

Information Technology Services

Infrastructure Management

Networking



User Guide

Accessing and Using FTCC Virtual Private Network (VPN)

Table of Contents

1	PURPOSE	3
2	SCOPE	3
3	ACRONYMS/DEFINITIONS	3
4	PROCEDURES	4
4.1	HOW TO LOG ON TO THE RSA SELF-SERVICE WEBSITE	4
4.2	CONNECTING TO FTCC VPN	6
5	EXCLUSIONS/EXCEPTIONS	8
6	RELATED COLLEGE DOCUMENTS, FORMS, AND TOOLS	8
7	DOCUMENT ADMINISTRATION.....	8
7.1	DOCUMENT OWNER	8
7.2	DOCUMENT REVIEW	9
7.3	VERSION HISTORY	9
7.4	APPROVAL HISTORY	9

1 Purpose

The purpose of this document is to define the process and uses of VPN (virtual private network) at Fayetteville Technical Community College (FTCC). VPN is used as a remote access tool to connect to your desktop computer to access information that cannot be accessed within Self-Service. It also allows for accessing other systems and files (OneDrive, Colleague, SharePoint, etc.) that are not accessible from off campus.

Self-Service can be used to view and advise students as long as you have been assigned as an Advisor within Colleague. Self-Service can also be used to access employment information, such as pay records, tax forms, etc., related to your employed position at FTCC. The following systems are internal only and require access back through VPN when off campus:

- Informer
- Etrieve
- Clarity
- Colleague UI
- SharePoint

This document will assist you in connecting to the FTCC VPN client and provide basic knowledge of how to use it. If, after using this document, you still have problems with any portion of the FTCC VPN client, please contact the FTCC Service Desk at 910-678-8502 or email help@faytechcc.edu.

2 Scope

This document applies to all College faculty and staff, whether full- or part-time members of the College community. This document applies to all information collected, stored, or used by or on behalf of any operational unit, department, or person within the community in connection with college operations. If any information at FTCC is governed by more specific requirements under other College Standards and Guidelines, the more specific requirements shall take precedence over this document.

3 Acronyms/definitions

- **Information Resource:** Data, information, and information systems used by FTCC to conduct College operations. This includes not only the information or data itself, but also the computer, network, and storage systems used to interact with the information.
- **Information Security:** The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the *confidentiality*, *integrity*, and *availability* of data.
- **RSA - Rivest–Shamir–Adleman:** An algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm.

- **RDP - Remote Desktop:** A separate program or feature found on most operating systems that allows a user to access an operating computer system's desktop. The access occurs via the Internet or through another network in another geographical location and allows users to interact with that system as if they were physically at their own computer.
- **VPN - Virtual Private Network:** An encrypted connection over the Internet from a device to a network. It is useful for corporate traffic over the Internet.
- **Self-Service:** A web interface that allows you to access information contained in the administrative database used by FTCC. The application system that creates this database, Colleague, is the product of Ellucian. This system contains the forms and supporting infrastructure to extract and deliver information from this database to your desktop browser.

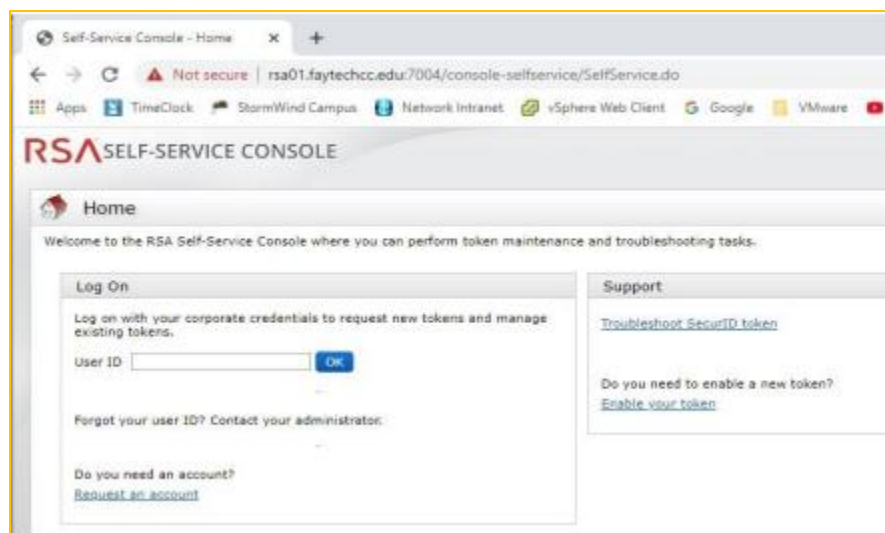
4 Procedures

This document will show you how to log on to the RSA self-service console for generating your token code for two-factor authentication, and how to connect to your office PC

Note: Before following this document, it is important to know that a VPN must be requested and approved. If you feel you need a VPN, it must be requested and started through DocuSign from Amanda Colores, Tracy Verrier, and/or Ginny Griffith (at the time of this document).

