Text

Description automatically generated with medium confidence

District Readiness Guide and Activities

*KETS Security Baseline   
  
Microsoft 365 EMS A3 Deployment*

Prepared for: KY School Districts and KDE

Prepared by: Microsoft & the Office of Education Technology

**7/15/2022  
Version 1.0**

**Any questions about any content in this guide should be directed to your KETS Engineer** (not the KETS Service Desk).  
  
**Overview**

This project is focused on improving security in the KETS environment, specifically targeted at the KETS Identity and Directory Standard systems (which are Active Directory and Azure Active Directory (M365). The KETS Security Baseline project will assist districts in implementing the required licenses (purchased by KDE) and security measures to bring all school districts and KDE to a baseline security posture utilizing Microsoft 365’s EMS A3 suite of security products. Some districts have already purchased licenses that cover this suite of tools and possibly have already implemented these measures. This project is geared to bring everyone to the following baseline:

***Self-Service Password Reset (SSPR) in M365 with writeback to Active Directory***

***Multi-Factor Authentication (MFA)***

***Conditional Access Policies  
Password Expiration Notification***

***Advanced Security Reporting and Alerts***

***KETS Adult Password Minimum Requirements (Reminder)***

The following is a brief description of each of these five baseline technologies.  
  
***Self-Service Password Reset (SSPR) in O365 with writeback to Active Directory***

This gives users the ability to reset their KETS password even if they have forgotten it. Coupled with the Password Notification Script even users that do not log in to Active Directory will get notified to change their password. This will by default change a user’s password in Office 365 and also write the password back to Active Directory. For those districts that utilize G Suite Password Sync (GSPS), this password change will also sync to your district’s Google Workspace for Education.

***Multi-Factor Authentication (MFA)***

MFA will work directly with KETS accounts and anything configured to use Office 365 for login. The Microsoft Office apps are included such as Outlook, Teams, Excel, Word, and PowerPoint. MFA will also work with anything connected via Single-Sign-on to Office 365 (ex. Google configured to SSO to O365). Also included in the Single-Sign-On are KDE’s Web Apps, thanks to a recent project that was completed in 2021. Infinity Campus will also force MFA on login as it is configured for SSO to Office 365. There is a project underway to also have MUNIS configured for all districts as well.

This MFA will not work with applications that aren’t connected to our KETS accounts via SSO. If it isn’t Microsoft, Google or SSO, it won’t work with our MFA. Some apps that don’t currently work maybe can be made to work if the vendor supports them.

***Conditional Access Policies***

Conditional Access policies at their simplest are if-then statements. If a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to do multi-factor authentication to access it. Use Conditional Access policies to apply the right access controls when needed to keep your organization secure.

***Password Expiration Notification***

The process provided and supported by OET will inform users by email that they need to change their password and where to do so, whether they log in to Active Directory or not. This looks in Active Directory to see when a user’s configured password policy will enforce a change. This can be applied to staff and/or students.

***KETS Adult Password Minimum Requirements (Reminder)***

All staff will be configured to have at a minimum the following password policy. This minimum policy config can be set by adding users to a group in AD (\_District Admins > *Users and Groups*) with the name of ***DIST Password Policy – KY K12 Staff Minimum Fifteen 180***. The new policy reflects the statewide staff password minimums. While no district is required to use this specific security group, every district staff member account must meet or exceed the password requirements described by this PSO. If a district wants to use a different password policy for their staff, they can request one to be created or an existing one be edited by contacting the KETS Service Desk. The new password policy must be more restrictive than the new minimum requirements (below).

**WARNING:** When moving staff users into the new PSO, be aware that if the user hasn’t changed their password in the last 180 days (the new password expiration minimum), their account will immediately be set to “expired.” This will prompt a

password change. Keep this in mind when moving a large number of staff users into the new password policy group, a sudden change in the password for a large group could stress support resources in your district. Moving folks in small groups may be helpful.

For further questions or concerns regarding these changes, please contact the *KETS Service Desk*.

The statewide staff MINIMUM password requirements are:

* Minimum Password Length – 15 characters minimum (use an easy-to-remember passphrase)
* Complexity - Set to false. ***(Complexity can be enabled if desired. Contact the KETS Service for any change requests)***
* Password Expirations – Every 180 days or less; immediately after a suspected data breach or compromised account
* Lockout Threshold – 10 attempts or fewer
* Lockout Duration – 10 minutes or more
* Minimum Password Age – 3 days or more
* Password History Count – Previous 12 passwords

More information regarding KETS password policies can be found in section 3.1.5 of the KETS AD Operations Guide: <https://education.ky.gov/districts/tech/Pages/Administration-and-Install-Guides.aspx>

**Project Timeline**

Planning and behind-the-scenes work have taken place at KDE with Microsoft in preparation for this implementation. This project is focused on Phases I and II. There will be future communications going through the actual implementation of district users. These first two phases are designed to get the environment technically configured to prepare for the implantation as well as prepare the district technical staff and leadership for the ‘why’, ‘what’, and ‘how’. Phase III will be the ‘when’, which will be discussed below. The following is a high level of the phases of implementation:

***PHASE I – Priming Environment   
 PHASE II – Workshop and Admin Enablement  
 PHASE III – Staff Implementation***

The following is a brief description of each of these five baseline technologies.

