VIRGINIA IT AGENCY

MAINFRAME ACCESS COORDINATOR RESPONSIBILITIES

Purpose and Description of the Process	This document supports the VITA oversight of Agencies' Mainframe Access Coordinator responsibilities.
Stakeholders Impacted by the Process	This process applies to all Commonwealth of Virginia agencies, departments, Localities and federal departments.
Rationale for Process (Law, policy, program, function it supports, etc.)	This process provides direction for VITA mainframe connectivity to Commonwealth of Virginia agencies, departments, Localities and federal departments.
Related Processes and Sub-Processes	This process is related to the following: • Contact of applicable COV Agency to initiate Use Agreement, or MOU for customer contacts with DMV or VEC for application access • • Logon ID Request (Form VITA 003-01) – IBM Mainframe instructions • COV Network Access form • VITA network access request form instructions • Legacy Applications Assessment Service Instructions • Comprehensive Services Credit/Change Request instructions
Forms Used By Process	This process may use the following forms: • Service Account Request to create, modify or disable a service account. • Onboarding Employee/Contractor to request a new COV account or to on-board a new COV user who requires a COV domain account. A COV domain account is required to log on to the COV domain. Each person who uses a computer on the COV domain receives his or her own unique account and user name. This account can then be assigned access to resources within the domain. Applies to VITA Executive Agencies (In-Scope) only.

	• Update Existing COV Account to change account information • Mainframe Access Coordinator (MAC): to submit new or update mainframe Access Coordinator appointees • Network Access Form to request COV network access through the firewall security team to connect to the mainframe • Billing Account Request Form to establish a billing account • Mainframe Services User ID Account Number to request an account number • Logon ID Request (Form VITA 003-01) – IBM Mainframe to request a LogonID for access to the mainframe and to add/delete/change LogonID(s) • Mainframe Service Billing Contact Change to request a change of the agency point of contact for mainframe service billing • COV Security Group Request to request new security groups or make changes to an existing security group. • Extend Existing COV Account to extend or renew COV accounts • Offboarding Employee/Contractor to off-board an employee or contractor • Okta Authentication to update user information related to Okta application access • Re-Enable Existing COV Account to re-enable COV accounts that are currently disabled • Temporary Disable COV Account temporarily disable a COV account in active directory (AD)
Process Compliant with VITA Records Management Policy?	Yes

Process Owner Name	Mike Shaffer	**Process Owner Directorate/ Division**	Technical Services Delivery Manager / Enterprise Technology Services and Solutions (ETSS)

VERSION HISTORY

Version	Date	Author(s)	Change Summary
V1.0		Arthur Midgette	

GLOSSARY	
	Definition
Access Coordinator	An individual that has been delegated the authority via the Access Coordinator Request form to administer mainframe access requests. The Access Coordinator has responsibility to manage all users and LogonIDs assigned to the agency, locality or department. The Access Coordinator submits updates (add, change, delete) of users to VITA. In some cases this term can also reference the Mainframe Access Coordinator, Information Security Coordinator and ACF2 officer
Access Coordinator List	The master list of approved Access Coordinators. This list is used to verify an individuals' delegated authority to sign off on access requests for specified locations.
Access Request	The annually renewed agreement between Virginia Employment Commission (VEC) and the locality for access to VEC mainframe functions.
ACF2	Access Control Facility 2. Access control software security system for the mainframe operating system.
Agency Commissioner	Chief Executive of an Agency will submit authority to VCCC to proceed with Access Coordinator Change Form.
AITR	Agency Information Technology resource
Billing contact	The individual and address receiving the monthly bill from VITA for payment of the mainframe access account. Changes to the billing contact person or address should be reported to VITA, as needed.
Customer	In this process, a Customer is a Commonwealth of Virginia Agency who is requesting the use of Mainframe services.
ISO	Information Security Officer
LogonID	The LogonID is a users' logon account, a minimum of 6 character designator. The first three characters is the "3 letter designator" Identifying the billing customer (assigned by VITA). The last three letters are the users' personal designator, generally the user's name initials. Localities can designate additional characters between the "3 letter designator" and the user's personal designator to further characterize user functions, if desired.
MOU	Memorandum of Understanding. The annually renewed agreement between Virginia Department of Social Services (DSS) and a mainframe customer for access to DSS mainframe functions

Out of scope entity	VITA supports executive level agencies and other agency departments eligible for VITA services. Localities, nonexecutive state agencies and departments, and federal departments are considered out of scope but may use state level services as administered or hosted by VITA.
3 Letter designator	The designator for a locality, or department as provided by VITA and is identified as the ACF2/UID1. This identifies the specific billing account and the first three letters in the LogonID. For example, Accomack County is "ACC." This will only be alpha characters. This is designated and provided by VITA Billing
TSO	Time Sharing Option: Allows for authorized Mainframe Access Coordinators to perform basic user management functions (e.g. reset passwords)
Use agreement	The annually renewed agreement between Virginia Department of Motor Vehicles (DMV) and the locality for accesso a DMV mainframe function.
VITA Customer Care Center (VCCC)	The helpdesk for COV access and technology issues and mainframe access.
VPN	Virtual Private Network
Additional Terms	For additional terms, see the IT Governance Glossary

Access Coordinator (AC) Responsibilities

- Be familiar with the various forms that will have to be completed for system access indicated in the 'Forms Used By Process' section of this document. Depending on the application, multiple forms may have to be completed for VITA and the owning agency before access is granted.
- Establish system access for users. System users are defined to Access Control Facility (ACF2) by creating a unique LOGON-ID record. The AC will complete the VITA03-001: Logon Request Form. Fill out the form completely for each individual user, sign form authorizing requested access.
- Serve as first level contact for security or access problems. User access problems should be routed through the Access Coordinator. The Access Coordinator should direct questions and other service issues to the VITA Locality and Out-of-Scope Agency CAM (Customer Account Manager).