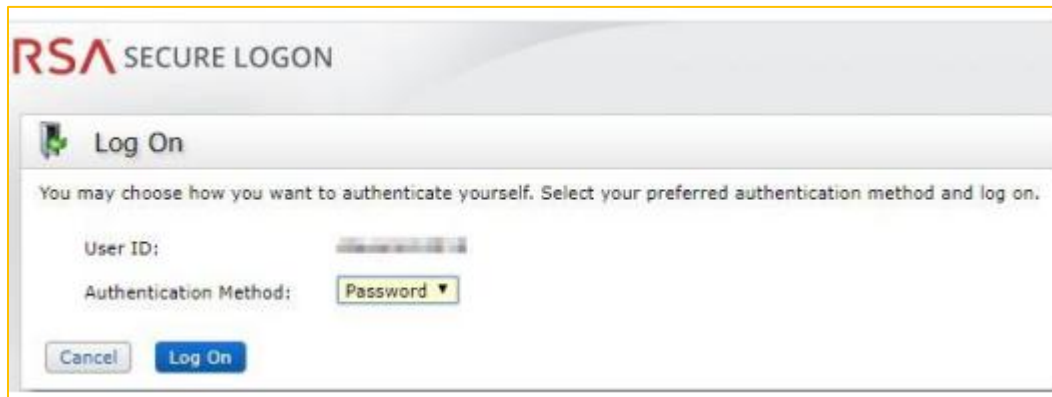
4.1 How to log on to the RSA self-service website

1. Click on the following website: <https://rsa01.faytechcc.edu:7004/console-selfservice/>



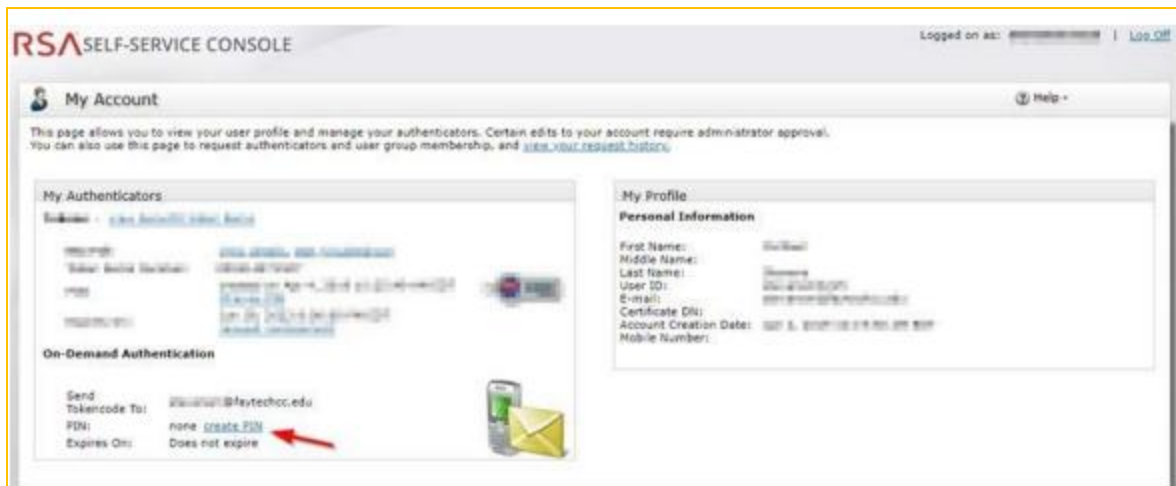
2. Use your AD username and password to log in
 - a. Username1234
 - b. Current Password
 - i. To reset your password, click here: <https://www.faytechcc.edu/its/self-service-password-reset/>

3. After you enter your username and click “ok”, you’ll be prompted with an authentication method. Please leave it set to password and click “Log On.”
 - a. *Note:* If this is your first time logging onto the self-service site, you will have to change your password. Requirements can be found by hovering the mouse over the link to the right.



The image shows the RSA Secure Logon dialog box. At the top, it says "RSA SECURE LOGON". Below that is a "Log On" button with a green checkmark icon. A message states: "You may choose how you want to authenticate yourself. Select your preferred authentication method and log on." There are two input fields: "User ID:" and "Authentication Method:". The "Authentication Method:" dropdown menu is set to "Password". At the bottom, there are "Cancel" and "Log On" buttons.

