job for 'User'.
7/25/2014 12:30:35 PM	Server=ED000FIMC1 Site=496 Role=1	Finished Delta job for 'User'.
7/25/2014 12:30:34 PM	Server=ED000FIMC1 Site=496 Role=1	Running Delta job for 'User'.

Note: Active Directory replication has to complete for a given user in order to have OLPS pick the change up. OLPS is reading/writing from REPLC1 which is in the same AD site as the tertiary Domain Controller (D3) from each district domain which resides in Azure. Active Directory replication is set to 15 minutes between sites, so it could take up to that long for AD to create the user object in a location that OLPS reads from.

3.5.5 Logs

This section displays information/error logs for multiple components of OLPS. District Admins can utilize this area for troubleshooting. You can search using the ***"Filter Subject"*** field by typing in the SMTP Address, SAMAccountName, etc. One of the most accurate attributes to search for in the logs is the ***"SystemID"***. You can find this on ***"KETS EDU"*** tab of the user object in the ADUC console. Also filtering based on ***"Date"*** can significantly increase the

processing time of a log query. Filtering by date will return logs that were on or after the date specified.

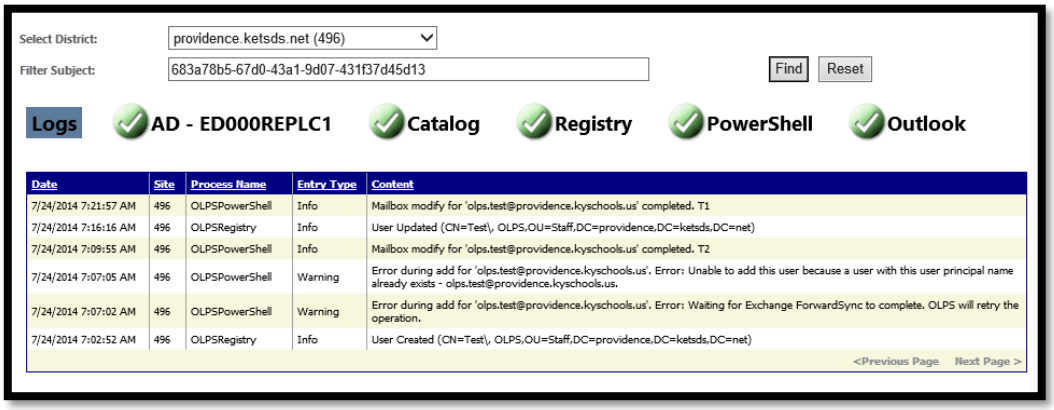


Date	Site	Process Name	Entry Type	Subject		Content
7/25/2014 8:10:11 AM	496	OLPSPowerShell	Info	4947fdee-5d10-4f67-a526-d67552257af3	...	Mailbox modify for 'anthony.stark@providence.kyschools.us' completed. T5
7/25/2014 8:02:59 AM	496	OLPSRegistry	Info	4947fdee-5d10-4f67-a526-d67552257af3	...	User Updated (CN=Stark\, Anthony,OU=Dog Food Users,OU=Staff,DC=providence,DC=ketsds,DC=net)
7/25/2014 7:52:12 AM	496	OLPSPowerShell	Info	4947fdee-5d10-4f67-a526-d67552257af3	...	Password reset completed for anthony.stark@providence.kyschools.us.
7/24/2014 8:06:55 AM	496	OLPSPowerShell	Info	4947fdee-5d10-4f67-a526-d67552257af3	...	Mailbox modify for 'anthony.stark@providence.kyschools.us' completed. T6
7/24/2014 8:03:06 AM	496	OLPSRegistry	Info	4947fdee-5d10-4f67-a526-d67552257af3	...	User Updated (CN=Stark\, Anthony,OU=Dog Food Users,OU=Staff,DC=providence,DC=ketsds,DC=net)
7/24/2014 7:51:15 AM	496	OLPSPowerShell	Info	4947fdee-5d10-4f67-a526-d67552257af3	...	Password reset completed for anthony.stark@providence.kyschools.us.
7/24/2014 7:21:57 AM	496	OLPSPowerShell	Info	683a78b5-67d0-43a1-9d07-431f37d45d13	...	Mailbox modify for 'olps.test@providence.kyschools.us' completed. T1
7/24/2014 7:16:16 AM	496	OLPSRegistry	Info	683a78b5-67d0-43a1-9d07-431f37d45d13	...	User Updated (CN=Test\, OLPS,OU=Staff,DC=providence,DC=ketsds,DC=net)
7/24/2014 7:09:55 AM	496	OLPSPowerShell	Info	683a78b5-67d0-43a1-9d07-431f37d45d13	...	Mailbox modify for 'olps.test@providence.kyschools.us' completed. T2
7/24/2014 7:07:05 AM	496	OLPSPowerShell	Warning	683a78b5-67d0-43a1-9d07-431f37d45d13	...	Error during add for 'olps.test@providence.kyschools.us'. Error: Unable to add this user because a user with this user principal name already exists - olps.test@providence.kyschools.us.
7/24/2014 7:07:02 AM	496	OLPSPowerShell	Warning	683a78b5-67d0-43a1-9d07-431f37d45d13	...	Error during add for 'olps.test@providence.kyschools.us'. Error: Waiting for Exchange ForwardSync to complete. OLPS will retry the operation.
7/24/2014 7:02:52 AM	496	OLPSRegistry	Info	683a78b5-67d0-43a1-9d07-431f37d45d13	...	User Created (CN=Test\, OLPS,OU=Staff,DC=providence,DC=ketsds,DC=net)
7/23/2014 8:21:53 AM	496	OLPSPowerShell	Info	4947fdee-5d10-4f67-a526-d67552257af3	...	Mailbox modify for 'anthony.stark@providence.kyschools.us' completed. T9
7/23/2014 8:16:05 AM	496	OLPSRegistry	Info	4947fdee-5d10-4f67-a526-d67552257af3	...	User Updated (CN=Stark\, Anthony,OU=Dog Food Users,OU=Staff,DC=providence,DC=ketsds,DC=net)

3.5.6 Viewer

By selecting ***"Viewer"*** on the left menu you can specify the SMTP address or SystemID of a user and see each component of the OPLS system that the user provisioning process has made it to.

VIEWER



3.6 SMTP Relay

The SMTP relay authenticates against Active Directory. The service account you create for SMTP relaying purposes must exist in Active Directory. Cloud only accounts will not work.

Any district applications which require SMTP relay services should be able to use the relay servers established by KDE. These relay servers accept mail from any authenticated accounts without special intervention. Most applications which use a relay provide a form where you can enter a username and password combination from a service account. With that information the applications can point to the **ketsmail.us** hostname or **10.16.1.25** IP. If the application/service accepts a URL for the hostname use "**ketsmail.us**." For those applications/services that do not accept a hostname/URL use the virtual IP address (VIP) 10.16.1.25.

If a district application/service does not support authentication first contact the KETS Service Desk requesting relay exemption for the application requiring relaying. Once access has been configured modify those applications to point to **ketsmail.us** for hostname or **10.16.1.25** for static IP. The SMTP services exist at KIDS so in the event that the link to KIDS is down this service will not be functional. This service is only available to devices that exist within the KETS network. Hosted services will not be able to use this service.

4 Exchange Online

The most used component of Office 365 as far as KETS is concerned is Exchange Online. This service is in many aspects identical to the Live@Edu implementation of email that districts are used to working with. For the most part this functionality will remain unchanged; districts should keep in mind that this is only one component that exists under the Office 365 suite of products.

4.1 Exchange Online Management Accounts

These administrative accounts are discussed in detail throughout the document in their respective areas. However, it was thought helpful to discuss them collectively in a summarized format. The following is a list of Security Groups in AD which are utilized within the O365 system as well as 'elevated' accounts/groups which exist in O365. *Note:* There are other groups in Active Directory (ex. *DIST Staff Account Reset)* which allow user password resets within AD which ultimately flow to the MSOID, but are not discussed here.

Remember that if you have staff turnover in your IT administration to change the shared O365 account passwords. A connection using these can be achieved from any internet accessible machine internal to the district or otherwise.

Below is a brief description of the different Admin accounts for user administration. Some are used in ADUC and KETS Control Panel while others are used for direct management in EAC and PowerShell. The differences are noted below. For any of the shared accounts that exist only in the cloud it is important to remember that districts with multiple IT personnel will be sharing these accounts. Any time staff changes you will want to make sure that the passwords to those accounts are changed accordingly. This is especially important since accessing a district's O365 information via PowerShell can be done from any computer with an Internet connection; one does not have to be on the district's network to gain access as long as the credentials are known.

- **OutlookAdmin@district.kyschools.us**
    - This is an O365 account (not in Active Directory).
    - Used for certain Recipient and Distribution Group administration, such as adding secondary SMTP Proxy addresses to mailboxes.

    - Can execute a subset of PowerShell commands against the O365 tenant as well as Exchange Online.
    - Has control over both staff and student users
- **OutlookAdmins@disctrict.kyschools.us**
    - This is an O365 Security Group whose members have the same access as the Outlook Admin account (this is not Active Directory).
    - Read-Only EAC access
    - OutlookAdmin has ownership, not DLAdmin.
    - Limited PowerShell in Exchange Online
        - Create new DG and DDG
        - DL/DDG Management
        - Recipient Management
- **DLAdmin@district.kyschools.us**
    - This is an O365 account (not in Active Directory).
    - MUST access through https://login.microsoftonline.com
    - Set as 'Owner' of all district Distribution Groups, whether created by Admins or users.
    - This covers both staff and student created DGs
- **SearchAdmin@district.kyschools.us**
    - This is an O365 account (not in Active Directory).
    - Used for 50
    - -Mailbox searches across all of a district's staff mailboxes.
    - Tasks can only be accomplished with PowerShell.
    - Has access to open SearchResults_district@staff.kyschools.us, where district is the district SMTP Domain Name.
    - Can search across all staff and student mailboxes for a particular district.
- **ServiceAdmin@district.kyschools.us**
    - This is an O365 account (not in Active Directory).
    - This is a Service Account only to be used to authenticate applications written to Exchange Web Services.

    - Has 'impersonation rights' to district staff/student mailboxes.
- **Members of the Active Directory group DIST Support Admins**
    - Security Group in Active Directory
    - User management access for user accounts
    - Management access through Active Directory Users and Computers and KETS Control Panel
- **Members of the Active Directory group DIST Staff User Admins**
    - Security Group in Active Directory
    - User management access for users (create users, reset passwords, etc.)
    - Management access through KETS Control Panel

4.2 GAL Visibility

Students are in the same tenant as staff users and as such, visible in the GAL along with any DGs student users create.

The KETS implementation of O365 consists of a single state-wide tenant. All users in the O365 system will be visible to every other user in the state and be able to utilize a shared contact list for use in the different O365 components (Exchange Online, Skype for Business Online). This includes staff and student accounts. This differs from the past setup in the Live@Edu system where different groups of users were segregated into separate GALs. Note that users can still be manually hidden from the GAL as needed. The process is described following section.

4.3 User E-Mail Access

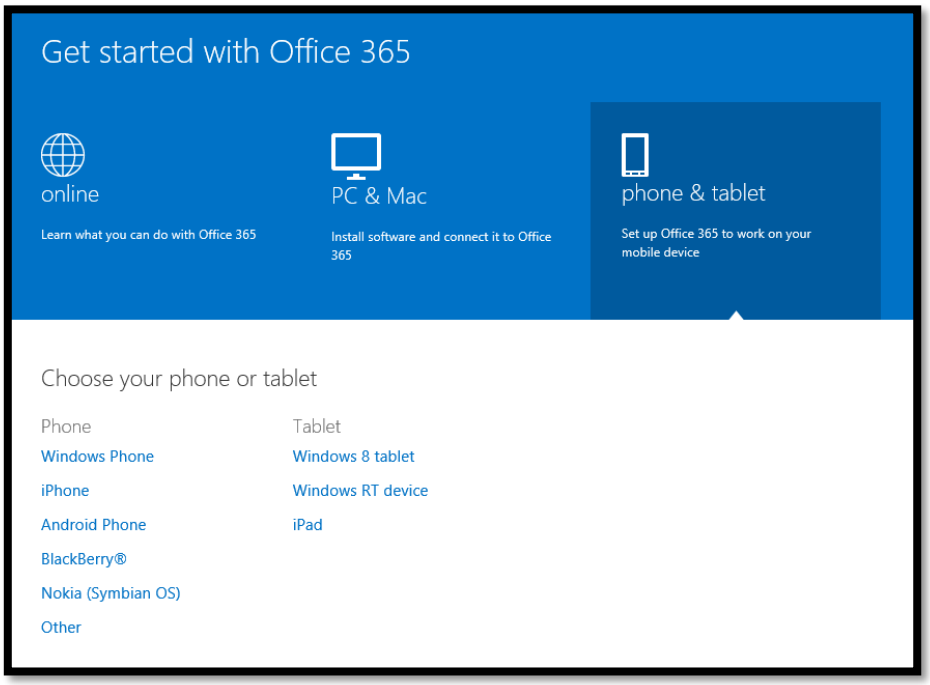
Exchange Online email services can be accessed through a variety of clients. The supported methods are as follows:

- MAPI (Outlook)
    - Setup - http://help.outlook.com/en-us/140/dd253202.aspx
- Active Sync (Mobile Devices and Other Supported Clients)
    - Setup - http://help.outlook.com/en-us/140/dd936215.aspx
- OWA (Webmail)
    - https://login.microsoftonline.com

- Click on the ***"Outlook"*** tab in the upper right hand corner of the screen

  - This is covered in the following section

- O365 Mobile Clients
  - These are accessible from the ***"Phone and Tablets"*** section of the O365 portal. https://portal.microsoftonline.com/IWGetStarted15.aspx?DisableIWLanding=true



A full list of supported clients for O365 is located at the following link.