Privilege Management (Optional TSO Management)

- Mainframe Access Coordinators have the option as TSO management privileges to manage users within their department (all users with same 3-character designator) or to use the VCCC for user management. Using VCCC is subject to helpdesk availability and delays, while a TSO enabled account allows for instant self-service to users. TSO enable account is requested through the VITA03-001: Logon Request Form.

- Ensure all newly created accounts have the least amount of privilege needed to operate
- Ensure account owners determine boundaries between accounts owned by Commonwealth agencies and accounts owned by the mainframe service tower supplier
- Contact VITA's Help Desk at (804) 786-3932 or 1-800-533-1659 to report problems with system access or with the ACF2 security product. Note that Application problems or functionality should be addressed to the owning agency
- Encourage localities or agencies to use the VCCC help desk for password reset and continue to remove accounts to reduce the total number of users with elevated privileges
- Be knowledgeable of password requirements and reset passwords for users
- Be knowledgeable of remote/VPN (Virtual Private Network) access requirements
- Suspend logon-ids of resigning/terminated employees
- Un-suspend logon-id of new users
- Establish a data base or file which would identify the logon-ids associated to each user. (Since there are multiple applications, an individual can be assigned several different logon-ids.)

User Logon-ids and Passwords

- Each user in a system protected by ACF2 is assigned a unique system identifier called a logon-id. Each logon-id is protected by a password known only to the user. At logon time, a user must enter both the logon-id and a password to gain access to the system.
- All new ACF2 logon-ids are suspended when they are first established. It is the responsibility of the AC to un-suspend the new logon-id before the user can access the system.
- Passwords are not predefined by VITA; the system will accept characters the user enters on the password line as a valid password. See "Choosing Passwords", below, for the required password rules and convention. VITA recommends selecting a set of characters for your password that is unique but easily remembered. Possible suggestions are replacing a number for a letter in a word, or using some kind of code. Passwords must be properly protected, known only to the owner of the logon id and not revealed to others, through conscious sharing or carelessness.
- Users must change their passwords every 30 days. After 90 days of inactivity the account is automatically suspended. ACF2 will require the end user to enter a new password once the 90 days has been exceeded. When a password expires, ACF2 requires verification of the new password by requiring the user to enter the new password twice.
- After 3 invalid logon/password attempts, the logon-id will be suspended due to password violations. The user will be unable to access the system or any other system

controlled by the same ACF2 logon-id record. The designated AC must reset the user's password, providing a temporary password in order to re-establish system access. As part of the sign-on process, after the user enters the temporary password, they will immediately be prompted for a new password that is unknown to the AC.

- If a user is leaving an agency/locality, suspend the logon-id and then submit the VITA03-001: Logon Request Form to VITA for deletion of the logon-id record.

Choosing Passwords

Users access several systems, some of which may be internal to the organization such as a Local Area Network (LAN) and some of which are external to the enterprise, such as the Virginia Information Technologies Agency (VITA) mainframe computer applications. For security and accounting purposes, each user must identify themselves to each system by inputting a logon-id and password for validation before access is granted.

Passwords

- are 6 to 8 characters in length
- are alpha/numeric
- have at least one number
- it is recommended that passwords have no special characters and no spaces

Remote Virtual Private Network (VPN) Access (VITA In-Scope Agency only)

- VPN is a network that uses the internet to transfer information using secure methods
- VPN allows users to connect to a pre-approved agency's network remotely as if the user were in the office
- The Multi-factor Authentication (MFA) Token request form is located on the VITA Service Catalog under Account Management and VPN
- For information regarding tokens and VPN access, visit the VITA service portal and navigate to the following knowledge base articles for more information
  - How to Create PIN for Soft Tokens
  - How to Activate RSA Soft Tokens
  - How to Activate Mobile RSA Soft Tokens
  - How to Activate Your VPN (and create your PIN)

VPN Options and Functions

	Dual-Factor VPN	Single Sign-on VPN
Approval Required?	Yes	Yes
Token Required?	Yes	No

	Dual-Factor VPN	Single Sign-on VPN
How is Access Granted?	RSA Token is purchased by the agency Procurement Coordinator and Account Administration creates the account and sends the token to the user. COV account is modified to have VPN access.	After AITR, ISO, or ISO Designee completes the COV Account Request Form, Account Administration completes the request and notifies the user.
Are the Credentials Related to the COV Account?	No, these are separate accounts	Yes, both use the COV username/password
Software Required?	Yes, Cisco VPN Client will be installed after a request to VCCC is made.	Yes, Cisco VPN Client will be installed after a request to VCCC is made.
Can Access Be Modified?	Yes, usernames, tokens, etc., are modifiable through VCCC with proper approval	Yes, usernames are modifiable through VCCC with proper approval.
Can Access Be Deleted?	Yes, an approver will send the request via the COV Account Request Form and AAO will complete the request and notify the requestor.	Yes, an approver will send the request via the COV Account Request Form and AAO will complete the request and notify the requestor.
What Do I Do With an Unused Token?		Tokens are purchased by the agency and are not required to be turned in to the VCCC or AAO.
Can Unused Tokens Be Reassigned?		Yes, an agency approver will e-mail the request to VCCC; AAO will reassign the token, and notify the requestor.

