Banner SSL VPN User Guide

Table of Contents

Document Control and Version info

Table of Contents

What do I need to be able to VPN into Banner’s Network?

Where do I get what I need?

What setup is needed before a VPN connection is possible?

Before calling the IT Service Desk, please complete the following steps

IT Service Desk contact information

What can the IT Service Desk help with?

What can the IT Service Desk NOT help with?

Pre-MobilePASS device enrollment

MobilePASS Device Enrollment

Post-MobilePASS device enrollment

Accessing Banner’s VPN

Testing your MobilePASS token

Frequently Asked Questions

<table>
<thead>
<tr>
<th>Version</th>
<th>By</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3</td>
<td>Jerome Casper</td>
<td>6-1-2016</td>
<td>Combined VPN/2FA documentation</td>
</tr>
<tr>
<td>Guide Maintainence</td>
<td>IT Service Desk</td>
<td>Ongoing</td>
<td></td>
</tr>
</tbody>
</table>
What do I need to be able to VPN into Banner’s Network?

1) Network account and password
2) MobilePASS application
3) Cisco AnyConnect VPN application

Where do I get what I need?

1) Network account and password
   a. Manager (or Banner contact) will provide the network account and password
2) MobilePASS application
   a. Banner laptops should have this already installed.
   b. Non-Banner computers can download the application, use the site below:
   c. Mobile device users can download the application from the app store
      i. Search for “SafeNet MobilePASS”
3) Cisco AnyConnect VPN application
   i. Banner laptops should have this already installed.
   ii. Any VPN user can download the application

1. See “Post-enrollment” instructions

What setup is needed before a VPN connection is possible?

1) Network account and password
   a. Account must have VPN permissions
      i. Manager submits a request for VPN access on employee behalf
   b. Account must be “Active”
      i. Account must not be expired or disabled
   c. Initial or expired passwords must be changed by the user before VPN’ing.
      i. Initial passwords are pre-expired, and passwords expire every 90 days
      ii. An account with an expired password cannot VPN
         1. BHS accounts: for password changes, use the site below
            a. [access.bannerhealth.com/owaresettool/](http://access.bannerhealth.com/owaresettool/)
         2. UMC accounts: for password changes
            a. contact IT Service Desk 602 747 4444 or 877 247 3499
   d. Account must have an email address
2) MobilePASS application
   a. The MobilePASS device must be enrolled correctly
      i. See “MobilePASS Device Enrollment” instructions
3) Cisco AnyConnect VPN application
   a. Required version of AnyConnect is 4.2. (Older versions may not connect)
   b. Must use appropriate login page URL and accurately perform VPN logon steps
      i. See: “Accessing Banner’s VPN” instructions
Before calling the IT Service Desk, please complete the following steps:

1) Verify you are able to get to the appropriate SSL VPN site below using an internet browser:
   a. accessaz.bannerhealth.com (Arizona)
   b. accesswr.bannerhealth.com (Western Region)
   c. fmhvpn.bannerhealth.com (Alaska)
   d. vpn.umcaz.edu (UAHN)
      i. If you are unable to access the appropriate site, please verify you are connected to
         the internet (IT Service Desk can provide generic instructions on configuring your
         wireless adapter for your home network). If you feel you are properly connected,
         please contact your Internet Service Provider (Cox, CenturyLink, Qwest, etc.) to
         troubleshoot your internet connection.

2) Verify that your username and password are valid by logging into Outlook Web Access:
   a. OWA URL: bhsmail.bannerhealth.com
      i. If you are unable to login to OWA, you can attempt to reset your password using
         the “Need to Reset your Password? Click Here” link at the bottom of the page. You
         may also call the Service Desk to have your password reset.
IT Service Desk contact information:
Arizona users can contact the Service Desk at 602-747-4444 or 877-247-3499.
Western Region users can call 800-424-8930.

What can the IT Service Desk help with?