Office365 Requirements

4.4 Group Calendars

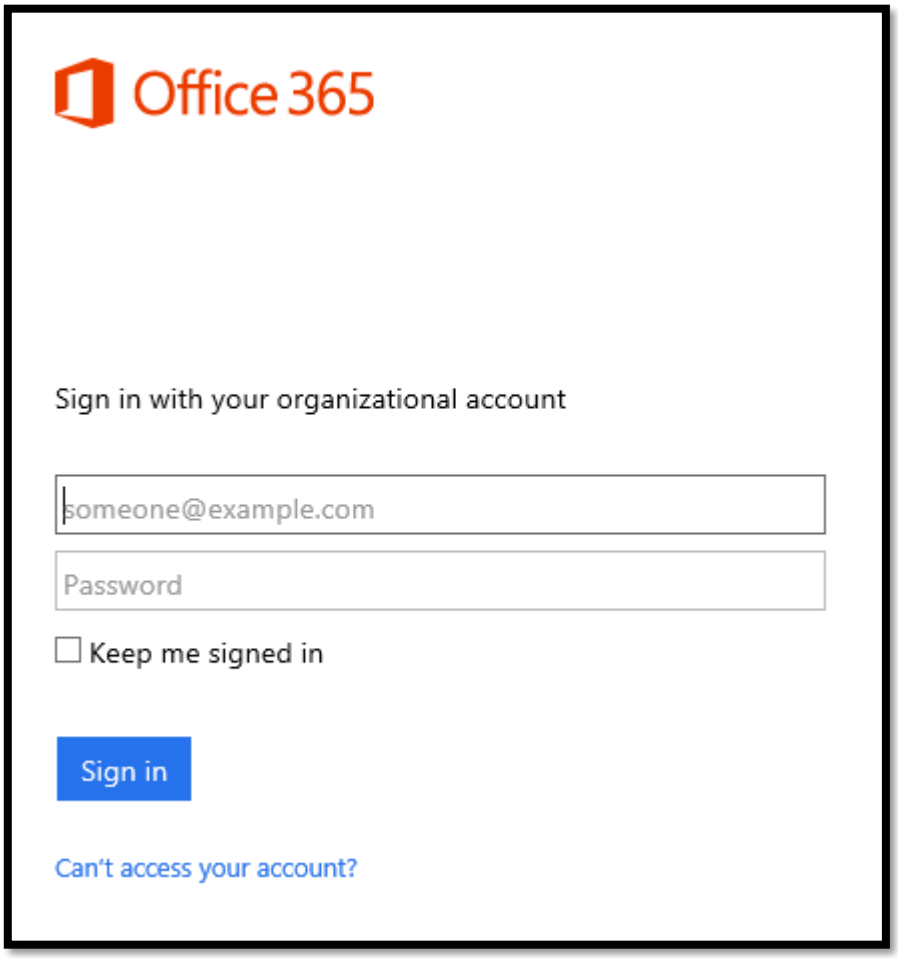
One feature that has been requested in this and previous systems are group calendars which can be accessed by multiple users. There are two options for deploying these calendars which are listed below.

1. (**Preferred**) **Create a new user object for the calendar**
    - IT Admins can create an AD object and allow it to provision or create a mailbox through Exchange Admin Center. Name this object the name of the desired Calendar and then give the appropriate users permission to view/edit content through PowerShell or GUI methods. This is explained in the following section.
2. **Secondary User Based Shared Calendars**
    - Users can create additional calendars within their own accounts by right clicking on their mailbox in Outlook or OWA, selecting ***"Create New Calendar"*** and then delegate appropriate permissions. The drawback to this method is that the group calendar is tied to a specific user account. That one person will have admin access over the calendar and if that account is deleted the group calendar will be as well.

4.5 Outlook Web App

OWA is one of the primary ways for a district to access O365 Email services. If you are a district that does not make use of the Outlook client application this is the method you will be using. The landing page for OWA is https://login.microsoftonline.com. For more information on how to make use of all the feature available in OWA see the link below: Getting Started with Outlook Web App

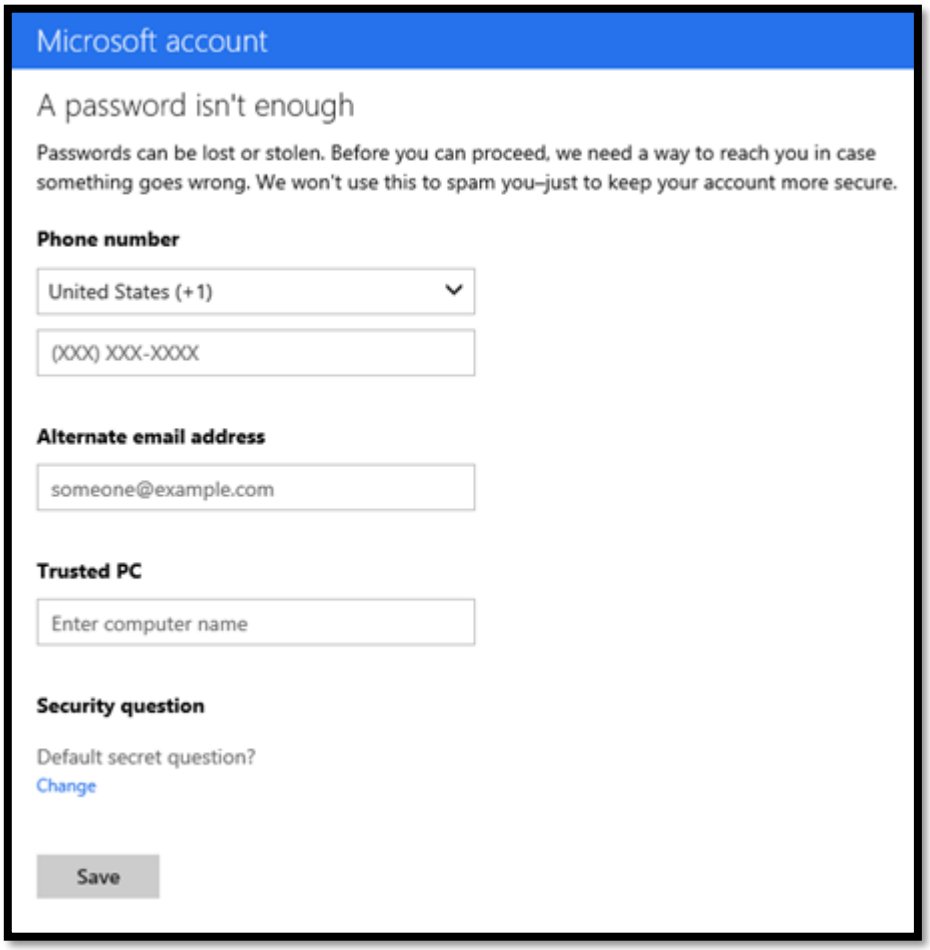
OWA



4.5.1 Password Recovery Questions

Users may get prompted upon logging in to OWA that they need to provide additional security information to be used for password recovery and to better protect their account. What type of information is entered here used here will be left up to the district to decide.

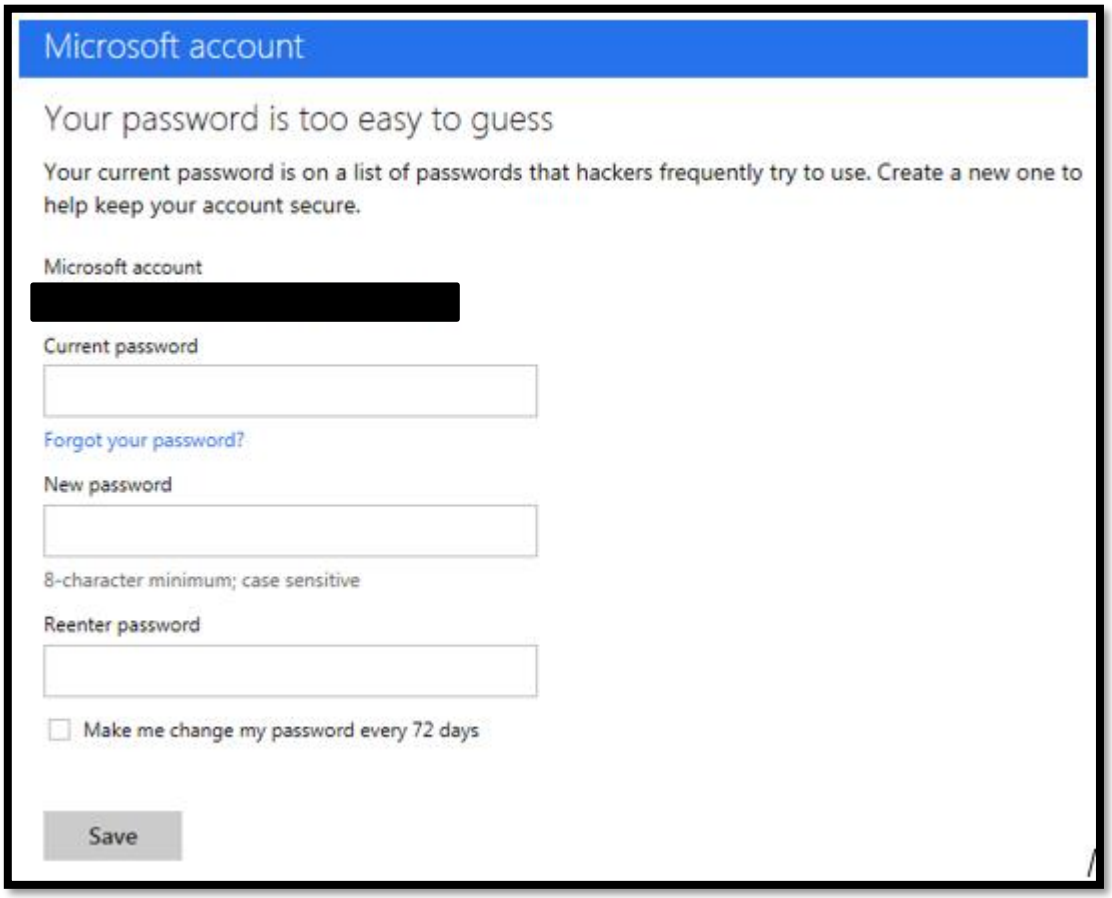
OWA PASSWORD RECOVERY QUESTIONS



4.5.2 OWA Password Security

As part of their increased security measures Microsoft also blocks the use of common passwords, even though they may still meet or exceed the minimum password length. For example, if using a password like “123456” or “password” you may be prompted to change your password through the following form. If you see this form, use it to change your password to something that meets the requirements and then afterward change your password in Active Directory to match the cloud. Make sure **NOT** to check the box below the form that reads ***“Make me change my password every 72 days”***. Active Directory needs to remain the authoritative source for password resets.

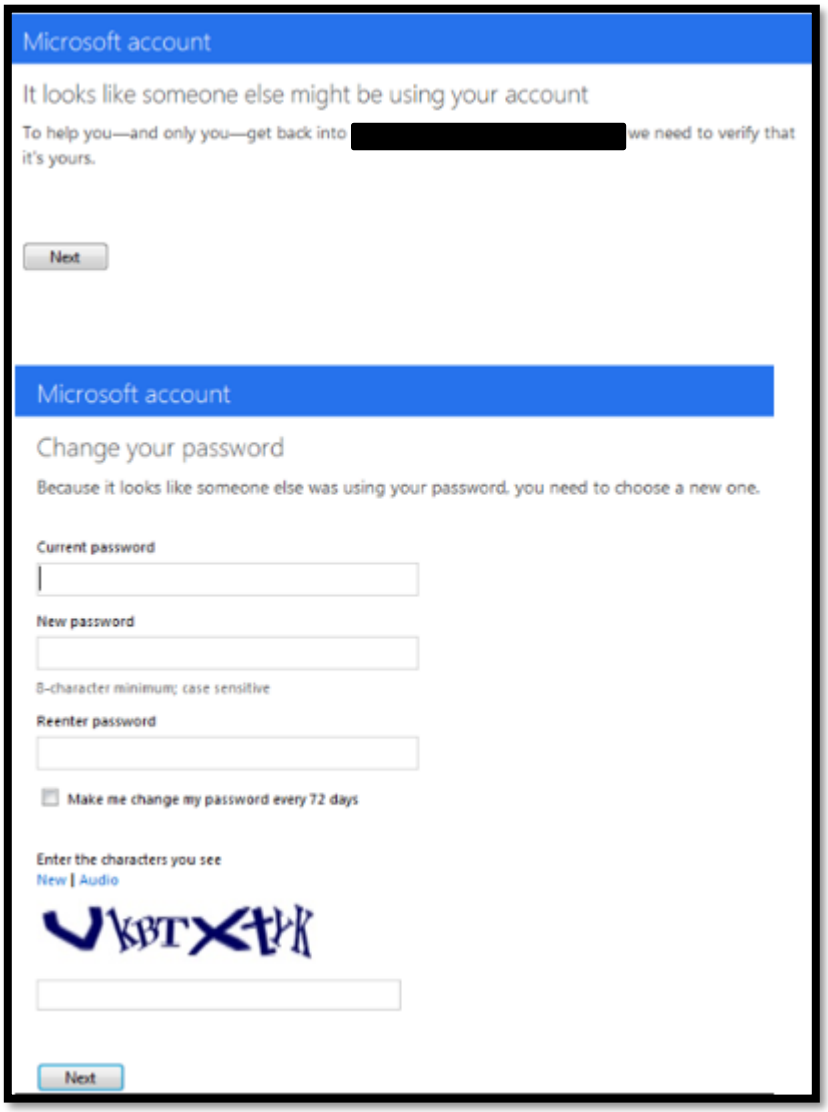
OWA PASSWORD SECURITY



4.5.3 Compromised Accounts

If Microsoft believes that an O365 user account may have been compromised in some way, they may also receive a prompt that looks similar to the one below. Changing the user's password here will change their password in the cloud, but not in AD. It is recommended that if users are prompted to do this, that they then go back and change their password to match in AD afterward.