Tools and applications that do not require VPN (VITA In-Scope Agency only)

A VPN connection is not required to use Gmail, Google Calendar, other Google Apps, Cardinal, SharePoint and other Microsoft Office 365 applications. VPN is only necessary when accessing file shares at your agency and other tools that are not accessible via the internet.

Contact commonwealthsecurity@vita.virginia.gov if you have questions.

To access the IBM mainframe computer

Each agency (or locality) must have:

1. Agency, and locality if requesting user account(s)
2. A billing account at VITA
3. A VITA logon id

4. Encrypted TN3270 emulator client software installed on the users' personal computers with TLS 1.2 and higher capability. See appendix A for Emulator tools (Most common in green)
5. A secure connection either over the internet or data circuit to the state data center

The steps to take with VITA in sequential order before an agency can connect for access to the IBM Mainframe:

1. Ensure the requestor has established a Use Agreement, Memorandum of Understanding (MOU), or Access Request with the appropriate agency. Before requesting access to the VITA mainframe, the owning agency (DMV, VEC, DSS) must authorize access to the agency applications and databases resident on the mainframe. Once authorized, the agency will direct the new customer to VITA for further account, network, and log-on processing. Contact the AITR and ISO at the agency that owns the application(s) for the Use Agreement, MOU or Access Request process.
2. Open a billing account with VITA if one does not exist. A billing account number is required for VITA logon requests as the 3 letter designator. If the requestor is not an existing VITA customer, a new account request form can be found at: Mainframe Services User ID Account Number.
3. Once cleared by the agency and VITA billing, establish new organization accounts and identify the primary mainframe access coordinator(s). The VITA billing office will work to assist upon receipt of the Billing Account Request Form.
4. Submit the Mainframe Access Coordinator form to the VCCC. This form verifies the organizations named mainframe access coordinators. VITA recommends two MACs per organization. The names and contact information will be entered in the mainframe database.
5. Once these items are complete, the new organization is ready to proceed to Commonwealth of Virginia (COV) network access and establish mainframe Logon ID's for mainframe access coordinator(s)
6. For non-VITA Agencies (Localities, Federal or other state departments) Submit the Network Access Form to VCCC to allow the customer's public IP address through the COV firewall, through the COV network and to the VITA mainframe. For VITA customer Agencies on the COV network, access to the mainframe is available without a Network Access Form.
7. Ensure each user with the new customer has purchased and installed a TN3270 emulator software package for each user's computer in their organization. Software suggestions are provided in Appendix A. Configuration requirements are provided further in this document.
8. Once network connectivity and emulator is configured successfully, a user should be able to view the mainframe "splash screen."

9. The Access Coordinator, or designee, will be the first individual to establish a mainframe logon and verify agency database access as all future users for the organization will be modeled from the AC permissions. Online instructions are provided for the VITA03-001: Logon Request Form.
10. AC's are not required to perform the initial or test mainframe access and can designate a "test" user.
    a. AC's can opt for Time Sharing Option system (TSO). Only an AC can have TSO access. Localities are not encouraged to have TSO (elevated privileges).
    b. In order to issue ACF2 commands, you must access TSO. Accessing TSO provides the capability of issuing ACF2 commands in an online environment.
    c. TSO allows a number of users to execute programs concurrently and to interact with the programs while they are executing.
    d. TSO access allows AC's to reset passwords of organization users. Otherwise the service desk can perform password resets.
11. Once connected, verify the databases operate as expected. Contact the owning agency (DMV, VEC, DSS) AITR and ISO for instructions and guidance for accessing data or navigating mainframe screens.
12. Recommendations for authenticating mainframe access and setting password:
    a. Have 30 minutes available to complete authentication and access process
    b. Open the emulator to the "splash screen" before calling the VCCC
    c. Have the six-digit logon ID ready, as provided from VITA 03-001 form
    d. VCCC phone number (866) 637-8482. Recommended call time after 10am
    e. VCCC will authenticate you using name, phone, address, and/or organization
    f. VCCC will provide a temporary password
    g. User will sign onto mainframe while on the phone with VCCC
    h. VCCC will verify the user is signed onto the mainframe and active
    i. User changes temporary password to new password and re-accesses the mainframe

Defining Users to ACF2: Add/Modify/Delete Users

System users are defined to ACF2 by creating a unique ACF2 LOGONID record. A logon id record defines each system user in terms of general identification, status, privileges, access history, attributes related to TSO, CICS, violation statistics, and so forth.

The AC must will complete the 'VITA03-001: Logon Request Form on behalf of the user to:

- create a logon for a new user
- update or modify an existing user's logon id
- Delete a logon for a retiring or terminated user.

- An AC cannot submit a VITA03-001 for him or herself. Another MAC in the same organization must submit a form on the other MAC's behalf.

Based on the information supplied on the form, VITA will process the system access request.

User access problems and requests should be routed through the agency, or locality Access Coordinator. VITA will accept help-desk tickets, logon ID request forms, questions and problems from the designated Access Coordinator. The Access Coordinator should contact VITA's Help Desk to report problems with system access.

