



Alternate Connections to the Cloud

Overview

Under normal conditions, a users day to day MUNIS work is performed from within the district offices where they access MUNIS over the internet through a secure hardware VPN (Virtual Private Network). There are occasions that prevent users from performing their MUNIS 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.

Why Consider Alternate Connections?

Whether it is for convenience or out of necessity, each district should plan for, establish and test alternate connections. Some of the reasons are:

- Convenience of working from home or other location while out of the office
- Power or internet outage at the office
- Storms or other conditions limiting access to the office
- Hardware VPN issues

An alternate connection ensures your staff continues to perform routine or critical processes in the event that you cannot connect through normal methods.

Internet Access Options

Connecting to the Cloud can be accomplished through most any internet connection. Today, internet access and devices providing access are readily available. Some options are:

- Internet access from another district that is live or in process of migrating to the Cloud
- Home, business or other providers of free or fee based internet access
- Air card device that plugs into your computer and provides internet access via cellular service
- Hot spot device that provides internet access via cellular service for multiple computers in close proximity to the device
- Tethering via a cellular phone allows internet access for one or multiple computers in close proximity to the phone

This is a sample list. Please speak with your district CIO for other options.

Secure Connection Methods

A secure connection is an absolute requirement to ensure the information accessed, displayed and processed by MUNIS users is not accessed or viewed by unauthorized individuals. Tyler provides two methods of securely accessing the Cloud servers:

- Hardware VPN: This device is installed in each district and provides hardware encrypted communication between the district and the Cloud servers. This type of connection is only available when a user is within the district intranet.
- Software VPN or SSL Connection: 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.

Preparing the Workstation

No matter the connection method, each workstation must be adequately configured and prepared to access the Cloud. If your workstation has previously connected to the Cloud and viewed the MUNIS Dashboard, it is "Cloud ready". Proceed to Establishing a Secure Connection.

If the workstation is not Cloud ready you may choose one of two options: 1) Seek the assistance of your technology staff to ensure the workstation meets minimum requirements, install software and adjust browser settings. 2) Follow the steps below to prepare the workstation.

Follow these steps to prepare the workstation:

1. Workstation minimum requirements:
 - Windows XP, Vista, or 7
 - 1 GB RAM or more
 - 50 MB Free disk space
 - Monitor with 1024 X 768 resolution
 - Internet Explorer version 7.x, 8.x or 9.x (32-bit)
2. Ensure Microsoft Silverlight 4 is installed. You can check for and install the latest version of Silverlight by clicking the link:
<http://www.microsoft.com/getsilverlight/Get-Started/Install/>
3. Ensure Microsoft .Net Framework 3.5 SP1 is installed. Click the link to install the latest release:
<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7>

4. Make any required adjustments to web browser configuration settings. Internet Explorer Security Level of Medium Low is sufficient for proper MUNIS operation. If you customize the Internet Explorer Local Intranet zone security settings, the following settings must be set to Enabled or Prompt:
 - I. ActiveX controls and Plugins
 - a. Automatic prompting for ActiveX controls
 - b. Download signed ActiveX controls
 - c. Run ActiveX controls and plug-ins
 - d. Script ActiveX controls marked safe for script
 - II. Downloads
 - a. Automatic prompting for file downloads
 - b. File Download
 - III. Miscellaneous
 - a. Software channel permissions – medium or low safety
 - b. Use Pop-up Blocker (disable)
 - c. Userdata persistence
 - d. Scripting
 - e. Active Scripting (recommend “Enable”)
 - f. Allow cookies
 - IV. Consider removal or configuration of any browser add-ons (such as Google Toolbar) that may interfere with web applications such as MUNIS.

Note: If the workstation is also used to connect to the Cloud from within the district (using the hardware VPN), internet proxy settings are necessary. See your CIO to establish these settings.

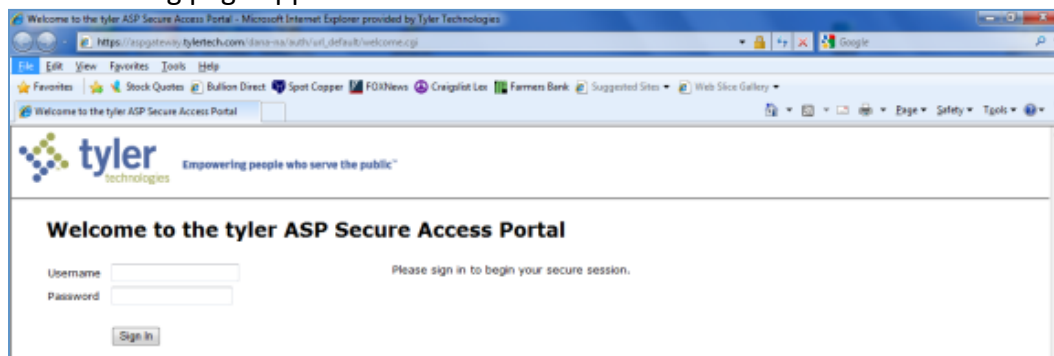
Establishing a Remote Secure Connection

A secure connection is established via Internet Explorer version 7, 8 or 9 through a secure http web site.