***PHASE I – Priming Environment***

The Project team configuring the environment to allow for future implementation of the project features (SSPR, MFA, etc). This includes security groups in AD to license EMS A3 as well as implement features like MFA methods for users. There will be pre-configured ‘baseline’ Conditional Access Policies the district can use as well.

***PHASE II – Workshop and Admin Enablement***

You will be scheduling a workshop with Microsoft, which is the foundation for this project.  During the workshop session Microsoft staff will actively guide you through each function of the security baseline project, along with step-by-step instructions to set up each feature in your own tenant.

Workshop Agenda

* What is changing?
  + Details of the Security Baseline changes (SSPR, MFA, CA)
* What is my role?
  + What is KDE role
  + What is the District IT Pro responsible for
  + What is Microsoft responsible for
* How do I enable the changes for my district?
  + Details of how the District IT Pro enables the change for their District
  + A suggested approach for enabling the change
* How do I support the change?
  + Incident Management process for Security Baseline changes
  + Troubleshooting in AAD (Demo)
    - Diagnose and solve problems
    - Audit Logs
    - Usage & Insights
  + How to get support from Microsoft if the District IT Pro cannot solve the issue (Demo)
  + Where can I find support information and what is available (Demo of Organization Repository)
* How do I proactively monitor the change?
  + Admin Portal Service Health (Demo)
  + Admin Portal Service Health/Message Center (Demo)
  + Microsoft 365 Defender (Demo and Interactive Demo)
  + Investigating Suspicious Activity by a User

***PHASE III – Staff Implementation***

Ultimately the purpose of this initiative is to increase the security posture of the environment with an expectation that all staff, including both privileged and service accounts, will have these baseline setting deployed within 6 months of Phase II (workshop date). You can certainly choose to implement as soon as you desire after your workshop as it’s highly recommended to do so while the knowledge transfer of the enablement processes are fresh on the mind. A solid communications plan to leadership and users will result in a successful rollout of these features, which is what Microsoft in their sessions are focused on.

**TASKS**

**Prior to PHASE II *(Workshop and Admin Enablement)***

☐ **ACTION ITEM – Identify Office 365 Global Admin Account credentials**

* Identify Global Admin account and password in Office 365 as they will be needed for some of the tasks outlined.

☐ **ACTION ITEM – Identify technical staff to attend Workshop**

☐ **ACTION ITEM – Identify Privileged Accounts to receive MFA for test** *(configured during Workshop)*

* Identity accounts in Office 365 that have elevated access for initial tests. You will be enabling MFA the day of your Microsoft workshop with the purpose of testing the configuration as well as preparing you for what users will experience in Phase III.

☐ **ACTION ITEM – Share overview of what’s coming with Superintendent**

* Share overview of what’s coming with this project with district leadership (ex SSPR, MFA for all staff, etc).

A good diagram of why the world is moving to MFA:  
<https://techcommunity.microsoft.com/t5/azure-active-directory-identity/flash-whitepaper-why-mfa-is-a-top-priority-in-2020/ba-p/1194467>

☐ **ACTION ITEM – Review existing MFA configurations and/or Conditional Access policies (if applicable)**

* If you currently have implemented MFA for users please bring this information with you to the workshop as well as any Conditional Access Policies your district has configured. Please be prepared to talk about what they do to the workshop. The purpose of this step is to ensure the new configurations don’t negatively conflict with any your district is currently using.

☐ **ACTION ITEM – Identify any users that will login outside the US**

* The day of your workshop there will be a policy set to block all non-US logins. Anyone in your district that will be logging in outside the US will need to be added to an exceptions group.

☐ **ACTION ITEM – Decide on Password Expiration Notification for your district**

Determine whether your district wants to implement the Password Expiration Notification service. This will send an email to users letting them know that their password will be expiring soon and what measures they should take to change it. This will be configured to only work for users that are in the M365-SSPRUsers security group in the ‘Staff’ OU in AD. This group along with others (in Appendix below) will be discussed during your workshop.   
  