1) Network account and password
   a. IT Service Desk can identify whether the account...:
      i. ...has VPN permissions
      ii. ...is active (“not disabled”)
      iii. ...is expired (“end-date in the past”)
      iv. ...has an email address attribute
      v. ...has an expired password
      vi. IT Service Desk can also do password resets

2) MobilePASS application
   a. IT Service Desk can...:
      i. ...assist with installing the MobilePASS application on a Banner computer
      ii. ...verify an account is found in the two-factor authentication system
      iii. ...verify the two-factor system recognizes an enrollment for the account
      iv. ...re-send enrollment emails
      v. ...revoke existing enrollments
      vi. ...change MobilePASS devices
      vii. ...assist with MobilePASS enrollment and enrollment issues
      viii. ...resolve “Unknown Token” encryption errors (“red exclamation point” tokens)

3) Cisco AnyConnect VPN application
   a. IT Service Desk can...
      i. ...assist with update/installation of AnyConnect to a Banner laptop
         1. Must be during business hours
         2. Laptop must be onsite at a Banner facility, connected to the Banner network

What can the IT Service Desk NOT help with?

- Troubleshooting your internet or home network connection
- Installing the SSL VPN plug-in on your home PC
- Any error messages that are related to the SSL VPN or Remote Desk software on your home PC
- Any configuration of your personal PC or printer
Pre-MobilePASS device enrollment – select a MobilePASS device

Select ONE device on which to use MobilePASS. Options are listed in order of recommendation:

1. **Your Banner-issued laptop.** Banner recommends using the MobilePASS application on its laptops for VPN users. This method will work great for anyone who will be using their Banner laptop each time they access the VPN.
   - Quick: MobilePASS is right there on your desktop
   - Easy: the "Copy Passcode" button allows you to copy/paste the Passcode - you do not have to remember or type the Passcode.

2. **Your smartphone or tablet.** Banner recommends the use of a smartphone as your MobilePASS device for anyone accessing the VPN from multiple devices. Smartphones allow flexibility, security, and simplicity.
   - Flexibility: no matter which device you are using to access the VPN, you will have your MobilePASS available.
   - Security: separating your MobilePASS device from your computer or other VPN device increases the difficulty for anyone attempting unauthorized access to Banner’s network using your account.
   - Simplicity: Getting the “SafeNet MobilePASS” app is easy: find it in the app store and install!

3. **Your personal or vendor-issued Windows or Mac computer.** If you will be accessing Banner’s VPN from this PC only, you can use a personal or non-Banner computer as your MobilePASS device.

MobilePASS device enrollment

1. Use your chosen MobilePASS device to access the “Self-enrollment” email you received. The “Self-enrollment” email is shown below. You will click the link in Step 1 to open the enrollment website.

![Banner Health](image)

**Hello Jerome Casper:**

This message is from the Banner Health Two-Factor Authentication Service featuring MobilePASS.

Banner employees viewing this email in Outlook will see an "EXTERNAL EMAIL" warning because this service is hosted by SafeNet Inc., outside of Banner’s network.

This enrollment email can be used to enroll one MobilePASS device.

Before you begin:

NOTE: Enroll MobilePASS on a device you will have with you when you access Banner's VPN.

NOTE: You MUST use the link below to perform a valid enrollment.

NOTE: Your MobilePASS device generates Passcodes, but you can use the Passcodes with any VPN device.

NOTE: Your MobilePASS device can be changed (contact IT Service Desk).

To enroll MobilePASS, carefully follow the 4 steps below from the device you want to enroll. You may forward this email.

Step 1. Click the link below to open the enrollment website in your browser in a new window.  **https://se.cafenet-inc.com/selfEnrollment/index.aspx?code=9guUCkTD7x4f5O2Y9D9GxM**  (link will expire after 10 days and cannot be reused)

Step 2. **ONLY IF YOUR DEVICE NEEDS MOBILEPASS**, click the MobilePASS icon to begin downloading the app. If your device has MobilePASS, move on to the next step.

Step 3. From the enrollment website, click "Enroll your MobilePASS device." This opens MobilePASS.