Access Issues and support

Typical access issues

- **User cannot log-on to the mainframe**
  - The user's DMV Use Agreement may have expired (one year agreement)
    - Contact DMV first to verify the user has not been locked out
    - Access coordinator may have to re-submit use agreement renewal to DMV
  - User's account may have been suspended due to in-activity (90 days)
    - Contact the VITA VCCC to unlock the account or
    - The AC can unlock / change password (if AC has TSO access)
- **User(s) cannot view the VITA mainframe splash screen**
  - If all users in the same locality have same problem, there is a local network, internet, VITA network or VITA mainframe problem
    - Contact your local network/IT support to ensure the local network is operating and internet access is active
    - Check your internet access by attempting to reach a website (Google: https://vita.virginia.gov), if you get to this website, the local internet access is good.
    - Check firewall rules to ensure all locality user traffic is exiting via the public IP
    - Organization's public IP has changed due to an unreported ISP change or a local firewall / network change has changed the public IP
  - If one user in an organization cannot connect (some can, others can't).
    - User should check emulator software settings with a user that is working.
    - User should contact local IT support as there might be a problem with their computer firewall, IP assignment, or other local issue.
  - If none of the above has occurred and internet access is confirmed, there may be an interruption from the VITA firewall or mainframe is down. Contact the Help Desk for additional information and guidance.

Network Access to the VITA Mainframe

Connection issues

- First, users should reach out the local access coordinator or local IT for help to ensure there isn't a local network issue (firewall problem or internet service may be down). If all users are having the same problem, note that to local IT person.
- If no local general issue exists and still having a connection problem, verify your emulator settings with the local IT or access coordinator.
- Contact your ISP to ensure you internet connection is still active or there are no outages in the area (cable cuts, downed trees, etc.)
- Contact the VCCC by phone or email and enter a ticket. Provide the VCCC helpdesk with the following data to allow the mainframe and network engineering to troubleshoot your problem:
  - Be specific (e.g. "I cannot reach the VITA/DMV/VEC mainframe logon page" or "I can reach the VITA mainframe page, but I cannot log on and access the DMV / VEC system")
  - Your public IP address from your location and local users IP
  - A phone number and email address where you can be reached
  - Is it just you or is the entire office having the same problem? When did the problem start to occur?
  - Your emulator tool name and settings (e.g. hostname IP, Port, Security setting)

Internet Service Provider Changes

One of the most common issues that will interrupt connections is the locality changing the Internet Service Provider (ISP)

- Submit the VCCC ticket **"3 WEEKS"** before the current IP is going to be removed. Please don't wait until the day-of or day-before, otherwise, you will experience an outage for a few days while VITA attempts to accelerate the process.
- Submit a VCCC ticket indicating the locality is changing the ISP. Use the Network Access Request form. Provide your current IP, new IP, and why the IP is changing so the Agency ISO (Agency Security) and CRSM (VITA Security) is aware you are an existing customer changing IPs, not a new customer (longer review time).
- VITA can keep both old and new IP's active during your transition to avoid an outage.

Network Access to the VITA Mainframe: Emulators

- TN3270 Emulator
  - Each individual user with a LogonID will need a secure-capable TN3270 Emulator installed on their workstation/laptop.
- Emulator Minimum Requirements

- TN3270 Emulation, Secure Port 992 compatible, Security crypto/encryption is TLSv1.2 compatible, supports multiple firewalls
- Generally, any version after 2014 meets the minimum requirements
- Avoid emulators that require peer-to-peer SSL security certificates, VITA does not support client to mainframe security certificates.
- See Appendix A for software suggestions.

Mainframe network access: TN3270 emulator local setup

- User Emulator Software Setup
  - Ensure you have confirmation that your local network setup and VITA network access is completed (see Local network changes section, below)
  - Mainframe IP or Host name: 166.67.70.224
  - Port: 992 / secure telnet
  - Security: TLSv1.2 and 256-bit encryption
  - All emulators purchased or upgraded since 2014 generally do support TLSv1.2
  - In some cases, a modern emulator may have a TLS or TLS1 option, which generally means it supports up to and including TLSv1.2
  - If these setups are in place and you cannot get the VITA mainframe "splash screen," please contact the VITA locality customer liaison for additional guidance

Local network changes for TN3270 emulator

- The locality's local network must be set up to allow connectivity to the VITA network
  - Local firewall must allow Port 992 bidirectionally
  - Port 992 is the secure telnet protocol accepted by the VITA network and mainframe. Generally, firewalls are not defaulted to allow this port and must be set up.
  - Direct all Port 992 activity outbound through the local public IP
  - This will be the same IP as provided on the VITA Network Access Worksheet
  - The local router and/or firewall must have this set up to ensure Port 992 traffic inside the locality is pointed to go out through the internet on the public IP

Local AS400 setup

- The AS400 operating system must be versions 7.0 or above for TLSv1.2 compliance.
- The secure connection is established and managed by the local AS400 and the VITA Mainframe. The emulator software on the user's computers behind the local AS400 does not need to have secure configuration.
- Contact your AS400 service provider for additional information. Most are aware of the VITA connectivity and security requirements and can direct your configurations to be compliant to TLSv1.2 requirements.

- Localities can migrate from AS400 connection to a direct mainframe connection. See "Local Network Changes" and "Emulator Local Setup" sections above.