COMPROMISED ACCOUNTS



4.6 AD Specific Management

The KETS EDU tab in ADUC allows administrative management options for O365 admins and is the preferred way to accomplish several specific O365 tasks. These are explained in more depth below.

4.6.1 Disable User Account

When talking about disabling user accounts it's important to note that the DIST Staff Deleted Mailboxes and DIST Staff Locked Mailbox groups within AD are **NOT** used for disabling user provisioning. These groups are legacy Exchange 2003 groups and have been left in case the district chose to utilize these Security Groups for other purposes. At present they have no applicable use in O365. The ***"Disable"*** option in the ***"Mailbox Options"*** section on the ***"KETS EDU"*** tab of ADUC allows a district to disable a user account in O365. Previously this only disabled the mailbox but has now been expanded to disable all services in O365 for the user.

MAILBOX OPTIONS

4.6.2 Re-Attaching AD/O365 Objects

It is important to know that if a district chooses to recreate AD user objects with the intention of re-attaching the account to an existing O365 account the SMTP email address would need to be populated in the AD user object upon recreation. If this is not done the provisioning system will generate a new MSOID for the user and append an incremented suffix to the end of the MSOID. For example, if there is already an O365 user named John Public (John.Public@district.kyschools.us) who had his AD account deleted and is now having it recreated, the email address field on his AD user object needs to be filled immediately with his MSOID or it will not reattach, and he will get a new MSOID and corresponding O365 account named John.Public2@dist.ksychools.us. Be careful when deleting accounts in this manner because you will only have until the ***"tombstone days"*** value expires to re-attach the account. After that the O365 account and associated MSOID will be deleted.

4.6.3 Preventing Incremented MSOIDs

If you would like to prevent a user from getting an incremented MSOID/SMTP email address, then you must specify what you want the MSOID to be by populating the ***"email address"*** field in ADUC as soon as the AD user is created. It is imperative that the account have this manual value filled in before provisioning has a chance to run or the account will be subject to the automatic logic built into OLPS. However, this does not allow a user with the same name as an existing user to have the same MSOID/SMTP email address. This is a case you would implement when you wish to change the MSOID in some way so that it does not follow the format of ***"First.Last@dist.kyschools.us".*** You can check to see if a user already exists in O365 by using the ***"Logs"*** section of the KCP and filling ***"Filter Content"*** with the desired email address.

4.6.4 User Name Changes

When a user requires a user name, and by extension email address, change it can be done within ADUC by highlighting the user object and pressing F2 to rename. This will highlight the name of the object and allow you to change it. You will then be presented a popup that will show other values you can choose to rename as well. It's suggested to correct the name in all places where the information needs to change and hit OK. The corresponding SMTP Address, UPN Login and MSOID will also be changed to reflect the new name. Also, the previous SMTP Primary Address before the name change will become a Secondary Proxy Address so the mailbox will continue to receive mail sent to the old SMTP Address.

4.7 Distribution Group/Contact Management

Distribution Group administration in ExO is handled differently than management of user objects. It is suggested to do all Distribution Group administration through EAC. You must be logged in as DLAdmin@*district*.kyschools.us, where *district* is your district's SMTP suffix name. Districts do have the ability to create groups in Active Directory which would provision through OLPS to Exchange Online. These groups can be created anywhere inside of the top level ***"Staff"*** or ***"Leadership"*** OUs except for ***"_Groups"***. At this time provisioned groups cannot be created within the top level ***"Students"*** OU. Even though groups can be

Groups created in Active Directory for the purpose of having a corresponding DG in Exchange Online must be set as 'Universal' Groups if they are to be provisioned to Outlook Live as well as the AD email address field being populated with the desired address for the group. This applies to both security and distribution type groups in AD.

created in AD and provisioned, there are certain tasks that can only be performed for DGs in Exchange Admin Center (such as setting ownership, permissions, etc.). No matter whether you create the group through AD and let it provision to Exchange Online or simply create the group in EAC, you **MUST** stick with the method you used to create the group to make membership modifications to it. Do not use EAC to make changes to a group that was provisioned with AD/OLPS or vice versa or there will be a mismatch between the groups in the two different environments. Groups in Active Directory which require an Exchange Online DG must NOT exist in any of the ***"_Groups"*** OUs. OLPS does not look at objects in these OUs. Ownership or permissioning of who can send to the group will not be synchronized to Exchange Online and must be set in Exchange Admin Center.

A couple of interesting features to point out are Message Approval and the ability for users to add themselves as members to DGs. Notice below that if the DG is set for 'Message Approval' you can specify the moderator who would have all messages sent to the DG first sent to them for approval or rejection. You can also select users who would not have their messages 'moderated'. Another extremely valuable for Distribution Group management is the ability to create DGs which are ***"Open"*** or ***"Owner Approved"***. This means that a group can be set any of three ways for membership.

Groups that are created in Active Directory are created in Exchange Online as "Closed". Those created using Exchange Admin Center are set to "Open" as default.

DISTRIBUTION GROUP MEMBERSHIP SETTINGS

- **Closed** - Member can only be added by an Owner of the group
- **Open -** Any user can add themselves to the group
- **Owner Approval** - Requests to be added are sent to group Owners. First Owner to approve or deny wins.

DLAdmin@district.kyschools.us is automatically set as an owner of any Distribution Group that's created in Exchange Online. This happens nightly via a job scheduled in OLPS. The DLAdmin or the creator of the group will need to add additional users as ***"Owner"*** if more than the initial creator is desired. Owners can perform tasks such as Enable Message Approval, Change Group Properties in Exchange Admin Center, use Remote PowerShell to manage groups, set who can send to the group, etc.

There are certain statewide shared DGs that districts should continue to maintain membership of such as ***"Allen Co Teachers"*** or ***"Pineville Ind Principals"***. These Distribution Groups are nested under top-level DGs such as ***"All State Teachers"*** which are used for mass mailings by selected individuals (Commissioner of KDE, etc.). Districts can look at the ***"Member of"*** tab on these suspected DGs to see the membership if there is a question. A single Outlook Live mailbox can only send to 10,000 individual recipients per day. However, DGs only count as one recipient. If a district has users, say a superintendent or principal, who need to send bulk e-mails they should utilize Distribution Groups to do so. Make sure that these DGs are limited in respect to who has permission to send to them. This can be done in EAC in the group settings.

Make sure to do this so that users cannot reply to all or see the other recipients of the bulk email.

Also, any time a user sends to large numbers of recipients they should adopt adding that Distribution Group/recipients to the 'BCC' field in the new mail form instead of the 'To' field. The sender should add his or her own account to the 'To' field. This is explained in greater detail in the following section.

Any user in Exchange Online may create a DG. Any DGs created by end users will be visible to all other users in the GAL if not hidden through the KETSEDU tab in ADUC or through the settings of the group in EAC. In order to keep the GAL in readable condition districts should use the naming scheme requirements in the following section.

4.7.1 KETS State-wide Shared Distribution Group Permissioning

The following Distribution Groups are sponsored by KDE and are to be provisioned properly to allow for certain individuals (KDE Commissioner, etc.) to send to the members. **Membership is to be properly maintained by the district.** Districts have the flexibility to add additional permissions if they so choose.

The permissions you set do not inherit downward to any sub-DLs which are nested under another group. Permissions must be set on each group at each level for mail to flow successfully.

To assign access rights to each distribution list, go to the Options link inside EAC (with the DLAdmin account), go to "Groups" and "Public Groups I Own" and follow the steps outlined below. If no one is listed in Delivery Management then everyone can send to the group; if there is a user or group listed in the Delivery Management then only the members

(not nested members) can send in to the group. Currently these DGs are restricted to receiving mail only from users within the tenant.

- ***District Name* Supt:** Click on "Delivery Management" and add "*All State Supt" and "Admin SDL" as well any additional user or group in your district that should send; Click Save.*
- ***District Name* Prin:** Click on "Delivery Management" and add "*All State Prin" and "Admin PDL" as well any additional user or group in your district that should send. Example: "**Adair Principals**" or **"Doe, Joe";** Click Save.*
- ***District Name* EL Prin:** Click on "Delivery Management" and add "*All State Prin" and "Admin EPDL" as well any additional user or group in your district that should send. Example: "**Adair El Principals**" or **"Doe, Joe";** Click Save.*
- ***District Name* MS Prin:** Click on "Delivery Management" and add "*All State Prin" and "Admin MPDL" as well any additional user or group in your district that should send. Example: "**Adair MS Principals**" or **"Doe, Joe";** Click Save.*
- ***District Name* HS Prin:** Click on "Delivery Management" and add "*All State Prin" and "Admin HPDL" as well any additional user or group in your district that should send. Example: "**Adair HS Principals**" or **"Doe, Joe";** Click Save.*
- ***District Name* Teachers:** Click on "Delivery Management" and add "*All State Teachers" and "Admin TDL" as well any additional user or group in your district that should send. Example: "**Adair Teachers**" or **"Doe, Joe";** Click Save.*
- ***District Name* EL Teachers:** Click on "Delivery Management" and add "*All State Teachers" and "Admin ETDL" as well any additional user or group in your district that should send. Example: "**Adair EL Teachers**" or **"Doe, Joe";** Click Save.*
- ***District Name* MS Teachers:** Click on "Delivery Management" and add "*All State Teachers" and "Admin MTDL" as well any additional user or group in your district that should send. Example: "**Adair MS Teachers**" or **"Doe, Joe";** Click Save.*
- ***District Name* HS Teachers:** Click on "Delivery Management" and add "*All State Teachers" and "Admin HTDL" as well any additional user or group in your district that should send. Example: "**Adair HS Teachers**" or **"Doe, Joe";** Click Save.*

- ***District Name* IT Teachers (for District Itinerant teachers):** Click on "Delivery Management" and add *"All State Teachers" and "Admin ITDL" as well any additional user or group in your district that should send. Example: "**Adair IT Teachers**" or **"Doe, Joe";** Click Save.*☒

In the examples above "All State Teachers" is not a group; it is actually a mailbox. Thus it does not contain actual users and should NOT be treated as normal security groups would be.

4.7.2 Renaming a Security or Distribution Group in Active Directory

If a Security or Distribution Group is being managed from Active Directory and the desire is to rename the group then highlight it in ADUC > hit F2 > and type desired name. This change will not change the SMTP address of the group. Districts should abide by the naming standards set forth in the following section.

4.7.3 Dynamic Distribution Groups

Exchange Online supports a special kind of distribution group called a Dynamic Distribution Group. District IT Administrators have the ability to create DDGs. Unlike the static membership list of a regular distribution group the membership list for a dynamic distribution group is calculated every time a message is sent to the group. This calculation is based on filters and conditions you define when you create the group. When an e-mail message is sent to a dynamic distribution group it is delivered to all recipients in the organization that match the filters and conditions you defined. This can be triggered off of a number of attributes of the Exchange Online user objects. Only the respective OutlookAdmin account has access to create DDGs. Dynamic Distribution Groups can only be created using Windows PowerShell. More information on syntax for creating DDGs can be found at the following link.

Even though DDGs can be created via EAC, a valid district domain suffix cannot be specified. Because of this districts should only use PowerShell to create DDGs.

4.7.4 State-Created Dynamic Distribution Groups

There are three state-created Dynamic Distribution Groups that exist for the users of each district. They are ***"everyoneDL@dist.kyschools.us", "districtco-staff@district.kyschools.us",*** and ***"districtco-students@district.kyschools.us"***. ***"everyoneDL@dist.kyschools.us"*** contains all the users in a district, both staff and students. ***"districtco-staff@district.kyschools.us"*** contains only the staff users in a district and ***"districtco-students@district.kyschools.us"*** contains only the student users in a district. Since these are Dynamic DGs they will automatically update their membership with any users that fit the criteria specified, so no one has to manually add membership to these groups. These are hidden DGs meaning they will not show in the Global Address List. Users within a district can send to these by typing the SMTP address of the DGs. The lists will have slightly varying naming schemes based on the type of district it is. See below for examples of the naming schemes.