Step 4. Assign a name to your MobilePASS token. Click "Activate". Enter and re-enter a 4-digit PIN. A Passcode will display. This completes MobilePASS enrollment.

For more information visit:  
IT Security MobilePASS Two-factor authentication Wiki page  
For urgent issues, please contact the IT Service Desk - (602) 747-4444.
2. Shown below is the enrollment website. Follow the instructions to download and install the MobilePASS app if needed. Once MobilePASS is installed on your device, click “Enroll your MobilePASS device”.

Two-factor authentication - Self Enrollment

Welcome to the Banner Health MobilePASS self-enrollment website!

STOP AND CHECK:
---Does your device have the MobilePASS application installed already?
If yes, skip down to the big "Enroll your MobilePASS device" link below.

IF MOBILEPASS IS NOT ON YOUR DEVICE, you may download it from the following location:

[Image of SafeNet logo]

Download MobilePASS Installer (.msi)

NOTE: If you need to enroll a Banner laptop as your MobilePASS device, but MobilePASS is missing, please contact the IT Service Desk for assistance. You will need to be on-site or connected to Banner network for installation assistance.

WITH MOBILEPASS INSTALLED ON YOUR DEVICE, select the link below to enroll your device.

Enroll your MobilePASS device

In the event you are experiencing difficulties with loading the token with this link, you may instead copy the following string, open the MobilePass application, select Automatic Enrollment, and then paste (on some platforms it may already be pasted):

RW5yb2xsbWVudFVSTD1odHRwczovL3NlLmNvbS9zZWxmZWR5yb2xsbWVudC9kZXRlMjIzNjQyMjA=

Close your browser
3. Smartphone users: the next two windows do not apply to you.
   Desktop users: after clicking “Enroll your MobilePASS device”, the window below appears. Select “Allow”.

![Image of Internet Explorer window](image1)

4. Desktop users - Another window will appear. Select “Allow”.

![Image of Internet Explorer Security window](image2)
5. MobilePASS has opened. Assign a name to your token and select "Activate" to activate.

6. Next you will set your Token PIN. Your Token PIN should:
   - be memorable. If you forget your PIN your MobilePASS token is unusable and MobilePASS will have to be re-enrolled.
   - never be shared with anyone. Do not share it with IT, or your boss, or your coworkers.
   - never be written down or saved anywhere except in your memory

   After you enter your desired PIN, select “Continue”.
7. Next you will re-enter the desired Token PIN to confirm it and select “Continue”:

That’s it! Your Token is now enrolled and MobilePASS should now display a 6-digit number known as a “Passcode”. MobilePASS Passcodes are used as your “Second Password” when using two-factor authentication at Banner. Each Passcode can only be used once, so you will use MobilePASS to generate a new Passcode for each login.

To generate a new Passcode: open MobilePASS, select your token, enter your PIN; a new Passcode will display.
Post-enrollment – set password and install Cisco AnyConnect

*Section may not be necessary for existing VPN users or those using a Banner laptop as their VPN device.

New VPN users will need to change their password

*A pre-expired initial password, or a password over 90 days old, will prevent successful VPN login.

BHS -- If you have not already done so, you will need to set your own password.

Go to [https://access.bannerhealth.com/owaresettool/](https://access.bannerhealth.com/owaresettool/) and follow the instructions on the page to set a new password.

You may also contact the IT Service Desk and use the manual reset prompts, or wait for assistance.

UMC -- To reset a UMC account password, contact the IT Service Desk: 602 747 4444 or 877 247 3499.

Installing Cisco AnyConnect

*MobilePASS must be enrolled before Cisco AnyConnect can be installed as indicated below.

“Cisco AnyConnect Secure Mobility Client” (AnyConnect) is the program that must be used to create a VPN connection to Banner.

To download/install AnyConnect, you will need to sign into a SSL VPN homepage (shown below).