1. To connect click the link below or paste it in the URL field of the browser:

Munis V10.5: <https://saasgateway.tylertech.com>

The following page appears:

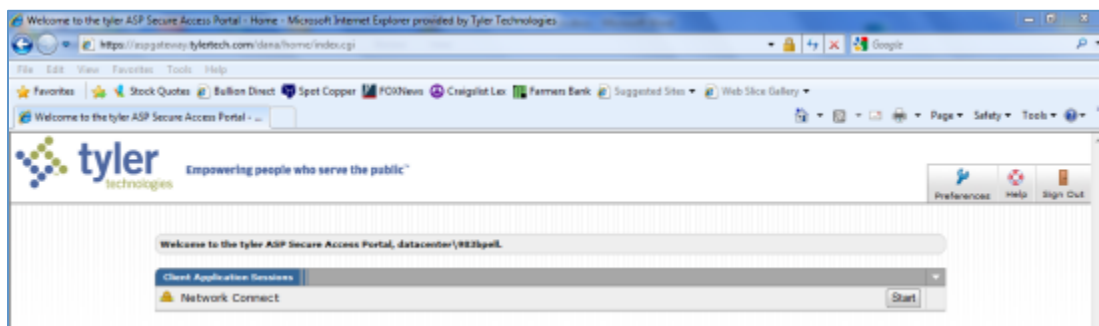


- Each time you connect to the Cloud from outside the district office, you must connect to the ASP Secure Access Portal first. Establishing a desktop shortcut icon facilitates future connections. From the menu bar click File -> Send -> Shortcut to desktop to establish a desktop icon shortcut. After creating the desktop icon you may wish to rename the icon description to "Cloud Secure Connection" by right clicking on the icon and selecting Rename.

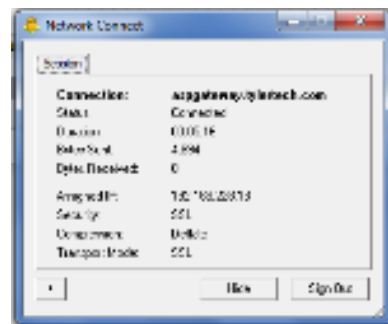


- Enter your login ID (e.g. datacenter\9234jsmi) and password. It may take a few minutes for the following screen to appear and you may be prompted to install an ActiveX control. If prompted to install the ActiveX control, proceed with the installation. After a period of time the pane below should appear.

Note: If the screen below does not appear after a few minutes, click the [Continue](#) link at the bottom left of the pane.



- Click the **Start** button to launch the SSL software. Upon connecting the following pane appears:



- Click **Hide** to hide the pane.
- You can now minimize the ASP Secure Access Portal web page from step 3. The secure connection is now established.

7. If your workstation previously connected to the MUNIS Dashboard, click on the Munis Cloud icon to connect to the Cloud. If you have never connected to the Cloud with this workstation, follow the instructions in KY Cloud First Login & Setup to establish a Cloud connection, create a desktop shortcut and install the Genero Desktop Client Active X control.

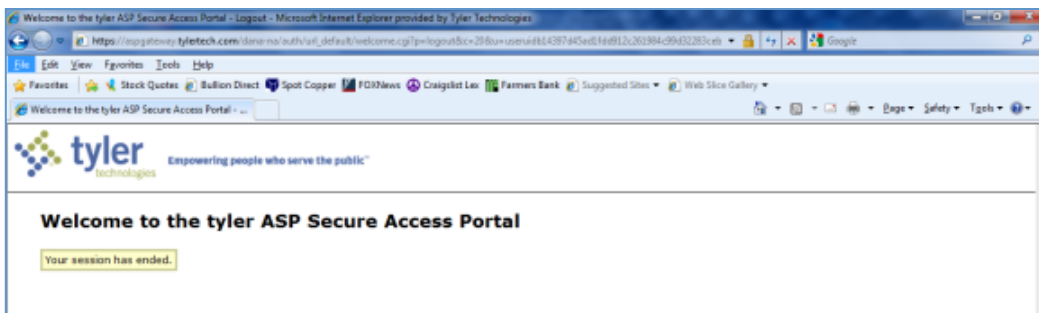


8. After logging into the dashboard you may notice navigating and opening programs is slower than at the district office. Connecting to the Cloud using the Secure Access Portal adds additional overhead which could result in slower response. Once a program is open however, performance should be similar to the district.

Closing the Secure Connection

To close the connection:

1. Close your dashboard web browser just as you would at the office
2. Maximize the ASP Secure Access Portal pane (from step #3 above)
3. Click the **Sign Out** button in the upper right corner of this pane. Upon completion you will see:




Printing from

a Remote Connection

Printing from a remote Cloud connection can be easily accomplished. Any printer accessible to the workstation can be utilized. Keep in mind that if the printer is not PCL 5 compatible the output may look different or not print at all.

If a long term outage occurs and you must print checks or reports, staff can take a printer home or to another location to print. It may require some advance work by the district technology staff to ensure the printer can connect to and be recognized by the workstation but this should be possible. As part of a business continuity plan, check with your technical staff on the ability to print from a workstation to a district printer in a remote location.



Keep in mind all of 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 as long as 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 an Air Card, Hot Spot device or tethering to a cell phone. If any of these options are selected, implement and test the solution to be prepared.