If you wish to have your district utilize this service please send an email :

To: [Patrick.wofford@education.ky.gov](mailto:Patrick.wofford@education.ky.gov) (and your KETS Engineer)  
Title of email: **Opt-in to Password Expiration Notification service**

body of email:

**District name -**

**Who to contact if there are issues or questions -**  
*\* this is used in the body of the email that will go to users. This could be your district help desk email, a tech contact, etc*

☐ **Informational – Validate ‘Priming’ objects**

We will be creating AD groups as well as objects in your Office 365 environment (MFA settings, Conditional Access Policies, Groups, etc). **PLEASE do not modify these objects**. A complete list can be found in the Appendix. These objects should be present 3 days prior to your workshop date. Please validate these groups and other objects are in fact created. If any are missing please send an email to your KETS Engineer and the project PM, [patrick.wofford@education.ky.gov](mailto:patrick.wofford@education.ky.gov)

**Phase II – Workshop and Admin Enablement   
*\* these items will occur the day of your district’s schedule workshop.***

☐ **Informational – Assign Licenses to Admins**

* With Microsoft’s assistance you will be assigning the EMS A3 license for Staff

☐ **Informational – Assign Admin Users to Enroll SSPR/MFA**

* Apply SSPR and MFA to the test group (walk through by Microsoft during the workshop)

☐ **Informational – Block non-US logins for all users**

* The day of your workshop Office 365 will be configured to block non-US logins for all users. There is an Action Item prior to Phase II for you to identify any users that will need to login outside of the US to add them as an exception to this rule.

☐ **Informational – District can opt-in to Password Expiration Notification process**

* After your workshop you can open a Service Desk ticket to implement the Password Notification process that will email users on when their AD password will need to be changed. This can be done for staff and/or students.

☐ **Informational – Risk Assessment Alerts**

* Messages will be configured to alert you when there is significant concern of potential breaches, etc.

**Appendix**

**Configuration objects created in to ‘Prime’ the environment**

**Groups**

|  |  |  |
| --- | --- | --- |
| **Group Name** | **Source** | **Purpose** |
| Cloud-M365-EMSA3 | Azure AD | Assigns the EMS A3 license (includes the Cloud MFA and Cloud SSPR groups as members) |
| Cloud-M365-MFAUsers | Azure AD | Used for Conditional Access policy scoping |
| Cloud-M365-SSPRUsers | Azure AD | Used for Self Service Password Reset policy scoping |
| Cloud-M365-GeoLocationExclusion | Azure AD | Used for the Block Non US Logins Conditional Access policy |
| M365-GeoLocationExclusion | On-premises AD | Excludes users from the Conditional Access policy that blocks access from outside of the USA |
| M365-MFAUsers | On-premises AD | Enables users for MFA |
| M365-SSPRUsers | On-premises AD | Enables users for Self Service Password Reset |

**Named Locations**

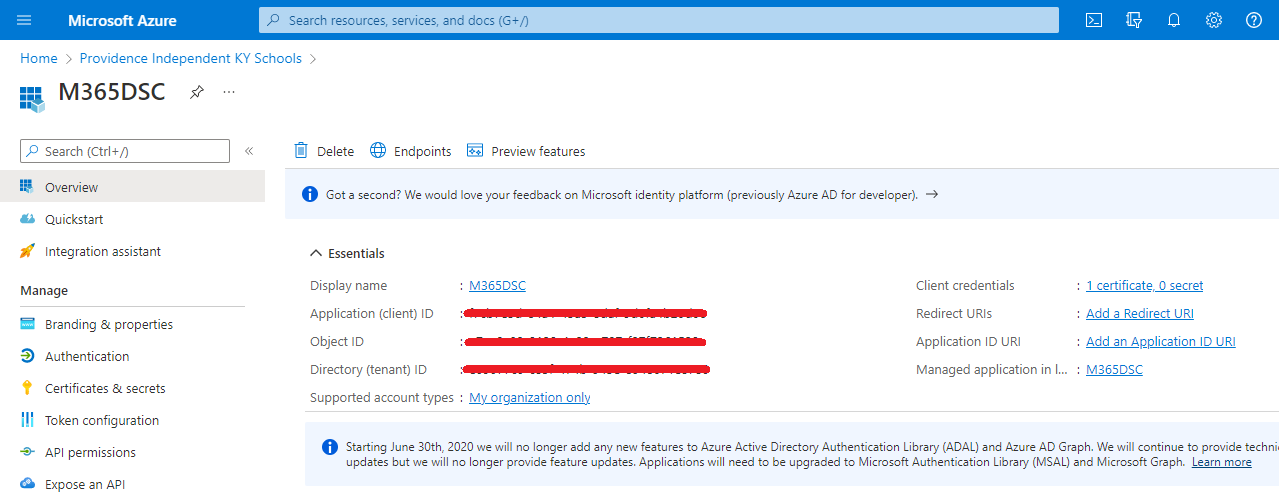
|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Trusted?** | **Comment** |
| In-District IP Ranges | IP ranges | Yes | Contains the external IP range(s) of the district |
| Non-US Locations | Countries (IP) | N/A | Contains all country objects available in AAD (including unknown locations) except for the United States |
| Restricted IPs | IP ranges | No | Contains a list of IPv4 ranges |
| United States | Countries (IP) | N/A | Contains the United States object |
| US-Based IPv6 Ranges | IP ranges | No | Contains a list of US based IPv6 ranges |