STATE-CREATED DG NAMING SCHEME EXAMPLES

District	Adair County	Harrodsburg Independent	Kentucky School for the Blind
All Users	everyoneDL@adair.kyschools.us	everyoneDL@hburg.kyschools.us	everyoneDL@ksb.kyschools.us
All Staff	adairco-staff@adair.kyschools.us	hburgind-staff@hburg.kyschools.us	ksb-staff@ksb.kyschools.us
All Students	adairco-students@stu.adair.kyschools.us	hburgind-students@stu.hburg.kyschools.us	ksb-students@stu.ksb.kyschools.us

There is a moderator set on each of these distribution groups meaning that any message which is sent to the SMTP address of the DG would first be sent to a moderator. This person would have to allow or reject any message sent to either of these groups. You can also select specific users whose messages do not have to go through a moderator. The account that is set as the moderator is DLAdmin@district.kyschools.us. A designated person in the district would need to either login to OWA/Outlook using this account to check for moderated messages sent to the DG or setup an Inbox Rule to forward the mail to another mailbox. If forwarding was set on the DLAdmin mailbox then the mailbox forwarded to would get the message, but they would have to also log in to the DLAdmin account to approve of the

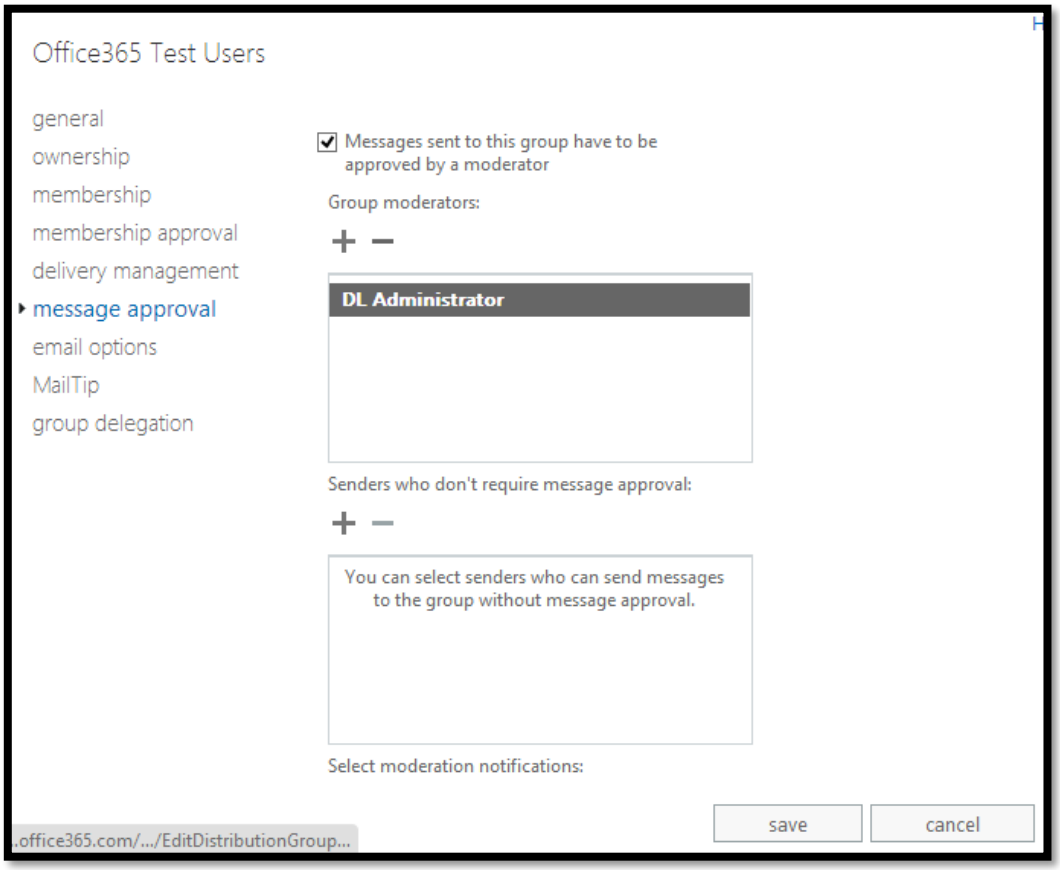
message and allow sending. To edit any of these settings you must use PowerShell. For more information on how to create/edit DDGs see the following article: Creating/Editing Dynamic Distribution Groups

4.7.5 Sending to Large Groups

Large Distribution Groups (those with membership larger than 500) or Dynamic Distribution Groups should be set with Moderation via EAC. Also, when sending to large Distribution Groups users should always send to the group using the BCC (Blind Carbon Copy) option on the New Mail form. Normally only district administrative staff should have access to send to larger groups. The best practice is for the senders to put their own email address in the ***"To:"*** field and the group they are sending to in the ***"BCC".*** By sending to the BCC you take away the potential for recipients of a message to a large group to hit 'Reply All' as objects on the BCC are not included on a 'Reply All'. Also, users cannot see the other members of the BCC.

Any distribution Groups that have large membership (ex. Providence Teachers) **SHOULD BE MODERATED**. This means that any messages sent to the Distribution Group would first go to a mailbox designated to approve messages that are sent. This limits the amount of unnecessary messages that are sent to large numbers of recipients. This can be done from within EAC.

ENABLE MODERATION



4.7.6 Creating Contacts

Contacts that are not AD users or associated with the tenant can be created in AD and then provisioned via OLPS. Contacts are only provisioned at night from AD to Exchange Online. Districts need to create all contact objects in the ***"_Exchange Resources"*** OU under the "**Staff"** or "**Leadership"** OUs in order to have them correctly provisioned to O365 via OLPS. You must specify the SMTP address of the contact upon creation.

4.8 Naming of Objects and GAL Visibility

It's imperative that districts utilize solid naming standards to segregate their objects as much as possible, specifically Distribution Groups. This is very important to convey to district users as any user with a mailbox can create a DG which will be visible to all other users in the state.

4.8.1 Naming of Distribution Groups

In the Exchange Online environment all Distribution Groups will be seen by all users in the state and not just by the district the DG exists in. Therefore, proper naming of objects is critical. With that in mind it is in the district's best interest to apply verbose naming standards when creating any objects. All groups should begin with the district name followed by either the ***"Co"*** or ***"Ind"*** designation and then the purpose of the group.

District administrators, and end users, should use the following standard when naming Distribution Groups (or possibly other accounts, like Conference Room, Library, etc.):

- **Examples**
  - Adair Co HS Teachers
  - Franklin Co Western Hills High School Library
  - Jackson Ind Coaches

To assist with this KIDS will be placing the district name in the ***"Company"*** field of AD user objects which will help in distinguishing objects with similar/same names in the Global Address List. This does ***not***, however, apply to Distribution Groups which do not have a ***"Company"*** attribute. The ***"Company"*** attribute in AD will not be populated by OLPS; only the Exchange Online account receives this attribute for GAL visibility.

4.8.2 Naming of Resource Accounts

Any resource account which must be visible in the GAL should be given a display name which begins with the name of the district. In this way, all of a given district's resource accounts will be clustered together in the GAL rather than dispersed throughout it. Similar to

Distribution Groups, district administrators should use the following standard when naming resource accounts.

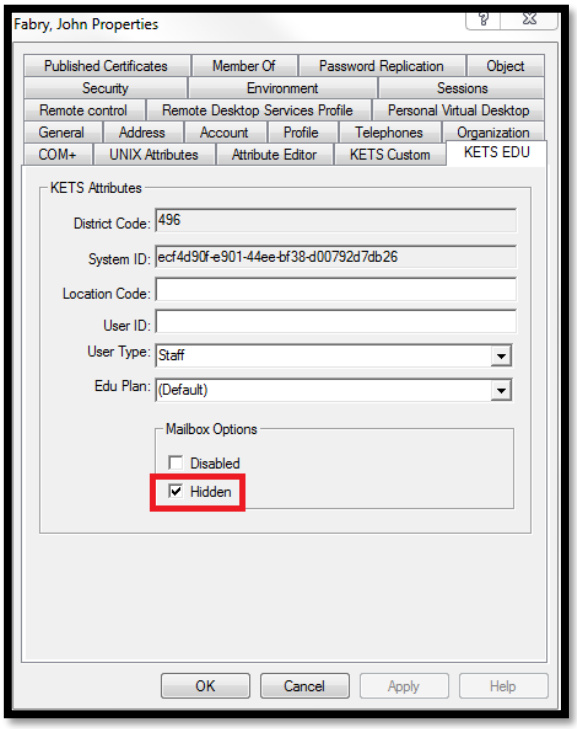
- **Examples**
  - Scott Co Board Office Conference Room
  - Somerset Ind Community Questions
  - Woodford Co Help Desk

Please be mindful of whether or not resource accounts actually need to be mail enabled. Resource accounts used purely for authentication purposes and which will never receive mail should not have a mailbox. Any such accounts should be set to **"NoMail"** on the KETSEDU tab in ADUC before provisioning to ensure it does not receive a mailbox. Also, accounts which need to receive mail but which do not need to searchable in the GAL should be hidden.

4.8.3 Distribution Group and Service Account GAL Visibility

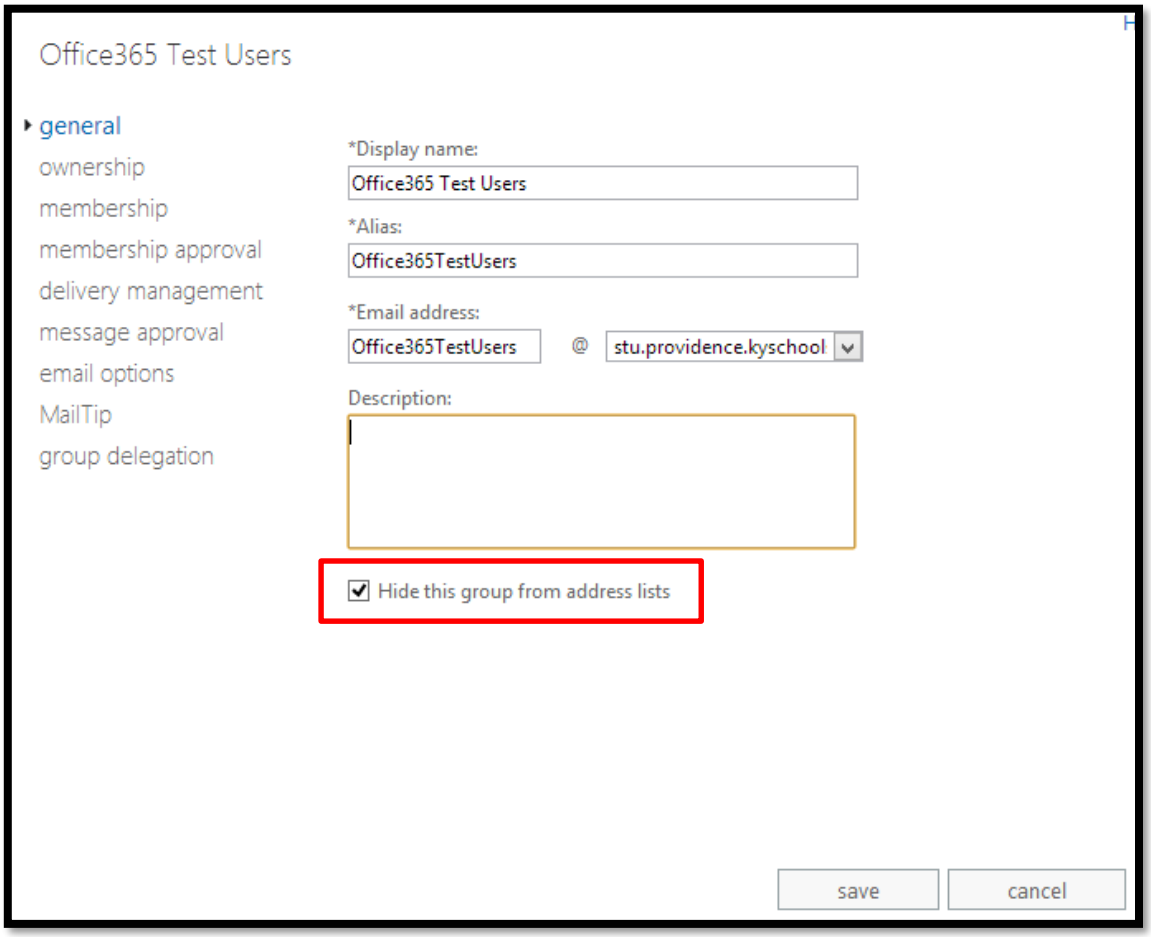
District administrators have the option to hide DGs from the GAL. Hiding groups and accounts that originated in AD and were provisioned to O365 can be done through EAC or the ADUC console. In ADUC you can hide users form the GAL by checking the ***"Hidden"*** checkbox on the ***"KETS EDU"*** tab.

HIDDEN ATTRIBUTE



In EAC, DGs can be hidden by going to the settings of the DG and checking the ***"Hide this group from the shared address book"*** option.

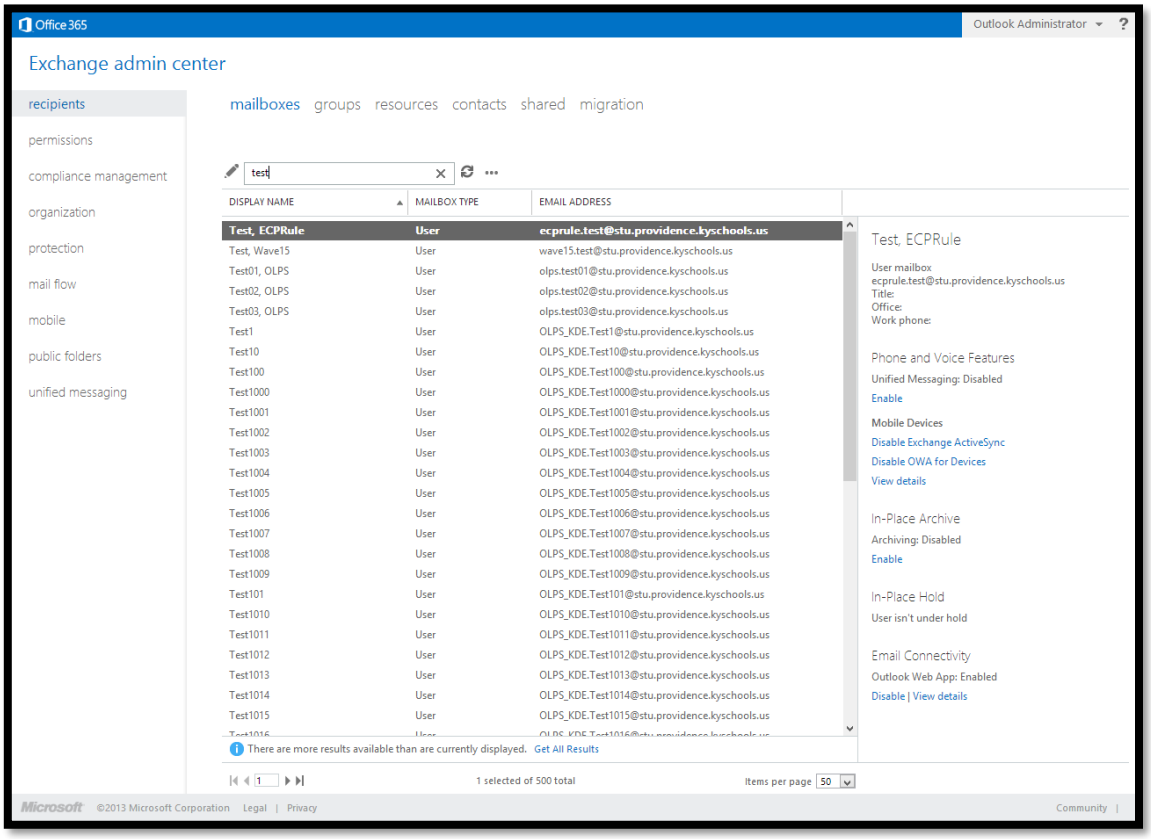
HIDE DISTRIBUTION GROUP



4.9 Exchange Admin Center

The Exchange Admin Center is the web interface that allows for common mailbox administration tasks in Exchange Online. Most tasks that a district administrator would need to accomplish in Exchange Online can be done through the ADUC management console thanks to the implementation of OLPS. But there are several features that can only be done through EAC. You can access EAC at the following link: Exchange Admin Center

EXCHANGE ADMIN CENTER



You will now be able to edit Exchange Online settings for your entire district. You can perform common tasks like change memberships of DGs, create mailboxes, etc. Understand that most tasks are automatically performed against objects in Active Directory as districts create and modify those objects and should not need to be accessed through EAC other than in select circumstances.

