



Kentucky Department of  
**EDUCATION**

**Enterprise ERP (EERP/MUNIS) CLOUD SYSTEM DISTRICT  
OPERATIONS GUIDE**

Office of Education Technology: Division of School Technology Services

Questions: [EERP@education.ky.gov](mailto:EERP@education.ky.gov)

**8/1/2024**

## **Table of Contents**

Note .....	2
Introduction .....	3
Update History .....	3
Overview of Environment .....	4
User Interface .....	4
Network .....	4
District Network Configuration .....	5
VPN Device.....	5
Network Configuration.....	5
Workstation Configuration.....	5
Additional System Requirement Information:.....	7
Application Customization .....	7
Alternate Access .....	7
Support Contacts .....	7
Enterprise ERP User Accounts.....	9
Overview .....	9
Multi-Factor Authentication (MFA).....	9
Conditional Access Policies .....	10
User Accounts – Tyler Datacenter Accounts .....	10
Security Considerations .....	11
Digital Document Archiving.....	12
Tyler Reference Documents.....	12

## **Note**

This document contains information specific to v2021.x and 2024.x. Tyler changed the version name/numbering from v2021 to v2024 to reflect the year of the release more accurately.

In 2022 Tyler Technologies updated the name of their products to represent their function. Munis has been renamed Enterprise ERP (EERP) and both names will be used interchangeably.

## Introduction

This document describes the operations districts must complete to maintain the Enterprise ERP (EERP) Cloud System, and the avenues available to access Tyler and KDE support. It is directed at technology staff who must support district EERP users. This document is a supplement to Tyler-provided documentation and focuses on the integration of the EERP Cloud System into the KETS environment.

## Update History

7 February 2013 – Initial Release

17 July 2013 – Updated proxy exception information due to Tyler datacenter changes

20 August 2013 – Updated proxy exception information (within browser only) related to Tyler datacenter changes

21 August 2013 – Corrected proxy exception list entry notation

12 March 2014 – Updated proxy exception information due to move of cloudadmin.tylertech.com site to non-VPN IP range; updated workstation requirements

14 August 2014 – Updated emergency contact list

16 Sep 2014 – Added information about optional products and modules

23 January 2015 – Updated browser and network configuration sections in preparation for MUNIS 10.5

6 February 2015 – Updated browser and network configuration sections with corrections and a clearer layout

21 May 2015 – Updated workstation and browser system requirements

11 June 2015 – Added note re Compatibility View for Internet Explorer 11

11 August 2015 – Updated browser and network configuration sections with specific guidance for Lightspeed

28 August 2015 – Added IP range 207.182.208.0/24 to exceptions lists

21 April 2016 – For MUNIS 11.2: change to IE versions supported; reversal in I.E. Compatibility View settings; removal of ActiveX client installation; no specific .Net Framework requirement; newer Silverlight required; addition of Chrome and Safari as supported browsers

12 January 2017 – Update support contacts including a new number for emergency issues outside of normal business hours

23 May 2017 – Update Security Considerations to address the security of files on MUNIS workstations

6 June 2018 - Updated browser and network configuration sections. Update support contacts.

3 June 2019 – Removed references to prior versions of Munis.

1 June 2020 – Added references to v2019.1 V12. Removed individual contact information.

4 June 2021 – Spelling and grammar corrections.

9 September 2022 – Removed references to specific IP filtering.

8 September 2023 – Added references to v2021.x, user accounts, and Tyler Hub.

1 August 2024 – Removed references to v2019. Changed Azure AD product name to Entra ID. Added information on required user attributes in Microsoft Entra ID. Additional security considerations added.

## **Overview of Environment**

### ***User Interface***

Tyler Hub is the primary user interface with each instance of EERP (Live/Train/Test) having a unique URL (example: <https://boeky.tylerhub.com/>). EERP is web-based and designed to be accessible to both financial staff and administrative staff at districts and schools (program directors, principals, etc.).

### ***Network***

Tyler provides a Virtual Private Network (VPN) device to encrypt network traffic for the Core applications between the district network and the EERP Cloud system. This device is located in the district's KEN rack and will be supported by Tyler, though if a device must be replaced or moved district staff will be asked to complete the physical disconnections and connections.

Tyler also provides a browser-based SSL VPN utility that can be used to securely access the Core applications of the EERP Cloud system from remote locations.

In addition to the EERP Core applications, Tyler offers an EERP Self-Service web application, which provides a convenient interface for employees to check pay statements, make vacation requests, etc. This web application's network traffic travels over the same pathways as other web traffic and does not utilize the Tyler VPN device.