Open your internet browser and access the appropriate SSL VPN homepage:

- Arizona: accessaz.bannerhealth.com
- Western Region: accesswr.bannerhealth.com
- Alaska: fmhvpn.bannerhealth.com
- UMC (UAHN/BUMC-T/BUMC-S): vpn.umcaz.edu

To sign in to the SSL VPN homepage:

- Enter your network username in the USERNAME field.
- Enter your network password in the PASSWORD field.
- Enter a MobilePASS Passcode in the last field.

Click “Login”
After signing into the SSL VPN homepage, you will see a page similar to the one below. To download/install AnyConnect, you will click the “Start AnyConnect” link shown below.

AnyConnect should automatically be installed to your machine (administrator approval may be required). After install, AnyConnect will establish a VPN connection to Banner using the existing SSL VPN homepage session.

Open the SystemTray (clip #1 below) - Look for the AnyConnect icon (clip #2 - w/lock engaged).

When the lock is engaged on the AnyConnect logo (shown), you are VPN-connected. You can start or disconnect VPN sessions by right-clicking the AnyConnect icon in the system tray; select “Connect” or “Disconnect”.

Once installed, the AnyConnect program can also found under “START” > “ALL PROGRAMS” > “CISCO”.

With AnyConnect installed (and MobilePASS enrolled), you are ready for the next section “Accessing Banner’s VPN”
Accessing Banner’s VPN

*The VPN login process requires Cisco AnyConnect 4.2 and an enrolled MobilePASS token, along with ID/pw.

1. Open AnyConnect

   NOTE: To find this program, open the “Start” button, select “All Programs”, and open “Cisco AnyConnect Secure Mobility Client” in the Cisco folder
   OR
   Open AnyConnect from the SysTray by clicking on the Anyconnect icon

2. Before you click “Connect”...

   Select the VPN login page URL appropriate for your location from the drop-down list (screen clip #1).

   **Banner VPN login page URLs**
   AZ: AccessAZ.bannerhealth.com
   WR: AccessWR.bannerhealth.com
   AK: fmhvpn.bannerhealth.com
   UMC: vpn.umcaz.edu

   If the appropriate VPN login page is not found in the drop-down list, you can click into the text box and manually enter (type) the URL (screen clip #2).

   **After use, URLs will be added to the drop-down list for future selection.**

3. Click “Connect”.

   **After use, URLs will be added to the drop-down list for future selection.**

   ![Screen clip #1](image1.png)
   ![Screen clip #2](image2.png)
   ![Screen clip #3](image3.png)
4. The VPN login page asks for “Username”, “Password”, and “Second Password”
   a. Enter your LAN ID in “Username”
   b. Enter your LAN ID password in “Password”
   c. **DO NOT CLICK OK YET…**

5. Open MobilePASS and select your token
6. Enter your token PIN and click “Continue”.

NOTE: The token PIN is set during enrollment – the token PIN must be entered each time MobilePASS is opened in order to generate a new Passcode.

7. You should now see a “Passcode” in the MobilePASS display. You will use this 6-digit Passcode as the “Second Password” in AnyConnect.
8. Enter the 6-digit Passcode from MobilePASS in the “Second Password” field of the AnyConnect login page.

![Cisco AnyConnect login page with Second Password highlighted.]

9. Click “OK” to submit the form.

![Cisco AnyConnect login page with OK button highlighted.]

10. Click “Accept” to agree to Banner’s Terms of Use.

   You are now connected!
Testing your MobilePASS token

You can verify that your MobilePASS token enrollment was successful by attempting to sign into the SafeNet self-service portal. You will use your BHS or UMC network ID and a Passcode generated by the MobilePASS token you have already enrolled.

1. Open the correct SafeNet self-service portal
   a. BHS accounts – click here
   b. UMC accounts – click here

2. Click on “Sign In” from the upper-right corner of the screen.

3. Click on “Sign in using your token”
4. Enter your network ID in the “User ID” field and enter a new Passcode from MobilePASS in the “OTP” field. Click “OK”.

5. If your login attempt was successful, you will be shown the initial self-service page with “Sign Out” in the upper right corner (as shown below) instead of “Sign In”. MobilePASS enrollment is successful and MobilePASS is ready for use with two-factor authentication at Banner.
If your login attempt was not successful, you will see the error message shown just below.