If districts choose to create mailboxes or DGs with Exchange Admin Center it is important to understand that these objects will NOT pass through the OLPS system. There will not be an equivalent AD object created, nor will there be any record keeping for these objects. OLPS keeps track, for instance, of all SMTP addresses that *it* assigns. This verifies that there are no duplicates. If a mailbox object is created using Exchange Admin Center, it would set the SMTP address automatically within Exchange Online. If afterwards a user is

created in Active Directory Users and Computers that had the same name (First Name and Last Name which concatenated together match the SMTP address of the mailbox) OLPS would throw an error because it has no knowledge of the account that already exists in O365.

There are occasions where it makes sense to create mailboxes that do not have an associated AD object, or Distribution Groups that do not have a corresponding Security Group in AD. It's important to think through the requirements and results before making these kinds of administrative decisions.

4.10 E-Mail Addresses and Secondary (Proxy) Addresses

The standard format for a Staff user's SMTP address is: FirstName.LastName@district.kyschools.us. This is automatically done through OLPS provisioning.

Districts have the ability through PowerShell to create secondary addresses for Exchange Online. This is covered in the following section. Alternately, districts that require additional e-mail addresses such as "webmaster", "administrator", etc. could create additional "resource" user objects in ADUC with the appropriate naming. Districts could then choose to access these additional mailboxes with https://login.microsoftonline.com or configure an Inbox Rule in the resource mailbox to flow messages to the desired mailbox (http://help.outlook.com/en-us/140/ms.exch.ecp.learnredirectto.aspx).

You may notice that every Staff mailbox has a Secondary E-mail Address following the standard FirstName.LastName.district@staff.kyschools.us that ends in "***staff.kyschools.us***". This address was used during the migration from on-premise Exchange and should not be deleted.

4.11 Allowed Attachment Extensions in Exchange Online

The following link shows the attachment extensions which are allowed through the Exchange Online system in O365. Note that the web page discusses changes that can be made in Exchange 2010 by administrators as well as other settings. This is to be ignored. The only pertinent information for this discussion is the table in the web link which shows the

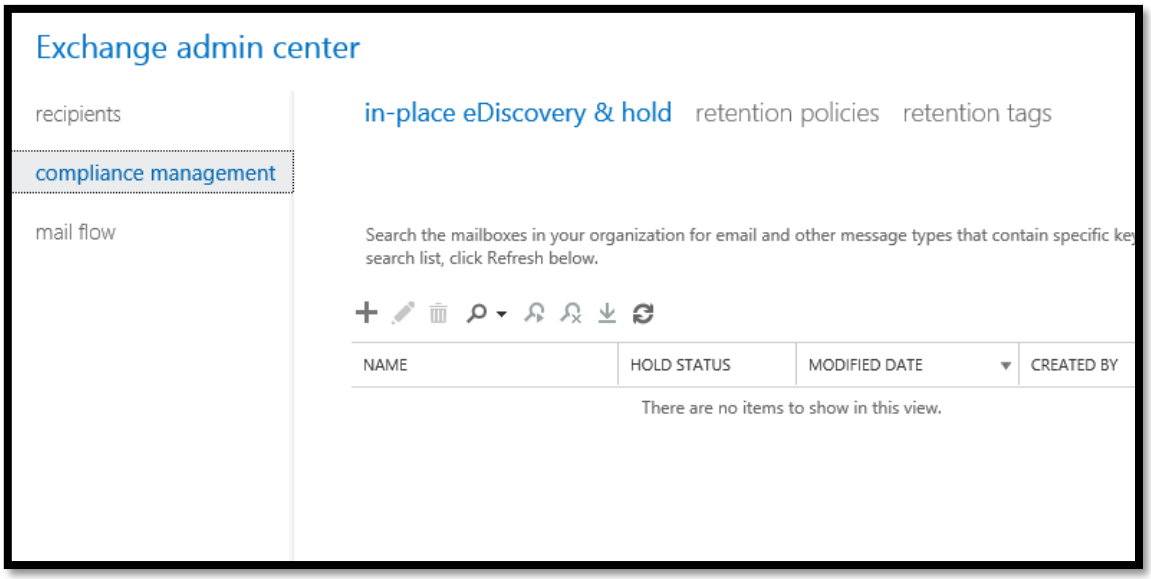
different file types that are allowed or blocked.

Allowed Attachment Extensions in Exchange Online

4.12 Mailbox Searches in EAC

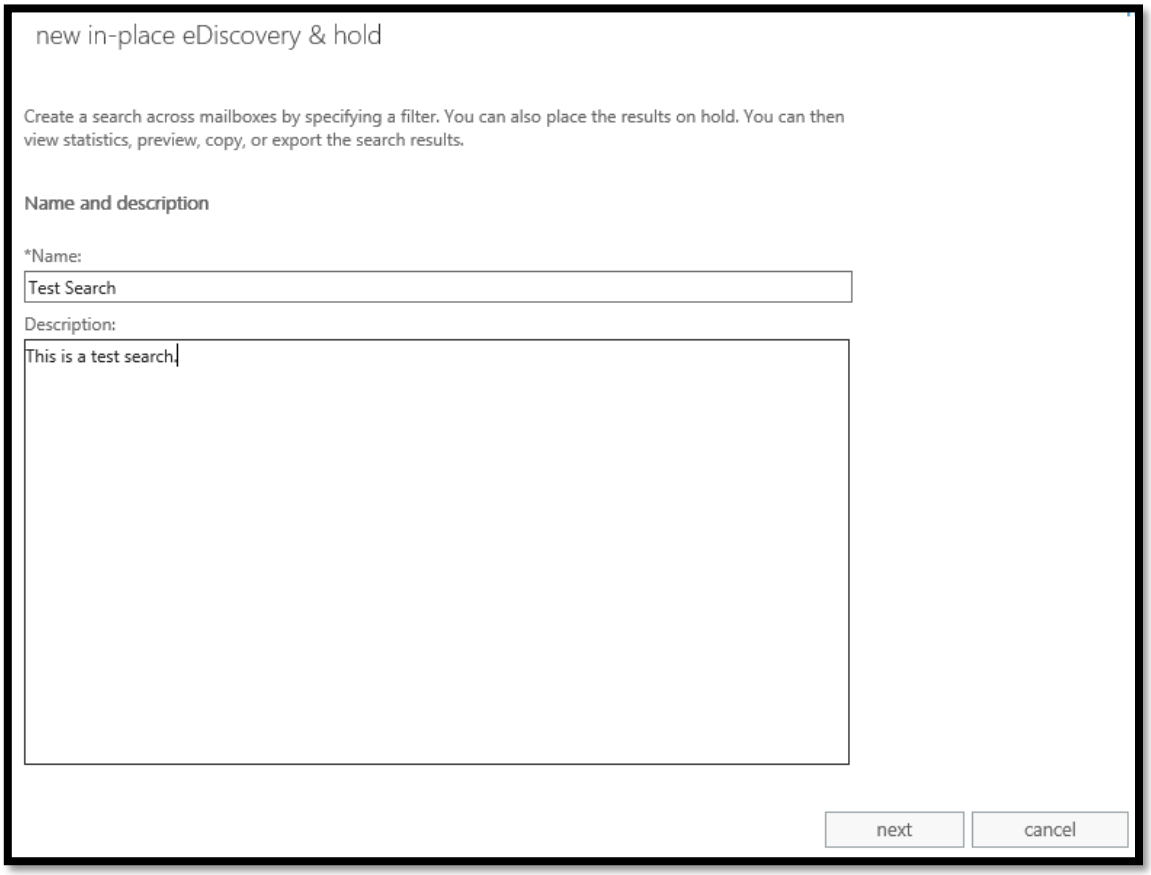
Districts have the option to run mailbox searches for content through EAC by logging in with the ***SearchAdmin@district.kyschools.us*** service account at https://outlook.office365.com/ecp.

Then select the ***"in-place eDiscovery & hold"*** option in the ***"Compliance Management"*** section to the right.



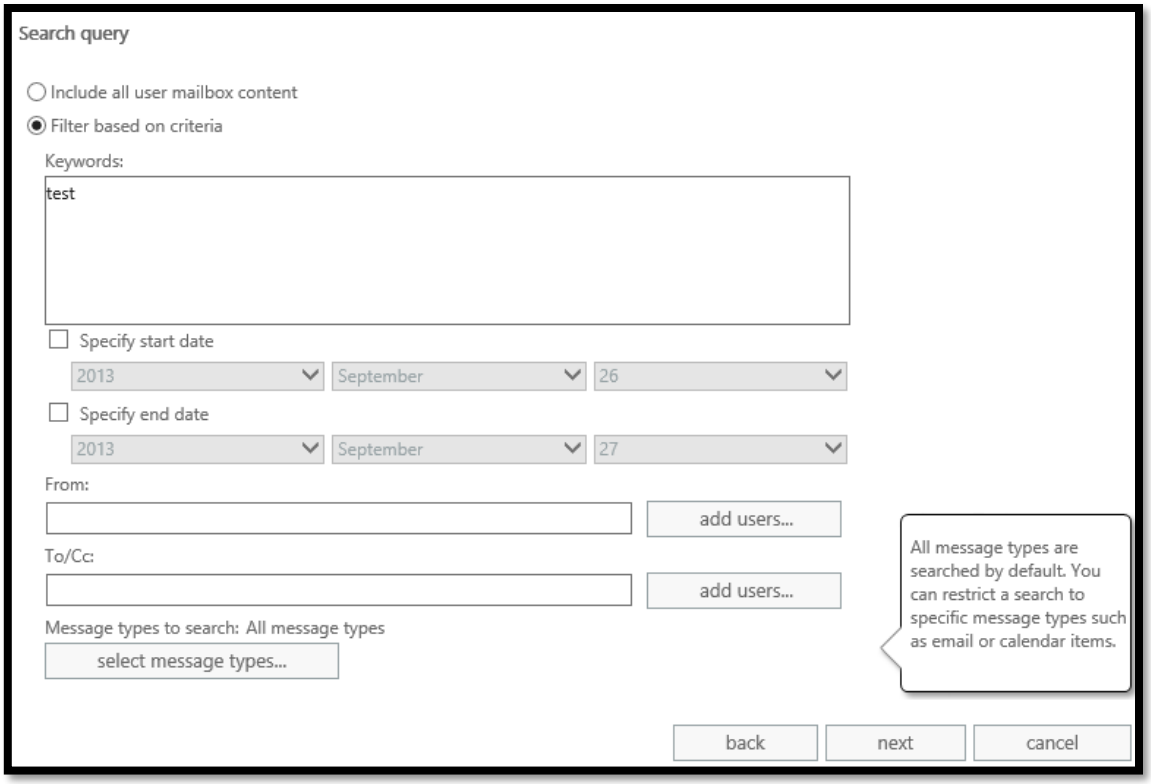
Click the ***"+"*** symbol to create a new search which will open a new search dialog window. In this series of windows you will define the parameters for your search.

*It is **VERY** important that you not name your search or the description something specific where the nature of the search could be determined as all districts will be able to see the listing of past searches done across the tenant.*

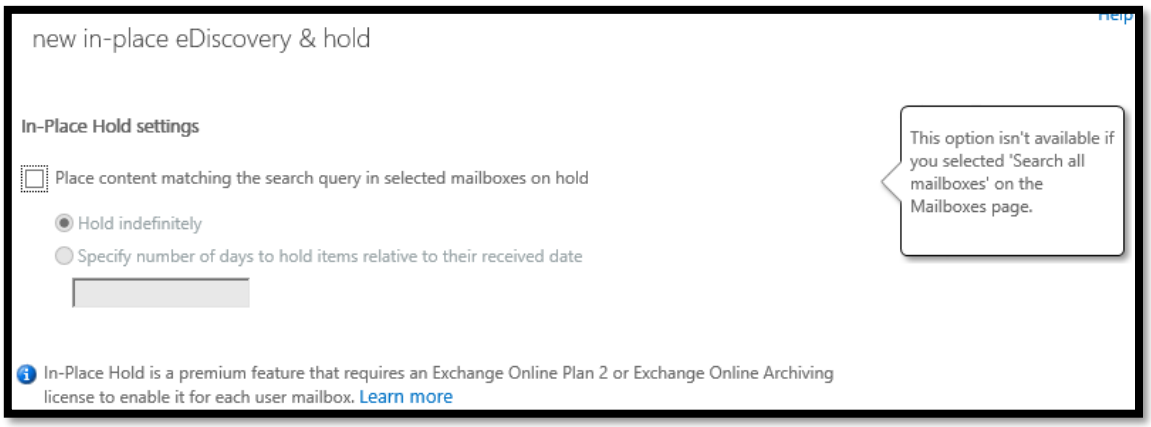


You can then specify what mailboxes you wish to search and what the criteria will be.