Security Restrictions

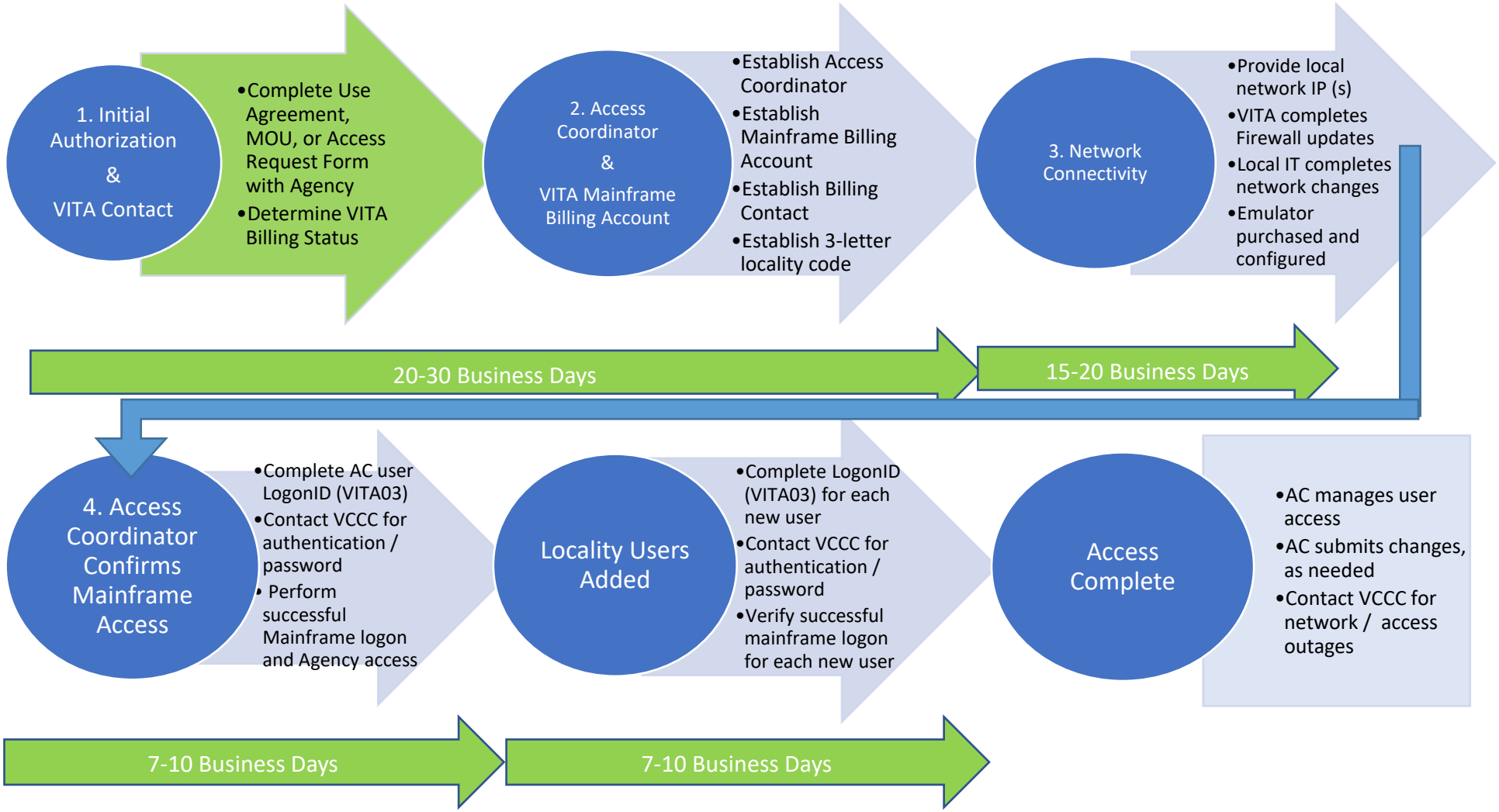
Security restrictions were enacted that will/may cause connections to fail. What to check for:

- TN3270 Emulators (e.g. Jolly Green, Mocha, etc.)
  - Set to TLSv1.2 and do they support TLS Version 1.2? ***AND***
  - The Port setting to secure port 992 telnet OR 990 ftp? ***AND***
  - Is the Mainframe IP or Host Name set to:
    - 166.67.70.223 or .224 (telnet) ***OR non-VITA customers***
    - 166.67.65.11 or 12 (file transfer-ftp) ***OR non-VITA customers***
    - s0121.vita.virgina.gov or s0221.vita.virginia.gov (VITA customers)
  - If different than these settings, please contact the VITA locality customer liaison immediately (customeraccountmanager@vita.virginia.gov)for instructions / verification
- How old is your TN3270 Emulator or FTP tool applications?
  - If purchased five or more years ago (pre-2015) or not updated five or more years ago, it probably does not meet the TLSv1.2 encryption and secure port requirements.
- Is your Mainframe Access Coordinator (MAC) list current? Are there identified MAC's that have since left your organization that may still be associated to your account?

If you are not sure or need additional information –please contact the VITA locality customer liaison.