Your login attempt was not successful. Please try again.

To confirm an unsuccessful result, generate a fresh MobilePASS Passcode and try Step #4 again.
If still unsuccessful, you can:
- Confirm you have selected the correct Self-Service Portal link in Step #1. If not, try again.
- Try again to enroll your MobilePASS token; see “MobilePASS Device Enrollment” instructions
- Remove “bad” or invalid tokens from MobilePASS. To delete existing tokens:
  - Selecting a “bad” token in MobilePASS
  - Entering your PIN
  - Selecting the trash can and “Delete”
    - (Windows): trash can icon is on the right sidebar
    - (iOS): use the gear icon to open the options menu and see the trash can icon
    - (Android): use the menu button to open options menu and reveal trash can icon
  - NOTE: PIN not required if there is an exclamation point “!” next to an “inactive token
  - NOTE: If MobilePASS has an “Unknown Token” with a RED exclamation point “!”", contact IT Service Desk for help with removal of that token.
  - Close MobilePASS (it will be opened at the right time during enrollment).
- If your enrollment email link does not open the enrollment website, but instead opens a web page that indicates your enrollment task was already completed or has expired, you will need a new enrollment email. Contact the IT Service Desk to have a new enrollment email sent.

6. Bottom Line:
If you ARE NOT able to log into the self-service portal as directed in this document, you have not successfully enrolled your token. Go back to the “MobilePASS Device Enrollment” instructions and correctly enroll your MobilePASS token. As indicated above, this may require the system administrator to send you a new enrollment email.
Frequently Asked Questions:

**What is SSL VPN?**
SSL VPN is a web-based method of securely and remotely connecting your PC to the Banner network.

**What is Two-Factor Authentication?**
Two-Factor Authentication (2FA) combines "something you know" and "something you have" in order to log into our remote access system.

When someone logs in, they enter a username – this is an identity claim.

- Then they enter a password – this is one “authentication factor” that verifies the identity claim.
  - Your password is "something you know".
- At Banner, the second “authentication factor” is a Passcode.
  - These single-use-only Passcodes are generated by using an enrolled MobilePASS device.
  - The MobilePASS device is "something you have".
- Passcodes are entered in the third field of a 2FA login page, after the usual username and password info.

**Do I have to enroll MobilePASS on all my devices?**
No, you can only enroll MobilePASS on one device at a time.

**Can I change my MobilePASS device?**
Yes. Please contact the IT Service Desk to have your existing MobilePASS enrollment revoked and have a new enrollment email sent to you.

**How do I enroll MobilePASS?**
See “MobilePASS Device Enrollment”

**How do I connect to the SSL VPN?**
See “Accessing Banner’s VPN”

**What does SSL VPN give me access to?**
SSL VPN securely connects your PC to the network. If you are on a Banner PC, it will function just as it would if you were on the PC at work. If you are on a home PC, you will be able to access websites that are normally only available from a Banner PC (such as the Intranet), but will not have access to shared drives, email through Office Outlook or non-web-based Banner applications. If you need access to these types of resources, you will need to remote control your work PC with Remote Desktop Connection.

**What is Remote Desktop Connection?**
Remote Desktop Connection is a tool used to connect to your work PC from your home PC. Once connected, you will see the same screen you would see if you were physically at your work PC and you will have access to any applications, network drives for files that you would see while at work. You must first connect to SSL VPN in order to use Remote Desktop Connection.
Do I need a PC at work for SSL VPN to work?
A PC at work is not required to access Banner websites (such as the Intranet) while on SSL VPN. You will need to use Remote Desktop Connection to remote control a PC at work if you would like to access your network drives, non-web-based applications or email through Office Outlook.

If so, does the office PC need to be turned on for me to access it remotely?
Yes, the PC must be turned on in order for you to remote control it. In addition, if you need to access network drives remotely, you must lock the PC instead of logging out when you leave the work. To lock the PC, press Ctrl-Alt-Del and then choose “Lock Computer”.