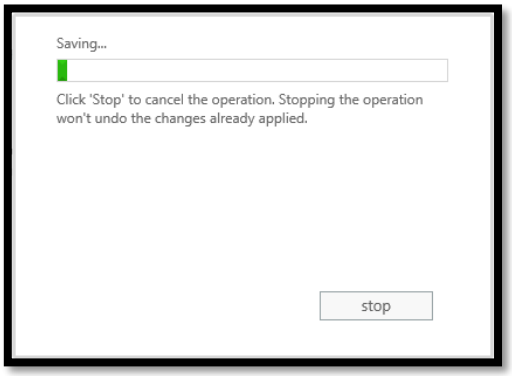
Mailboxes
Search all mailboxes
Specify mailboxes to search
Test01, OLPS
Test02, OLPS
Test03, OLPS

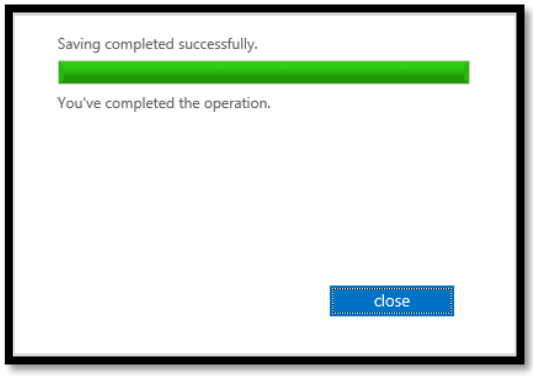

Search query
Include all user mailbox content
Filter based on criteria
Keywords:
test
Specify start date
2013
September
26
Specify end date
2013
September
27
From:
add users...
To/Cc:
add users...
Message types to search: All message types
select message types...
All message types are searched by default. You can restrict a search to specific message types such as email or calendar items.
back
next
cancel

The fourth screen will ask you for In-Place Hold settings. KETS does not have this service as part of our office 365 plan, and as such you will not be able to use it. Make sure to leave the box here unchecked.

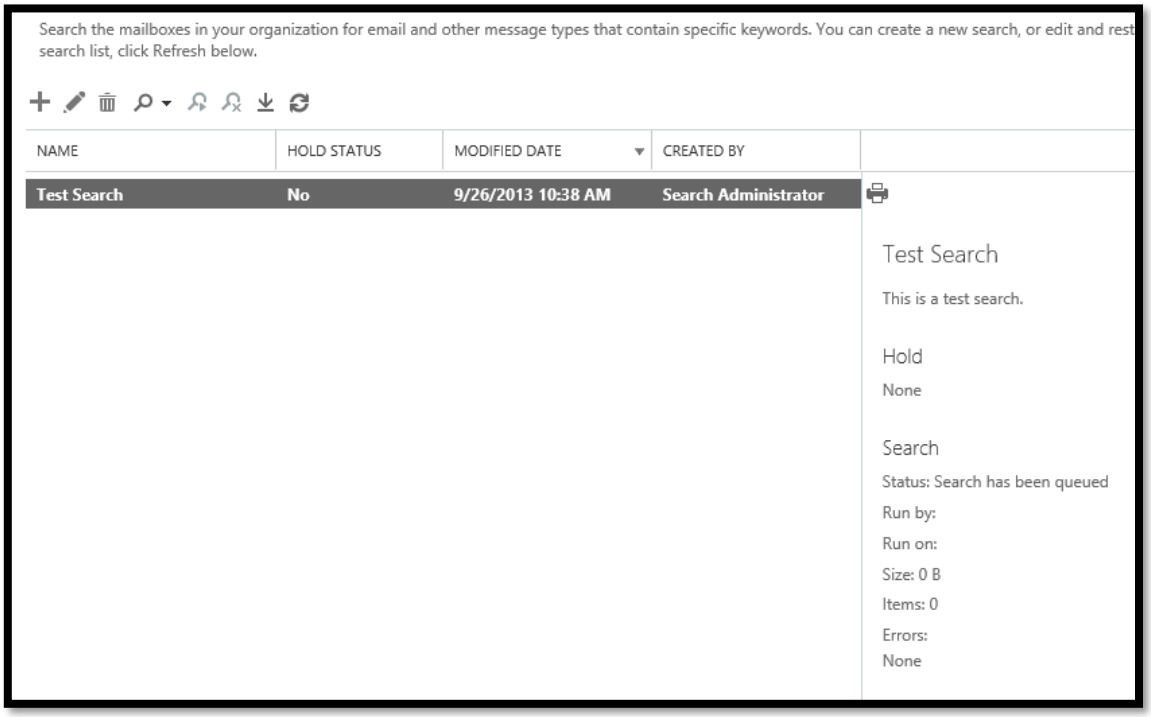


After clicking finish you will see a window showing the creation progress of your search.

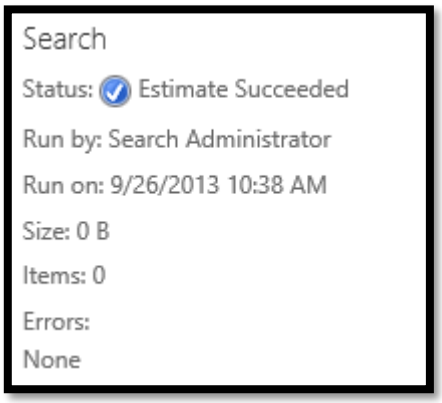




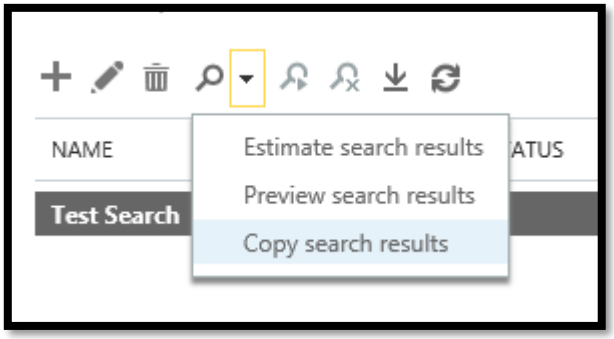
Now you will see your search listed in the eDiscovery page you started on.



Initially it will say that your search has been ***"Queued"***. The search estimation process itself will execute automatically and if you refresh the page after a short delay you should see the status turn to ***"Estimate Succeeded"***.



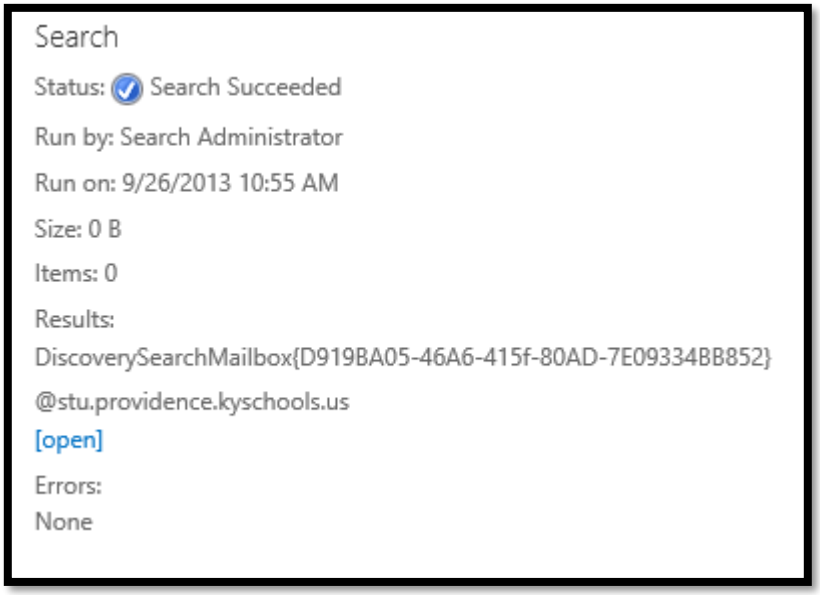
From here, if you actually want to perform the search you can do so by clicking on the arrow next to the magnifying glass icon at the top of the screen with your search selected in the job list.



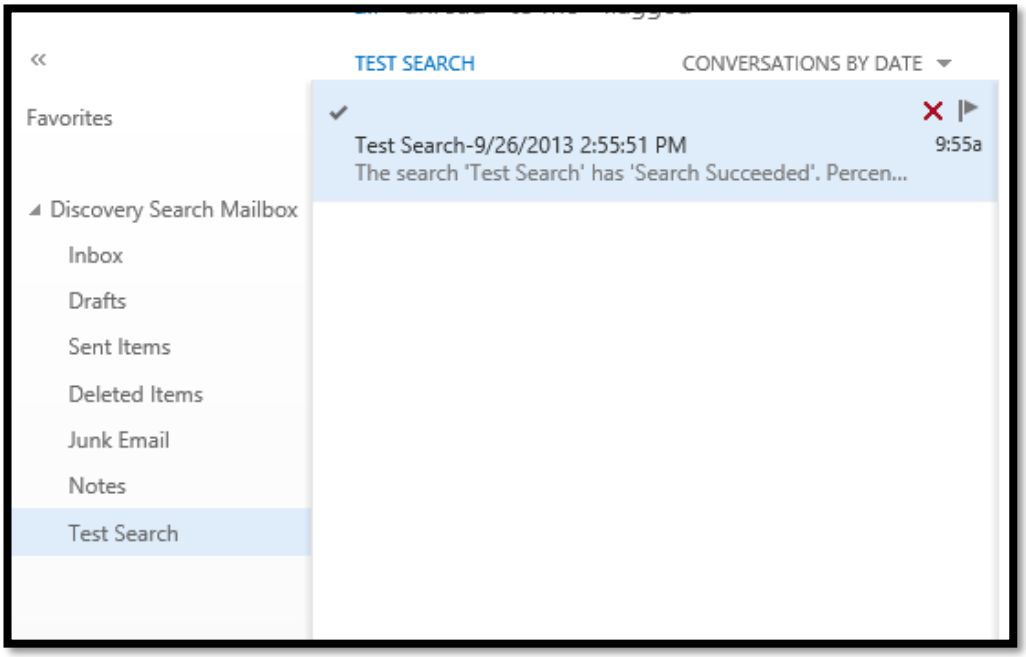
*Only the **searchadmin** account has access to view the contents of a discovery mailbox. If you need to send the results to another user, use the **"download pst"** option explained later in this section, or use PowerShell to write the results to a normal mailbox that can then be permissioned for viewing.*

Choosing to copy the results will allow you to put the results into a discovery mailbox later viewing. You need to make sure that you select the proper discovery mailbox for your district. The format will be ***SearchResultsMailbox@district.kyschools.us***. Make sure ***not*** to check ***"Include unsearchable items"***. This will put all items that could not be searched into the results. You can also specify if you would like to be notified when the search completes.

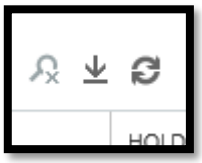
When the search completes you can look at the results by opening the discovery mailbox that contains the results from the search job properties menu. Click on the ***"Open"*** link to view.



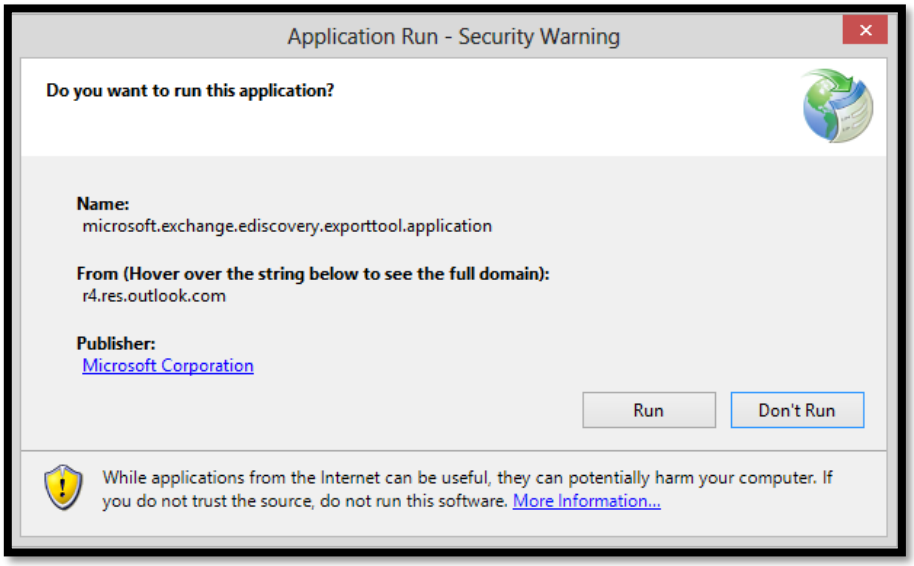
This will open the mailbox in OWA and you should see your search to the left in the folders list.