**Conditional Access Policies**

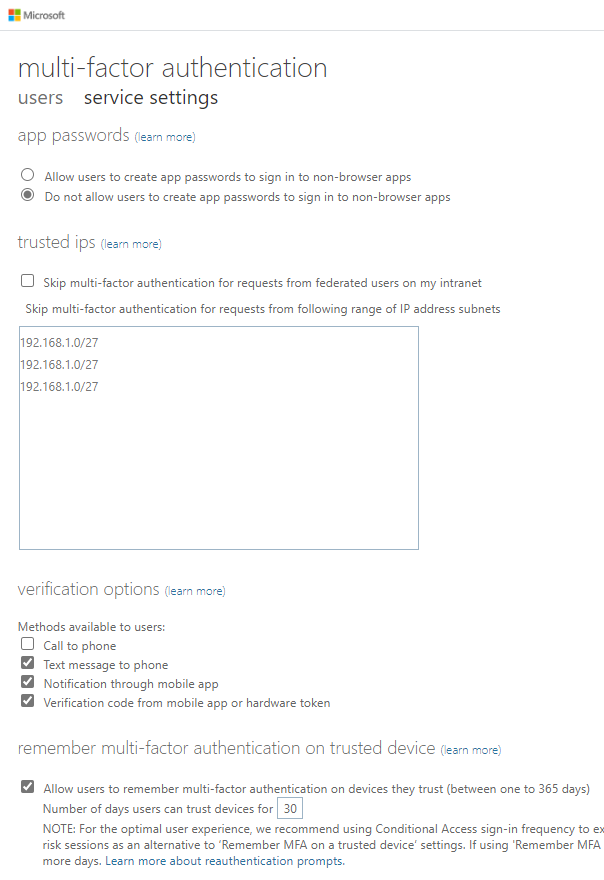
| **Policy Description** | **Assignment | Users and Groups** | **Asgnmnt Cloud Apps** | **Assignment Condition | Device Platforms** | **Assignment | Condition | Locations** | **Access Control** |
| --- | --- | --- | --- | --- | --- |
| Baseline Policy: [KDE-CA001: Require MFA - Admins](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Factive-directory%2Fconditional-access%2Fbaseline-protection&data=05%7C01%7CJohn.Logan%40education.ky.gov%7Cf6c0d8517cc442fede7508da4dfeb51e%7C9360c11f90e64706ad0025fcdc9e2ed1%7C0%7C0%7C637908053636464852%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=O%2FuHKjGKlnQa97JjlTEdspn2X95Paf4JG4fltqt4BtQ%3D&reserved=0) | Users with AAD Admin roles  **Exclude:** KETS Administrator | All Cloud Apps | Not Configured | Not Configured | Grant Access: Require MFA |
| KDE-CA004: Require MFA\*\* | Cloud-M365-MFAUsers  **Exclude:** KETS Administrator | All Cloud Apps | Not Configured | Any Locations (Exclude In-District IP Ranges) | Grant Access: Require MFA |
| KDE-CA200: Block Non-US Logins | All Users  **Exclude:** Cloud-M365-GeoLocationExclusion | All Cloud Apps | Not Configured | Any Locations (Exclude In-District IP Ranges, MFA Trusted Ips, United States and US-Based ipv6 Ranges) | Block Access |
| KDE-CA201: Block All Access for Specific IP Address | All Users  **Exclude:** KETS Administrator | All Cloud Apps | Not Configured | Restricted IPs | Block Access |
| KDE-CA006: Require MFA for Azure management | All Users  **Exclude:** KETS Administrator | Microsoft Azure Management | Not Configured | Not Configured | Grant Access: Require MFA |

**Service Principal**

Used by the M365DSC service to connect to the district tenant. No action is required by the district and the service principal should NOT be modified in any way.

****

**Azure MFA Service Settings**

****

**Self Service Password Reset Settings**

**Graphical user interface, text, application, email

Description automatically generated**

**Link to other important artifacts such as ACM Plan, Operations Guide, etc.**

<https://staffkyschools.sharepoint.com/sites/KETSDocumentation/SecurityBaseline>

If there are any questions please send an email to your **KETS Engineer and the project PM,** [**patrick.wofford@education.ky.gov**](mailto:patrick.wofford@education.ky.gov)