4. After changing your password, if necessary, you will see the screen below.
5. Please click the link for “create PIN”.



The image shows the RSA Self-Service Console "My Account" page. The page title is "RSA SELF-SERVICE CONSOLE". The user is logged in as "jessica.martinez" and can click "Log Off". The page has a "My Account" header with a "Help" link. A message states: "This page allows you to view your user profile and manage your authenticators. Certain edits to your account require administrator approval. You can also use this page to request authenticators and user group membership, and [view your request history](#)." There are two main sections: "My Authenticators" and "My Profile". The "My Authenticators" section shows a table of authenticators with columns for "Name", "Status", "Type", and "Expires". The "My Profile" section shows "Personal Information" including First Name, Middle Name, Last Name, User ID, E-mail, Certificate ID, Account Creation Date, and Mobile Number. In the "On-Demand Authentication" section, there is a "Send Tokencode To:" field with the email "jessica.martinez@haytechoc.edu". Below that, there is a "PIN:" field with the value "none" and a "create PIN" link with a red arrow pointing to it. The "Expires On:" field shows "Does not expire".

6. Your PIN can be all numbers or a combination. Enter your PIN twice, then click “OK”.
 - a. You’ll be returned to the main page, and you’ll see the green bar at the top stating that you have successfully updated your PIN.



7. You may come back and change your PIN should you ever need to, only if you know what your current PIN is. If you do not remember, please contact the service desk so someone can reset it for you.
8. You may now connect to the VPN. Once you start the login process via the VPN client, you will receive a token code in your email automatically. Access your email account to get your token code and utilize the VPN service.
 - a. *Note:* Token codes are only good for 15 minutes or when used, and not after. If you log out or take longer than 15 minutes to use the code, another will have to be requested from the system. The token code is only part of your password for VPN access.

4.2 Connecting to FTCC VPN

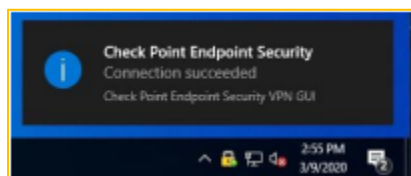
1. On the left end of the taskbar, select the Start icon (or press the Windows logo key on your keyboard), type in "Check Point", and click on "Check Point Endpoint Security VPN" in the Start menu.



- a. NOTE: If at any time you do not see the above screen, please click Start Button -> Check Point -> Check Point Endpoint Security VPN to launch the client.
2. Enter your AD username and the PIN you just created. Then click "Connect".
3. The next screen will ask for a PASSCODE. This will be an 8-digit code that is sent to your email.



4. Next, check your email (you should receive one typically within 1 minute) from RSAadmin@faytechcc.edu with a subject of "On-Demand Token code". Enter that in the "Response" textbox, then click "Connect".
 - a. Note: If you have received multiple emails from RSAadmin@faytechcc.edu, always use the latest email you have received, as the previous codes will be invalid.
5. After a few seconds, you should hear a sound, and a pop-up may occur in the system tray (clock area) notifying you have been connected. Once you have connected with the VPN client, you may now remote to your desktop with the following command.



6. Click on the Start Menu and in the Search box at the top, type:
 - a. "Mstsc.exe /v:w11-xxxxxx.ad.faytechcc.edu"
 - i. Replace xxxxxx with the last 6 numbers of your state ID on your office pc.
 - ii. Note: If your office PC is not turned on, you **will not be able to connect** using Remote Desktop.
7. To end the remote session on your desktop, you can simply click the "X" (appearance will depend on your screen resolution).
- 8.
- 9.



10. To disconnect from VPN, simply right-click on the gold padlock in the system tray (lower right corner of your screen) and click "Disconnect". You can also double-click the padlock, and the screen below will appear; You can click "Disconnect" here as well.



5 Exclusions/exceptions

No approved exceptions exist at this time.

6 Related college documents, forms, and tools

7 Document administration

7.1 Document owner

This document is owned by the Information Technology Services Office, which is responsible for its content and maintenance. For questions or comments, please email help@faytechcc.edu.

7.2 Document review

This document is subject to periodic review to validate that the content remains relevant and up-to-date. Significant or material changes to this document must be submitted to the AVP for ITS

7.3 Version History

Version	Version Date	Author	Reason / Comments
1.0	3/9/2020	PLS	Document origination
1.1	3/9/2020	MS	Change section 4
2.0	7/1/2023	MW	Formatting update
3.0	10/29/2025	L. Clark	Formatting, font, and naming convention changes
5.0	Click or tap to enter a date.		

7.4 Approval History

Version	Version Date	Name	Title
1.0	3/9/2020	P. Scully	AVP for MIS
1.1	3/9/2020	P. Scully	AVP for MIS
2.0	7/1/2023	T. Prevatte	AVP for ITS
3.0	10/29/2025	T. Prevatte	AVP for ITS
5.0	Click or tap to enter a date.		