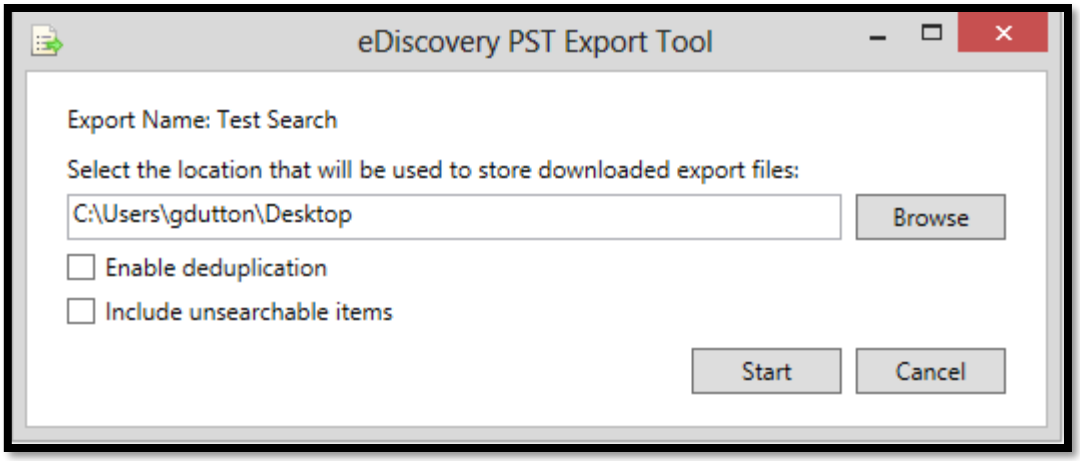


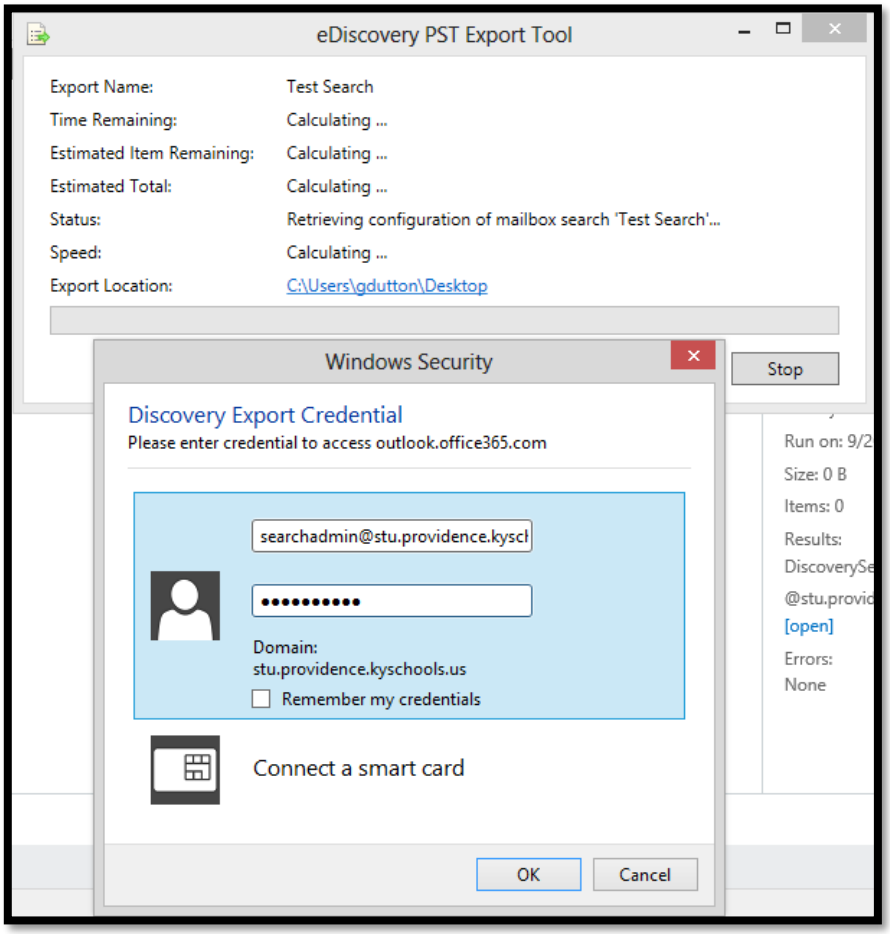
You may also download a PST of the results using the down arrow at the top of the eDiscovery page.

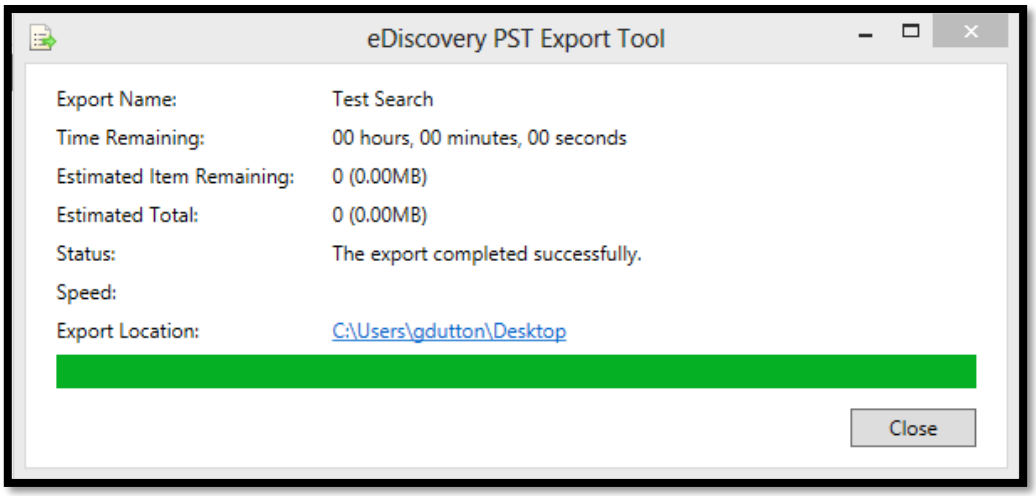


This will download an application that will allow you to get the PST file version of your search results. You will be prompted for credentials to verify you can run the search. You should use your district's ***searchadmin*** credentials here.


Application Run - Security Warning
Do you want to run this application?
Name:
microsoft.exchange.ediscovery.exporttool.application
From (Hover over the string below to see the full domain):
r4.res.outlook.com
Publisher:
Microsoft Corporation
Run
Don't Run
While applications from the Internet can be useful, they can potentially harm your computer. If you do not trust the source, do not run this software. More Information...


eDiscovery PST Export Tool
Export Name: Test Search
Select the location that will be used to store downloaded export files:
C:\Users\gdutton\Desktop
Browse
Enable deduplication
Include unsearchable items
Start
Cancel


eDiscovery PST Export Tool
Export Name: Test Search
Time Remaining: Calculating ...
Estimated Item Remaining: Calculating ...
Estimated Total: Calculating ...
Status: Retrieving configuration of mailbox search 'Test Search'...
Speed: Calculating ...
Export Location: C:\Users\gdutton\Desktop
Stop
Windows Security
Discovery Export Credential
Please enter credential to access outlook.office365.com
searchadmin@stu.providence.kyscl
Domain:
stu.providence.kyschools.us
Remember my credentials
Connect a smart card
OK
Cancel
Run on: 9/2
Size: 0 B
Items: 0
Results:
DiscoverySe
@stu.provid
[open]
Errors:
None


eDiscovery PST Export Tool
Export Name: Test Search
Time Remaining: 00 hours, 00 minutes, 00 seconds
Estimated Item Remaining: 0 (0.00MB)
Estimated Total: 0 (0.00MB)
Status: The export completed successfully.
Speed:
Export Location: C:\Users\gdutton\Desktop
Close

- **In Place eDiscovery**
  - http://technet.microsoft.com/en-us/library/dd298021(v=exchg.150).aspx

5 Skype for Business Online

Skype for Business Online is the instant messaging/web conferencing solution implemented in O365. Currently users will receive a Skype for Business Online account when they are provisioned with OLPS. By default the ***"Edu Plan"*** will be populated with the value ***"default"*** which will create the necessary Skype for Business Online account in addition to an Exchange Online account. At the moment there are few administrative tasks to be completed with Skype for Business Online. PowerShell to Skype for Business Online is also not supported at present.

5.1 Skype for Business Online Client Installer

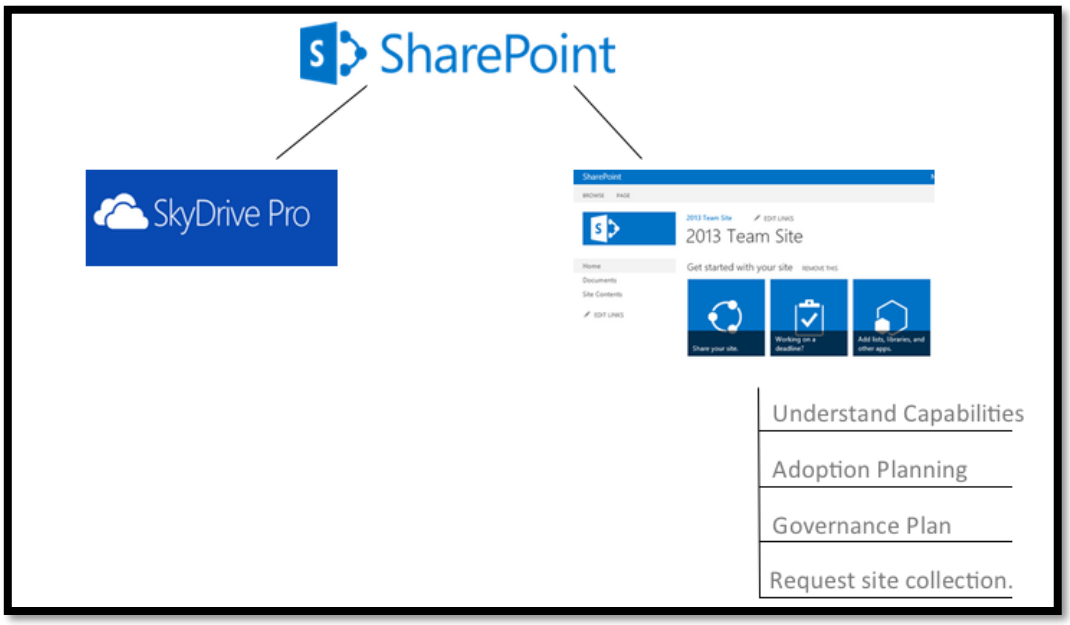
The full Skype for Business Online client can be downloaded from the ***"Software"*** section of the ***"O365 Settings"*** section in O36: https://portal.office.com/OLS/MySoftware.aspx .

Once you have downloaded the installer, run the program and follow the instructions to complete the Skype for Business client installation.

For more end user information regarding Skype for Business Online and its use please refer to the following documentation: Skype for Business Online Information

6 SharePoint Online

Both OneDrive for Business and Team Sites (SharePoint Online) are based on the Microsoft SharePoint 2013 platform. If you do not plan to use SharePoint Team Sites, you may skip this section, as governance strategies are not applicable to OneDrive for Business.



If you are considering deploying SharePoint Online Team Sites, you should first understand the capabilities of the platform and then plan for user adoption and create a governance plan. To prepare for deploying SharePoint Online please review these resources from Microsoft. Though some of these are created for SharePoint 2010, the general concepts are applicable to current and future versions of SharePoint Online (2013 and beyond).

Understanding the SharePoint platform and its capabilities

- SharePoint in Plain English

Planning for user adoption and creating a governance plan

- SharePoint Adoption Guide

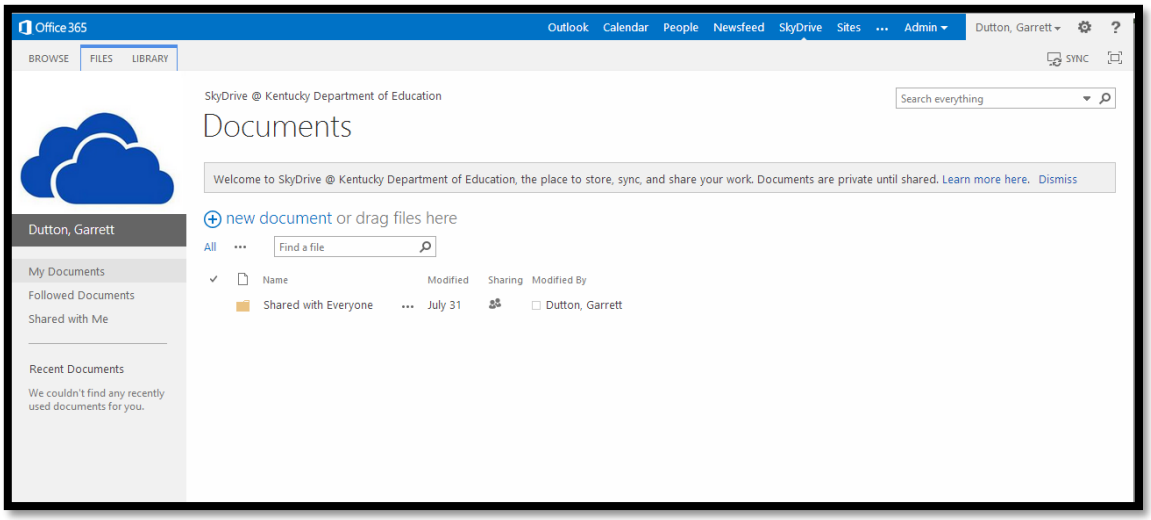
After you've reviewed these resources, a SharePoint Online site collection may be created for your district by contacting the KETS Service Desk.

6.1 OneDrive for Business

OneDrive for Business is the user based document storage solution available in O365 SharePoint Online. This service replaces the standard consumer SkyDrive service that users may currently have. User will get 25GB of storage space and can sync with a desktop folder for easy access and editing via the OneDrive for Business desktop application.

ONEDRIVE FOR BUSINESS SYNC APPLICATION INSTALLER

More information on OneDrive for Business and its functionality can be found at the following link: What is OneDrive for Business?