Can I connect to a PC that I share with my coworkers?
Only one person can be logged into the PC at a time, whether they are accessing it locally or remotely. Remote Desktop should not be used on shared PCs for this reason.

How do I connect to my work PC?
First, connect to SSL VPN using the steps above (see “Accessing Banner’s VPN”). Once you are connected, you will need to open Remote Desktop Connection. On Windows 7 this can be found by going to Start->All Programs->Accessories->Remote Desktop Connection.
You will see the following screen once Remote Desktop Connection is opened:

![Remote Desktop Connection](image)

Type in your work PC name and click “Connect”. Once you are connected, you will be prompted to login to your work PC. After logging in, you will see your work desktop as if you were sitting in front of your PC at work. You can go to Start->Disconnect when you are done and wish to disconnect from your work PC.

Note: Mac users can download the Remote Desktop Client from http://www.microsoft.com/mac/downloads.mspx. The Service Desk does not support the installation or configuration of this application.
You will receive the following error message if you are unable to contact your work PC:
The main causes of this issue are not being connected to SSL VPN or the remote PC being turned off. Please see the “How can I verify that I am connected to SSL VPN?” section of this document if you receive this message.

How do I find my work PC name?

You can find your work PC name by running the Myinfo application. There are three ways to access it.

You can access it by clicking the Myinfo icon by your Start button in Windows:

You can go to Start->Run, type “myinfo” and press OK:

You can also go to Start->All Programs->Banner Programs->Myinfo.
Your PC name will be the third item listed on the Myinfo screen.

How can I verify that I am connected to SSL VPN?

When you are connected, Windows will show the following icon by the clock at the bottom right of your screen:

Mac OSX will show the same symbol by the clock at the top right of the screen.

You can also verify connectivity by attempting to ping network resources that are only available while on VPN. Ping is a simple tool that verifies that your PC is able to communicate with a website or server.

To run a ping test on Windows, go to Start->Run, type “cmd” and press OK:
This will bring up a command line window:

![Command Line Window](image)

Type “ping intranet.bannerhealth.com” and press Enter. If you are connected, you will see the following result:

```
C: \WIN\DO\syst\32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]  
(©) Copyright 1985-2001 Microsoft Corp.  
H:\>
```

```
Pinging phx00140.bannerhealth.com [10.64.2.170] with 32 bytes of data:
Reply from 10.64.2.170: bytes=32 time<1ms TTL=126
Reply from 10.64.2.170: bytes=32 time<1ms TTL=126
Reply from 10.64.2.170: bytes=32 time<1ms TTL=126
Reply from 10.64.2.170: bytes=32 time<1ms TTL=126
```

```
Ping statistics for 10.64.2.170:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

If you are not connected, it will say “Request timed out”.

You can use the same process to verify that your work PC is online. Type the word “ping” followed by your work PC name (e.g. “ping phx011111111”) and press Enter. You will receive replies from your work PC’s IP address if it is currently online. If the PC is not online, it will say “Request timed out”. The most common cause of this problem is the PC not being turned on. If you receive this message, you can contact someone who has access to the PC to have them verify it is powered on.
These steps can also be completed on a Mac by using the Network Utility. You can access it by double-clicking your Hard Drive and going to the Applications folder. Double-click the Network Utility icon to launch it. Click on the Ping tab, type the address you wish to ping (e.g. “intranet.bannerhealth.com” or “phx101111111”) and click the Ping button.

**How can I fix the error message “The VPN Client Driver has Encountered an Error”?**
Cisco has provided a possible fix for this error message. The steps are located at: [http://www.ciscopress.info/en/US/products/ps6120/products_tech_note09186a00809b4754.shtml#rty](http://www.ciscopress.info/en/US/products/ps6120/products_tech_note09186a00809b4754.shtml#rty)

**How can I enable the numeric keypad when remoting to a Banner PC using a Mac?**
If you are remoting a Banner PC with a Mac and the numeric keypad is not working, press the “Clear” key on the keypad to enable it.