*Note:* Tyler offers several additional products and modules that districts may acquire in addition to the core EERP system. These products and modules may have their own network and system requirements in addition to those described in this document. If you are using any of these products or modules, please contact Tyler Support or search the Tyler support site for information about additional technical requirements.

# District Network Configuration

## VPN Device

A Tyler-provided VPN device is installed on a shelf in each district’s KEN rack. Tyler is responsible for monitoring, configuring, and troubleshooting this device.

If this device fails and must be replaced, Tyler will configure and ship a replacement device to the District CIO. A member of the district’s technology staff will be asked to physically swap the devices and ship the failed device back to Tyler.

If a KEN rack must be moved, KDE will coordinate a graceful shutdown of the VPN device, and Tyler testing of the device after the move, as part of the overall coordination of the move.

## Network Configuration

Some configuration of the district’s network and web proxy and/or filtering systems may be required to support the EERP Cloud System.

If you need assistance with configuring your content filter, please reach out to the respective vendor for assistance.

## Workstation Configuration

Microsoft Windows PC Requirements	Minimum*	Recommended
Operating System	64-bit Windows 10	64-bit Windows 10
Processor	Intel Core i3 1.8 Ghz	Intel Core i5 2.5+ Ghz <i>(or better)</i>
Memory	6 GB RAM	12+ GB
Disk Space	50 MB	200 MB
Screen Resolution	1280 x 800	1920 x 1080

**NOTE:** Meeting the minimum workstation requirements will ensure the Tyler applications will operate but will not guarantee performance. All performance and benchmark testing are done with workstations that meet (or exceed) the “recommended” hardware configuration.

### Supported Microsoft Windows Operating Systems

- Windows 10 64-bit

### Supported Web Browsers

- Chrome (latest available version, auto updates enabled) **recommended**
- Microsoft Edge (latest available version, auto updates enabled)
- Firefox (latest available version, auto updates enabled)

### Supported Microsoft® Office Versions

- Microsoft Office 2019
- Microsoft Office 2016

- Microsoft Office 2013
- Microsoft Office 365

**NOTE:** Microsoft 365 is a subscription-based version of the Office suite with several subscription plans offering various options. A subscription including the Office desktop version is required to take advantage of the following advanced Office integration with Munis:

- Microsoft Excel desktop client is required to create connections with Munis Data Cubes and is recommended to view these reports. SharePoint Excel Services, which requires Microsoft SharePoint Enterprise, can be used as an alternative to view these reports.
- Microsoft Word desktop client is required to create templates for Munis Mail-Merge functionality.

Microsoft Excel and Word® desktop clients are also recommended for Export to Excel and Export to Word functionality, however users can save these exports and open in any application compatible with these formats (e.g., Excel Online, Google Sheets).

<b>Apple Mac PC Requirements:</b>	<b>Minimum*</b>	<b>Recommended</b>
Operating System	macOS Mojave (10.14)	macOS Catalina (10.15)
Processor	Intel Core i3 1.8 Ghz	Intel Core i5 2.5+ Ghz <i>(or better)</i>
Memory	6 GB RAM	12+ GB
Disk Space	50 MB	100 MB
Screen Resolution	1280 x 800	1920 x 1080

**NOTE:** Meeting the minimum requirements will ensure the Tyler applications will operate but will not guarantee performance. All performance and benchmark testing is done with PCs that meet (or exceed) the ‘recommended’ hardware configuration.

#### ***Supported Apple Operating Systems***

- macOS Catalina (10.15) *(Recommended)*

#### ***Supported Mac PC Web Browsers***

- Safari 13.1+ *(with auto-updates enabled)*

#### ***Supported Microsoft Office for Mac***

- Microsoft Office 2019
- Microsoft Office 2016
- Microsoft Office 365

### **Apple macOS Limitations**

Munis is fully supported on macOS with the following exceptions. This functionality can be obtained using alternative solutions such as RDS to a Windows environment or “Windows on Mac” virtualization (e.g., Parallels Desktop for Mac, VMware Fusion).

- Microsoft Office for Mac does not support connections to SQL OLAP cubes. Due to this Microsoft limitation, Munis Cubes cannot be accessed from macOS.
- Tyler Reporting Services / SQL Server Reporting Services reports cannot be created or modified.
- Advanced Tyler Content Manager functionality such as batch document scanning is not supported on macOS.