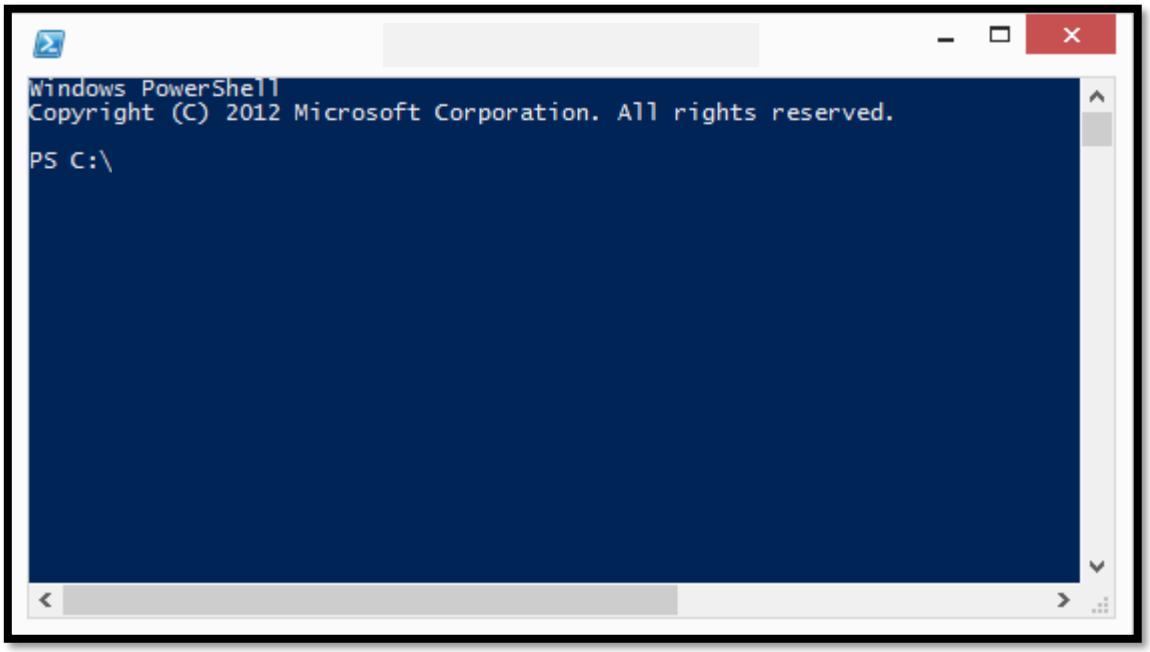


7 PowerShell

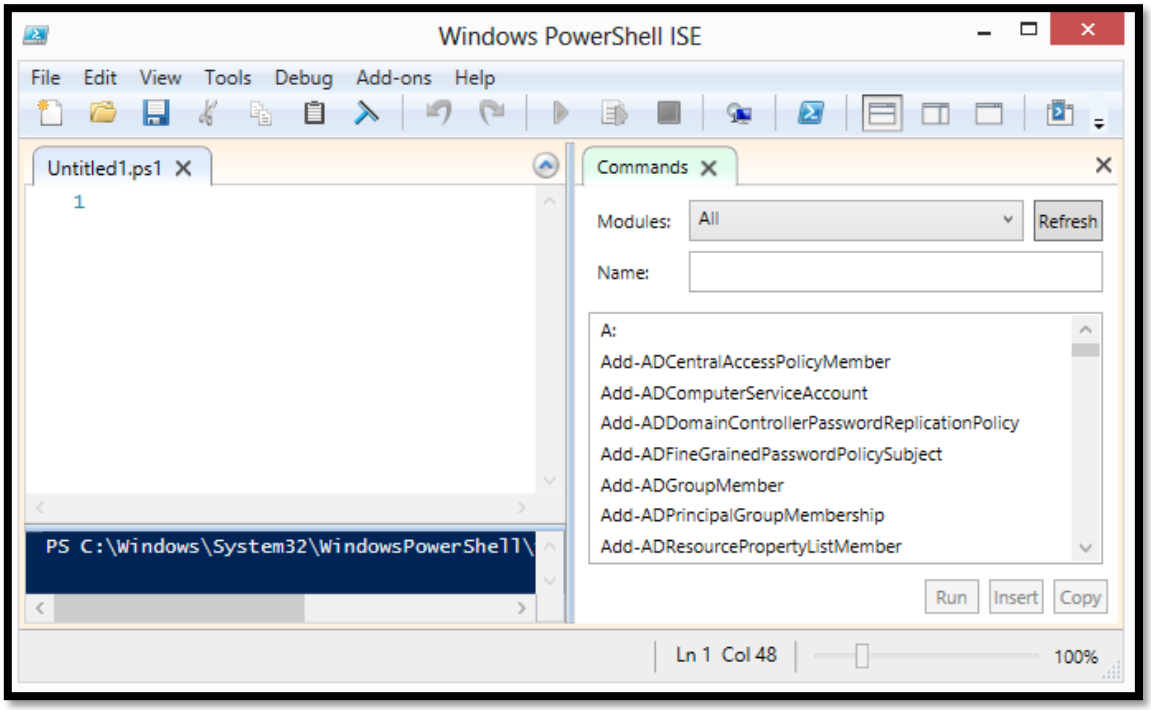
Windows PowerShell is a task-based command-line shell and scripting language designed especially for system administration. Built on the .NET Framework, Windows PowerShell helps IT professionals and power users control and automate the administration of the Windows operating system and applications that run on Windows. Any commands that were run via the Windows Command Prompt that administrators are used to can also be executed in PowerShell. Scripts can also be written using the PowerShell ISE. The vast majority of tasks in O365 can be achieved by using various other management applications (ADUC, EAC, and KCP). However, some tasks relating to O365 must be performed with PowerShell and in some cases batch type jobs can most efficiently be completed using PowerShell.

PowerShell is preinstalled in Windows Vista, 7, and 8 but may need to be installed or upgraded on administrative machines. You can get the latest version of the Windows Management Framework which includes PowerShell at the following link:
Windows Management Framework

POWERSHELL COMMAND PROMPT



POWERSHELL ISE



In order to run PowerShell scripts on a machine you must first set the execution policy of the machine. To allow all PowerShell scripts to run, regardless of origin, you must set the execution policy to ***"unrestricted"*** as shown below.

SET EXECUTION POLICY

You will need to launch PowerShell as an administrator to perform this operation.

```
PS C:\> Set-ExecutionPolicy -ExecutionPolicy unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust.
Changing the execution policy might expose you to the security risks
described in the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the
execution policy?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
PS C:\> _
```

You can learn more about PowerShell at the link below:

Learn about Windows PowerShell

7.1 PowerShell in Exchange Online

Using PowerShell against Exchange Online in O365 is fundamentally unchanged from the previous implementations of Microsoft hosted email services used by KETS. This is because under the hood they are the same technologies. Exchange Online has some unique aspects to it as opposed to Exchange on premises, but for the most part PowerShell functionality is still intact to the degree districts are accustomed to having control over.

Most remote tasks performed with PowerShell in ExO will require elevated permissions. This means that depending on what a district needs to do they will most likely have to make use of the privileged accounts assigned to them in order to execute remote PowerShell commands. A listing and description of these accounts are in the following section.

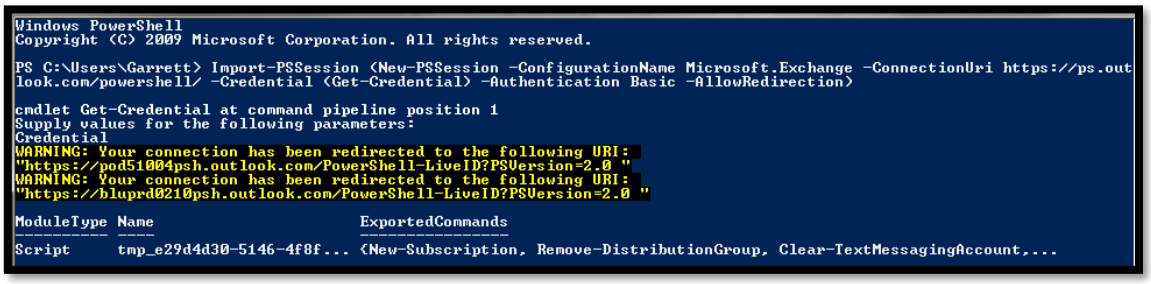
For more information about PowerShell in Exchange Online see the following link:

PowerShell in ExO

7.1.1 Connecting to Exchange Online

After installing the Windows Management Framework you can open the shell and begin. You must first start by connecting to Exchange Online for your accepted domain. You must **proceed with caution** as there can be irreversible effects from running cmdlets without complete understanding of what you're doing. You can create a connection with the command below:

```
Import-PSSession (New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://outlook.office365.com/powershell/ -Credential (Get-Credential) -
Authentication Basic -AllowRedirection)
```



You should now be connected to Exchange Online for your environment and able to run Exchange specific cmdlets against it. Once you are finished running your commands **MAKE SURE** to disconnect. There are a finite number of concurrent connections available for remote PowerShell and if they are all used you must wait for the timeout period to expire before making a new connection. You can disconnect all open Exchange Online connections with the command below:

```
Remove-PSSession (Get-PSSession | Where-Object {$_.ConfigurationName -eq
"Microsoft.Exchange"})
```

7.1.2 Retrieving Mailbox Information

*The " **| fl** " is short for **"formatted list"** and adding it at the end of your command means that you would like the information returned in a list so you can see all attributes and their properties.*

To retrieve information about a specific user mailbox you can use the ***Get-Mailbox*** cmdlet.

Example:

```
Get-Mailbox John.Smith@district.kyschools.us | fl
```

By just running the ***Get-Mailbox*** cmdlet without any parameters, you will return all mailboxes in your accepted domain. You can also use a wildcard to search for mailboxes that match a pattern:

Example:

```
Get-Mailbox *smith*
```

The above command would return all mailboxes in the accepted domain that contain the word ***"smith"*** in the SMTP address.

7.1.3 Retrieving Distribution Group Information

You can retrieve distribution group information in much the same way that you retrieve mailbox information. The difference is that you would use the ***Get-DistributionGroup*** cmdlet.

Example:

```
Get-DistributionGroup DistrictSouthernHighTeachers@district.kyschools.us | fl
```

7.1.4 Adding Proxy Email Address

The following code can be used to create a secondary SMTP address for a given user. This is useful if a particular user also needs to have a generic address that mail can be sent to. For example a high school principal could have the secondary address: **NorthHighPrincipal@district.kyschools.us** .

```
Set-Mailbox first.last@district.kyschools.us -EmailAddresses

@{add="secondarysmtpaddress@district.kyschools.us"}
```

Replace ***first.last@district.kyschools.us*** with the MSOID of the user that needs the secondary address added and replace ***secondarysmtpaddress@district.kyschools.us*** with the name of the email address you would like to add to the user.

7.1.5 Grant Mailbox Permission to Other Users

This functionality replaces the "Open Mailbox" feature that was in the previous KETS Control Panel.

There are some cases in which districts may need to open the mailbox of a specific user. You can use PowerShell to grant mailbox access to any user you specify. This useful if more than one person needs to operate within a shared mailbox, or if more than one person needs to use the same mailbox for administrative purposes. The following command will add permissions to John Smith's mailbox for access by Janet Smith.

Note that this example grants FULL access. Which means the user you grant access to can do anything the normal user can inside their account.

```
Add-MailboxPermission -Identity John.Smith@district.kyschools.us -User
Janet.Smith@district.kyschools.us -AccessRights fullaccess –Automapping $false
```

When you want to remove the permissions you have granted the command is exactly the same, except you use the **`Remove-MailboxPermission`** cmdlet instead. The following command will remove the permissions assigned in the previous **`Add-MailboxPermission`** command.

```
Remove-MailboxPermission -Identity John.Smith@district.kyschools.us -User
Janet.Smith@district.kyschools.us -AccessRights fullaccess
```

7.1.6 Mailbox Searches in PowerShell

The Exchange Online administrators can perform searches against a single mailbox or perform multi-mailbox searches. This is utilized to find email or calendar events that match a certain set of criteria and export the results to a specified mailbox. Best practice for running PowerShell mailbox searches is that you create a search results service account mailbox to store the results in.

Searching mailboxes in Exchange Online via PowerShell is done through a cmdlet named ***New-MailboxSearch.*** This cmdlet will search across a DL or single/multiple specified user accounts. Below is an example of a new search using the ***New-MailboxSearch*** cmdlet:

```
New-MailboxSearch -Name “MyNewSearch” -SearchQuery “Test” -LogLevel Basic -
SourceMailboxes “districtmathteachers@district.kyschools.us” -TargetMailbox
serviceaccount@district.kyschools.us
```

The above command creates a new search named ***“MyNewSearch”*** and will search all the mailboxes in the DL with the email address ***districtmathteachers@distrit.kyschools.us*** for the word “test” anywhere in email messages, contacts, or calendar events and export the results to the ***serviceaccount@district.kyschools.us*** mailbox. More information on New-MailboxSearch can be found here. Once a search object is created via ***New-MailboxSearch*** you will then have to execute the search by name with ***Start-MailboxSearch*** as shown below:

```
Start-MailboxSearch -Identity “MyNewSearch”
```

You can also query as to the status of your search at any time by running ***Get-MailboxSearch*** and using the name of your search:

```
Get-MailboxSearch -Identity “MyNewSearch”
```

For more information about this cmdlet and AQS syntax see the links below:

New-MailboxSearch Help
AQS Syntax Help

7.1.7 Create Contacts

Mail contacts can be created in Active Directory if desired, but they can also be created directly in Exchange Online PowerShell. You can use the command below to create contacts.

To create a mail contact use the following example:

```
New-MailContact -Name "Smith, Bob – CompanyA” -ExternalEmailAddress
bob.smith@companya.com
```

7.1.8 Create Dynamic Distribution Group

For example, the following will create a DDG named “District Staff” with SMTP address diststaff@district.kyschools.us that only includes members with CustomAttribute1 set to “000”.

```
New-DynamicDistributionGroup –Name “District Staff” –PrimarySmtpAddress
diststaff@district.kyschools.us –RecipientFilter {customattribute1 –eq “000”}
```

Pay close attention to the query for DDGs. You will most likely want a combination of attribute values to get the desired list. The example above would create a list of users that included staff and students because it is simply all users that have the district attribute set to 000 and all users in the state are in the same tenant. If you wanted a list that was only the staff accounts you would need a query that looked like the following:

```
–RecipientFilter {(customattribute1 –eq “000”) –and (customattribute4 –eq “staff”)}
```

For a full list of the attributes that can be used to query on you can run the ***“Get-Recipient”*** cmdlet on a specific mailbox:

```
Get-Recipient first.last@district.kyschools.us | fl
```

Learn more about managing DDGs at the following link:
Exchange Dynamic Distribution Groups