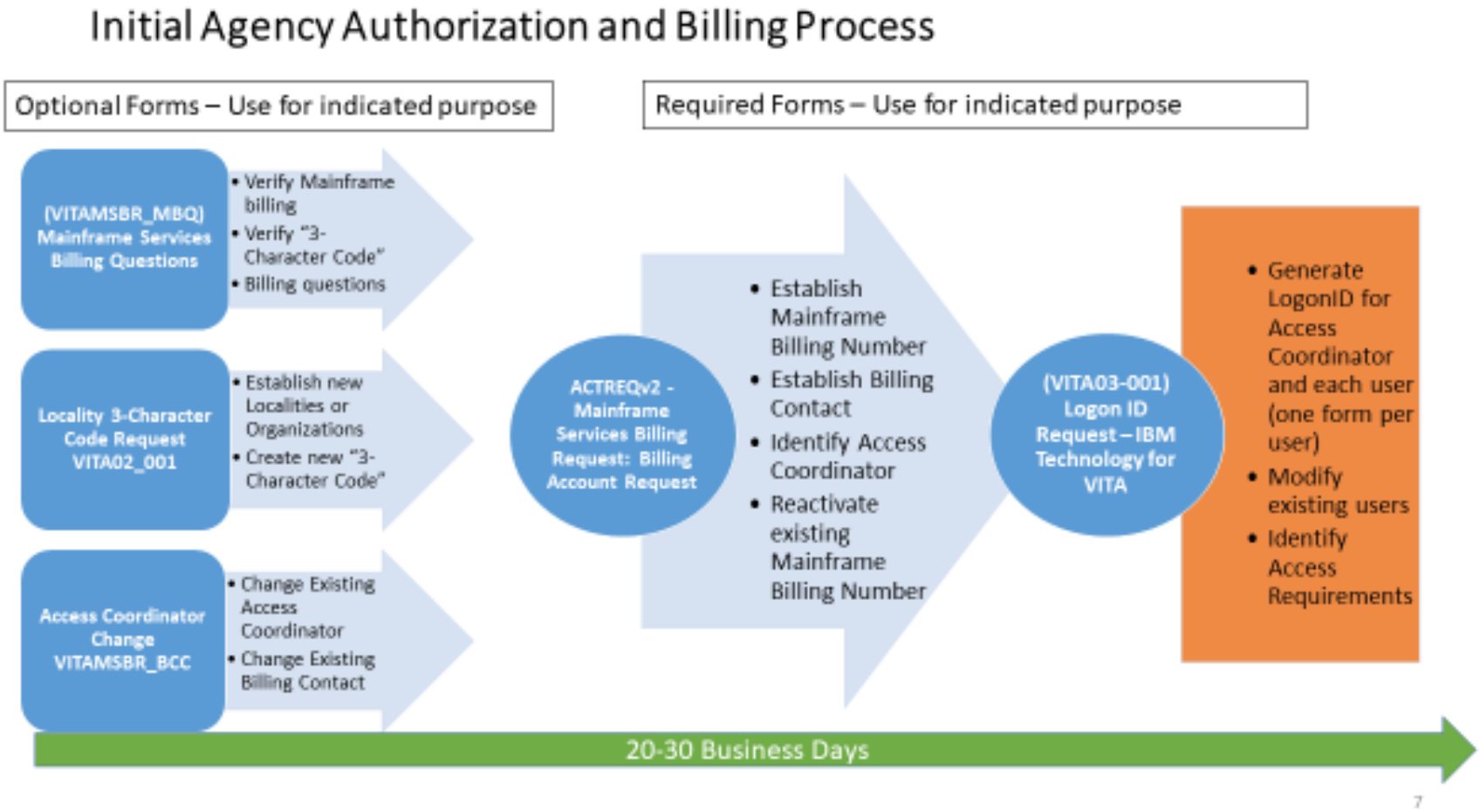
Mainframe Access Instructions

PROCESS OVERVIEW DIAGRAM



Access Coordinator Responsibilities

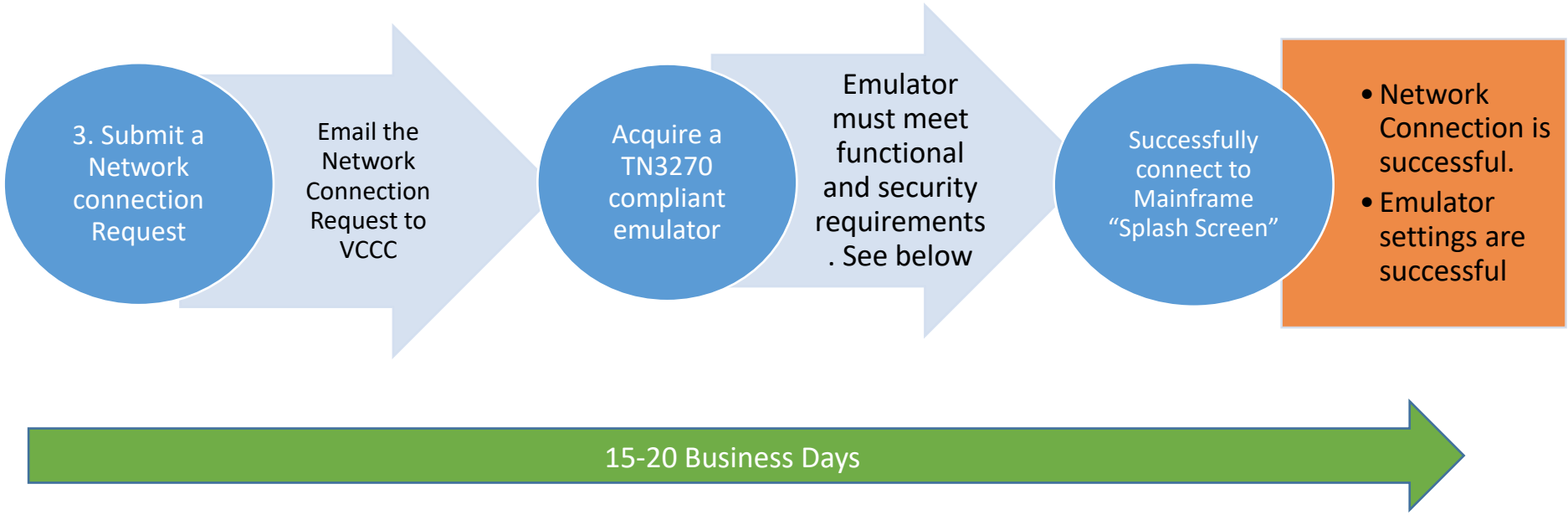
PROCESS FLOW



Access Coordinator Responsibilities

PROCESS FLOW

Network Connectivity to the Mainframe



Access Coordinator Responsibilities

PROCESS FLOW

Network Connection Request to the Mainframe: VITA Mainframe Access Worksheet Instructions

- Copy and paste the entire worksheet **(next page)** into the body of an email
- Fill in the Highlighted Yellow entries
- In the email To: enter the following email recipients
  - vccc@vita.virginia.gov
  - customeraccountmanagers@vita.virginia.gov

- You will receive a VCCC Ticket number, provide that number to the CAM and mainframe services owner via email to help with tracking and to answer any questions or issues from the network / security teams.

PROCESS FLOW

Network Connection Request to the VITA Mainframe: VITA Mainframe Access Worksheet

<Name of county/city/organization> requests access to the IBM mainframe at the Commonwealth Enterprise Solution Center (CESC) from the internet using encrypted TN3270 software. As information Security Officer (ISO) or Locality Mainframe Access Coordinator for <Name of