### **Additional System Requirement Information:**

[System Requirements for Muis Version 2021.1+](#)

## **Application Customization**

District staff are responsible for implementing or overseeing the implementation of any district-specific customizations to the EERP system. In some cases, districts may have to collaborate with third-party providers of customizations. Districts should plan to implement any customizations as desktop applications that access the EERP database using ODBC. District staff may contact Tyler for advice and suggestions regarding options for implementing required customizations.

## **Alternate Access**

Districts should have a plan in place for alternate access to EERP in case of issues with the local or KETS network infrastructure. The document [Alternate Connections to the Enterprise ERP](#) provides an overview of the methods available.

## **Support Contacts**

Cases can be entered through the online support portal at [Enterprise ERP Support | Tyler Technologies](#).

<b>Supported function</b>	<b>Who to contact</b>	<b>Contact info (during business hours)</b>
Enterprise ERP Financials	Enterprise ERP Help Desk	800.772.2260, #3, #1 <a href="mailto:financialsupport@tylertech.com">financialsupport@tylertech.com</a>
Enterprise ERP Payroll	Enterprise ERP Help Desk	800.772.2260, #3, #2 <a href="mailto:payrollsupport@tylertech.com">payrollsupport@tylertech.com</a>

Supported function	Who to contact	Contact info (during business hours)
Enterprise ERP Crystal /Reports	Enterprise ERP Help Desk	800.772.2260, #3, #7 <a href="mailto:tylerrreportingservices@tylertech.com">tylerrreportingservices@tylertech.com</a>
Enterprise ERP Tyler Forms	Enterprise ERP Help Desk	800.772.2260, #3, #7 <a href="mailto:formunissupport@tylertech.com">formunissupport@tylertech.com</a>
<p>Enterprise ERP Cloud (SaaS)/System Functionality</p> <ul style="list-style-type: none"> <li>-Printing</li> <li>-New users* (See User Accounts info that follows)</li> <li>-Training/Test Database Refresh*</li> <li>-Backups &amp; restorations*</li> <li>-Assistance with MIU Updates</li> <li>-Remote Access support</li> </ul>	<p>Enterprise ERP Help Desk</p> <p><i>*These processes can be performed by district personnel using Cloud Admin. Refer to the document, <u>Cloud Admin</u>, found in the <u>System and Administration</u> section of the <a href="#">Enterprise ERP (MUNIS) Support and Guides</a> webpage for instructions on how to access and use Cloud Admin.</i></p>	800.772.2260, #3, #9 <a href="mailto:asp@tylertech.com">asp@tylertech.com</a>
<p>Enterprise ERP business assistance for:</p> <ul style="list-style-type: none"> <li>- policies</li> <li>- procedures</li> <li>- codes</li> <li>- reporting</li> <li>- data collection</li> <li>- audits</li> <li>- web form submissions</li> <li>- KY-specific Financial, Payroll (including Personnel) application usage</li> </ul>	<p>Enterprise ERP Help Desk</p> <p>KY Specific Reporting Questions: <a href="mailto:EERP@education.ky.gov">EERP@education.ky.gov</a></p>	Refer to the respective Financials, Payroll, Reporting Services, or Tyler Forms contact information above



Supported function	Who to contact	Contact info (during business hours)
Network or workstation support (cannot reach the Munis login page and cannot access external websites, cannot configure browsers or install required workstation software updates)	KETS Service Desk	866.538.7435 or <a href="mailto:ketshelp@education.ky.gov">ketshelp@education.ky.gov</a>

**REPORTING AN EMERGENCY ISSUE OUTSIDE OF NORMAL BUSINESS HOURS**

In the event of a critical Cloud (SaaS) issue outside of normal business hours (weekdays from 8:00 AM-5:00 PM EST), please call 800.772.2260 ext. 4801 to reach SaaS after-hours support.

When calling, please be prepared to provide:

- Your name
- Contact information
- The site that you are calling from
- Brief description of the issue

**Enterprise ERP User Accounts**

***Overview***

In conjunction with the Multi-Factor Authentication (MFA) integration with Entra ID, each district’s Enterprise ERP (MUNIS) system has been configured to use Tyler Identity Workforce (TID-W). TID-W is a cloud-based authentication platform powered by Okta. It is designed to integrate with Entra ID so that your users can access Tyler products using credentials to which they are already accustomed. When logging into EERP, users sign in with their KETS account (email login) instead of a separate Tyler user object. When creating a user account via the User Attributes program in EERP, the account must have an email address that matches the Entra ID (Office 365) account. For Enterprise ERP authentication, the user attributes in Entra ID should be populated with the user’s first name, last name, email address, and principal name within the AD.

