Connecting to Enterprise ERP from Outside Your District

Office of Education Technology: Division of School Technology Services
Questions: eerp@education.ky.gov

Contents

Overview

Under normal conditions, a user's day-to-day Enterprise ERP (EERP) work is performed from within the district offices where they access EERP over the internet through a secure hardware VPN (Virtual Private Network). Some occasions prevent users from performing their EERP tasks in the office or even through the hardware VPN. This document describes various methods to securely connect to the Cloud from within or outside of the district's intranet.

Secure Connection Methods

- Tyler Software VPN or SSL Connection (https://secure.tylertech.com/): This is a software VPN that is installed on a workstation and provides software-encrypted communication between the user workstation and the Cloud servers. This type of connection is available anywhere a user can establish an internet connection and ***has rights to install software on their PC***. This connection also requires a second set of user credentials (datacenter accounts) that are maintained via the Cloud Admin by your EERP System Administrator (typically the finance officer).

- Alternately, district users can connect to EERP via the Cisco Secure Client. District users needing access, authorization, or support for KETS Enterprise VPN should contact their local district technology support staff or district technology coordinator.

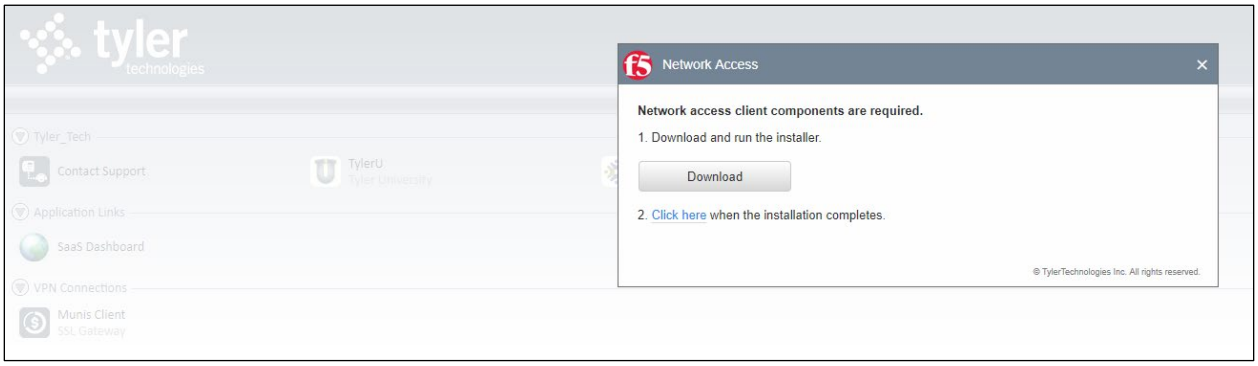
Establish a Remote Secure Connection

A secure connection is established via a secure https website. To use the Tyler provided software F5 software VPN, a datacenter account established through the EERP Cloud Admin is required (https://muniscloud.tylertech.com/). Once the secure connection is created, users will log into their Tyler Hub using their email address and password the same way they would in the district.

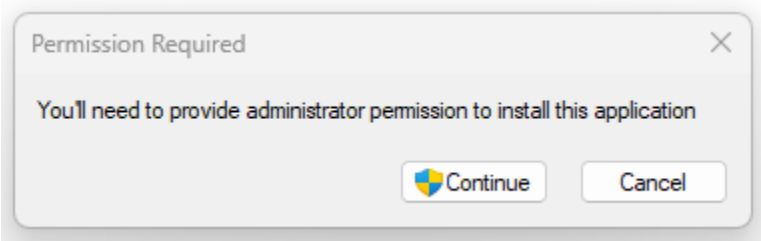
1. To connect click the link below or paste it into your browser:
   https://secure.tylertech.com/