county/city/organization> I hereby request assistance and coordination necessary for the creation of the connection. The request is in the form of a Service Request. Please include the following information in the Service Request.

VCCC Helpdesk – Assign Service Request to “Network-FW-TIER-II” Action: Add FW rule NAT to the secure public internet portal as indicated below:

- New Customer Source IP: <Current Source IP> Provided by Requestor
- Destination DNS or IP: s0221.vita.virginia.gov
- Mainframe LPAR: SYS2
- Mainframe TCP Stack Name/IP Address: SYSTCP2B
- VITA Public IP (Secure FTP): 166.67.70.224
- Protocol: Secure TN3270, Port 992

The local technical point of contact for questions, coordinating implementation and testing:

- Name: <Enter name>
- Email: <Enter email address>
- Phone: <Enter preferred telephone number>

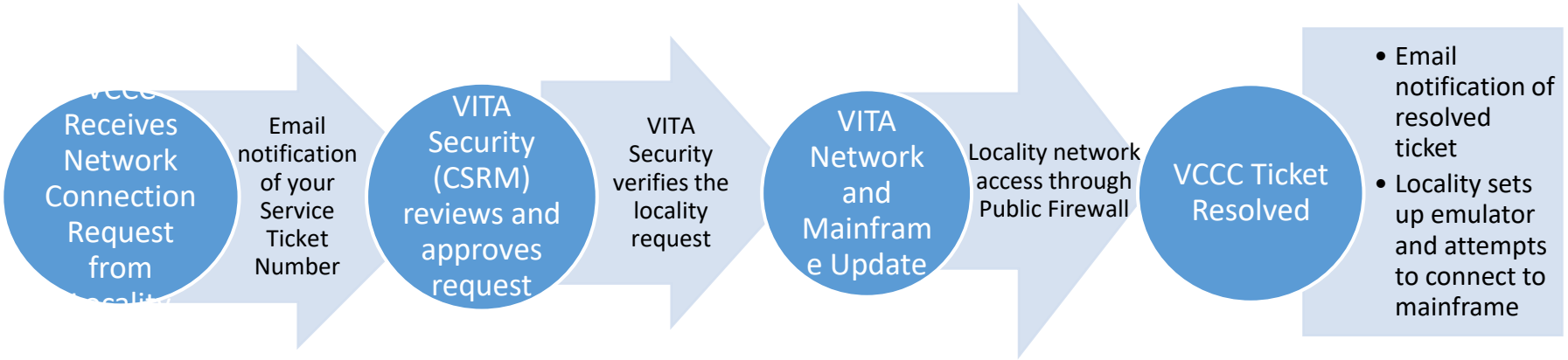
Tips on acquiring emulator:

- Most have a free 30-day trial downloadable without purchase. Wait until the Network Connection Request is complete before downloading trial.
- Try out a couple different types before purchasing. Some are more user-friendly than other.
- High cost does not mean better performing, we've found the lower cost emulators perform just as well or better.