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

As part of the KETS Security Baseline (Microsoft EMS A3) rollout, MFA will work directly with KETS accounts and anything configured to use Office 365 for login, including Enterprise ERP.

## ***Conditional Access Policies***

A preconfigured Entra ID Conditional Access Policy requires MFA for all users when they login to EERP and should be enabled by each district's Entra ID administrator. Questions on the conditional access policy for Enterprise ERP should be directed to the KETS Service Desk (866.538.7435 or ketshelp@education.ky.gov).

## ***Tyler Datacenter User Accounts***

With the adoption of Tyler Identify Workforce (TID-W), users access EERP via Entra ID integration using their district email address and password. Enterprise ERP (Munis) datacenter accounts (example: 983jsmit) that are created via the Munis Cloud Admin

(<https://muniscloud.tylertech.com/>) will still be required to access the following Tyler services:

- Excel Cubes
- Munis Cloud Admin
- ODBC
- Tyler F5 VPN (<https://secure.tylertech.com/>)
  - Note: Users do have the option of using the KETS Enterprise VPN to access EERP outside of the school district. The Cisco AnyConnect VPN client utilizes Entra ID (Office 365) credentials. District users needing access, authorization or support for KETS Enterprise VPN should contact their local district technology support staff or district technology coordinator.

Unless a user needs access to any of the listed services, their named datacenter account can be disabled in Munis Cloud Admin (<https://muniscloud.tylertech.com/>). Any accounts that remain will still require a password change every 90 days.

## Security Considerations

Because the EERP Cloud system uses browser-based authentication, the system itself cannot prevent users from saving their passwords within their web browsers. Users should be instructed NOT to click the checkbox to save credentials when prompted by the browser. Note that even if a user does click this checkbox, their stored EERP credentials will only be used when they are logged into the workstation; other users logging into the workstation with different workstation/Active Directory credentials will NOT be able to use the first user's stored EERP credentials.

With EERP (like most web applications) there is a risk that documents, including those containing sensitive or confidential information, may remain on a workstation upon which a user has opened or downloaded the document. Each web browser/operating system combination behaves slightly differently when a user opens or downloads a document; some will always place files into an explicit Downloads directory, but others will use other directories, and in various scenarios, these files will not be automatically removed after use.

Based on KDE research and discussions with Tyler, this is only an issue for district staff using the full EERP system that allows opening/downloading Office documents; it should NOT be an issue for employees who only use the EERP self-service web application.

Districts can minimize this risk using two general approaches: first, educate EERP users on the risk and how to address it; second, assume that any workstation used for EERP access is likely to contain sensitive files. Specific steps could include:

- 1) Training EERP users to periodically remove downloaded files
- 2) Training users to use EERP-related workstations only for work activities, avoiding access to personal email and other websites
- 3) Training users to ONLY access EERP from secured workstations (not personal/home computers)
- 4) Minimizing the number of staff with access to sensitive data within EERP
- 5) Implementing full-disk encryption technologies (e.g., Microsoft's BitLocker) on workstations used to access EERP
- 6) Minimizing the number of users who can log into each EERP workstation
- 7) Ensuring that workstation backups are stored securely
- 8) Minimizing the number of workstations used to access EERP
- 9) Thoroughly purging ALL files from a EERP workstation before it is decommissioned or reallocated to another use

Additional security considerations with the saved reports (spool) directory in Enterprise ERP should also be considered. The saved report files (spool directory) should be reviewed on a periodic basis and any files with sensitive information should be purged. User account settings

in the Munis System Roles should also be reviewed to ensure the appropriate level of access for each user.

- 1) Spool file maintenance access (full, personal, or departmental)
- 2) File Transfer:
  - a. Browse export directory
  - b. Download from the spool directory

## **Digital Document Archiving**

Tyler offers several options to support districts that use the Tyler Forms blank stock printing solution and wish to maintain their financial record archive using digital copies rather than paper copies. The Tyler Content Manager solution provides a searchable repository hosted and maintained by Tyler. If districts instead choose the option to have Adobe PDF copies of Tyler Forms documents transferred to a district-owned FTP server, they should keep in mind the following:

- 1) The KETS Service Desk must be contacted to make firewall adjustments
- 2) The district will be responsible for the provision and operation of the FTP server
- 3) The district will be responsible for securing the FTP server and its confidential contents

## **Tyler Reference Documents**

Tyler documentation for EERP can be found by using Tyler Search within the Tyler support site, <https://www.tylertech.com/client-support/enterprise-erp-support>.