2. Enter your datacenter login ID (e.g. 9234jsmi – do not enter datacenter before your account name) and password.

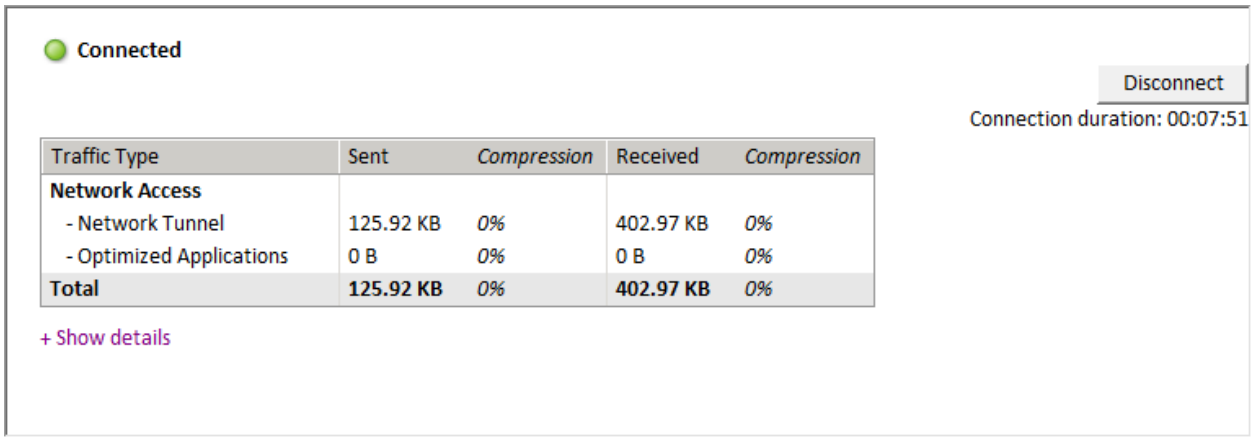
3. Upon Login; you will be prompted to download an installer if it is not already installed. If you do not see a prompt to download the software, please click on the icon 'Munis Client SSL Gateway'.



4. If you see a pop-up alert regarding needing administrator permission, please hit 'Continue'. If you do not have administrator access to your computer, please contact your district technology office.



5. Once the software is installed, you will see a new screen that provides connection status, traffic type, connection duration, and an option to Disconnect.



6. In your browser, select your saved links to your district instance of Tyler Hub. Log in to EERP using your email address and password.

Closing the Secure Connection

To close the connection:

1. Close your dashboard web browser just as you would at the office.
2. Maximize the SSL Gateway pane (f5 application window).
3. Click the ***Disconnect*** button in the upper right corner of the SSL Gateway window (5f application).
4. On the https://secure.tylertech.com/ webpage, select the **Logout** button in the upper right-hand corner of the browser window.

Printing from a Remote Connection

Printing from a remote Cloud connection can be easily accomplished using PDF output.

If a long-term outage occurs and you must print checks or reports, staff will need to work with EERP support and the district technology staff to set up an alternate printing location. As part of a business continuity plan, check with your technical staff on the ability to print from another location such as a neighboring school district.

Keep in mind all the components needed to print and distribute forms. Your district may have a check signer, folder, sealer, and other equipment necessary to perform a printing/distribution task.

Hardware VPN Problems

In the unlikely event that your district experiences a problem with the hardware VPN, users can still access the Cloud within the district if your internet connection is active. If the VPN is down, users can access the Cloud the same way they would access it if they were remote. To do this, follow the instructions above "Establishing a Remote Secure Connection". This will bypass the hardware VPN and allow access to the Cloud.

Business Continuity

Establishing a remote connection begins the process of ensuring business continuity in the event of an outage. We suggest you establish and test one or more of the following options:

- Identify laptops to use in the case of an outage and test the connection to the Cloud from your home or other location. This should be done for all staff requiring access to perform critical processes.

- Establish a reciprocal agreement with one or more neighboring districts to use their internet connection. You should be able to use their internet connection from any of the district facilities (schools, central office, bus garage, etc.).
- Establish a relationship and agreement with a local business, public library, or other location having internet connectivity.
- Explore the viability of a Hot Spot device or tethering to a cell phone. If any of these options are selected, implement and test the solution to be prepared.