Emulator tools (Most common in green)		
Product Name	**Vendor**	**URL**
Mocha TN3270	Mochasoft	http://www.mochasoft.dk/tn3270vista.htm
QWS3270 Secure	Jolly Giant Software	http://www.jollygiant.com/qws3270-secure/
Bluezone TN3270	Rocket Bluezone Software Corp	http://www.rocketsoftware.com/products/rocket-bluezone-terminal-emulation
Reflection Desktop (formerly Attachmate)	Micro Focus Corp	https://www.microfocus.com/products/reflection/
TN3270 Plus V4.x	SDI Group	http://sdisw.com/

PROCESS FLOW

Network Access to the VITA Mainframe: VITA Network Access Processing



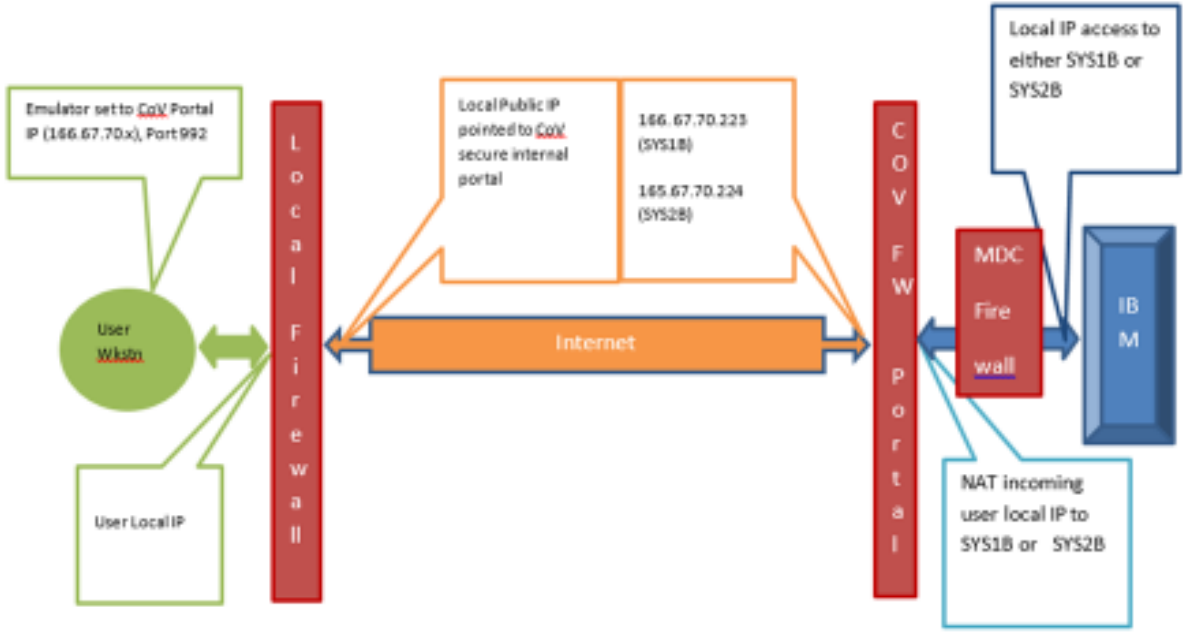
Tips on VITA network access processing:

- Notify your CAM of the ticket number provided for tracking. If the ticket is not resolved in two weeks, contact CAM for status and help.
- CSRM may contact the Access Coordinator or Information Security Officer network access request for security verification.
- The local IP provided must be a full IP. Subnet IP's (e.g. 123.456.0/24) are not permitted
- Contact the Mainframe Service Owner for technical help or questions.

PROCESS FLOW

Mainframe Network Access Process: Network Access

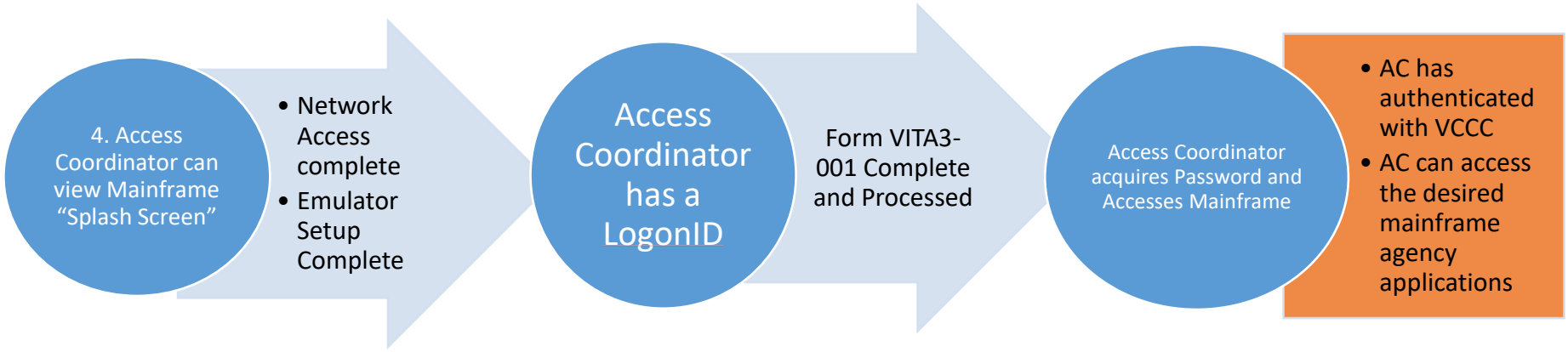
This section describes the mainframe network access from the locality through the internet to the mainframe. This is a typical network map of the network connection from the locality to the VITA Mainframe.



12

PROCESS FLOW

Network Connectivity to the Mainframe: Confirming Mainframe Access

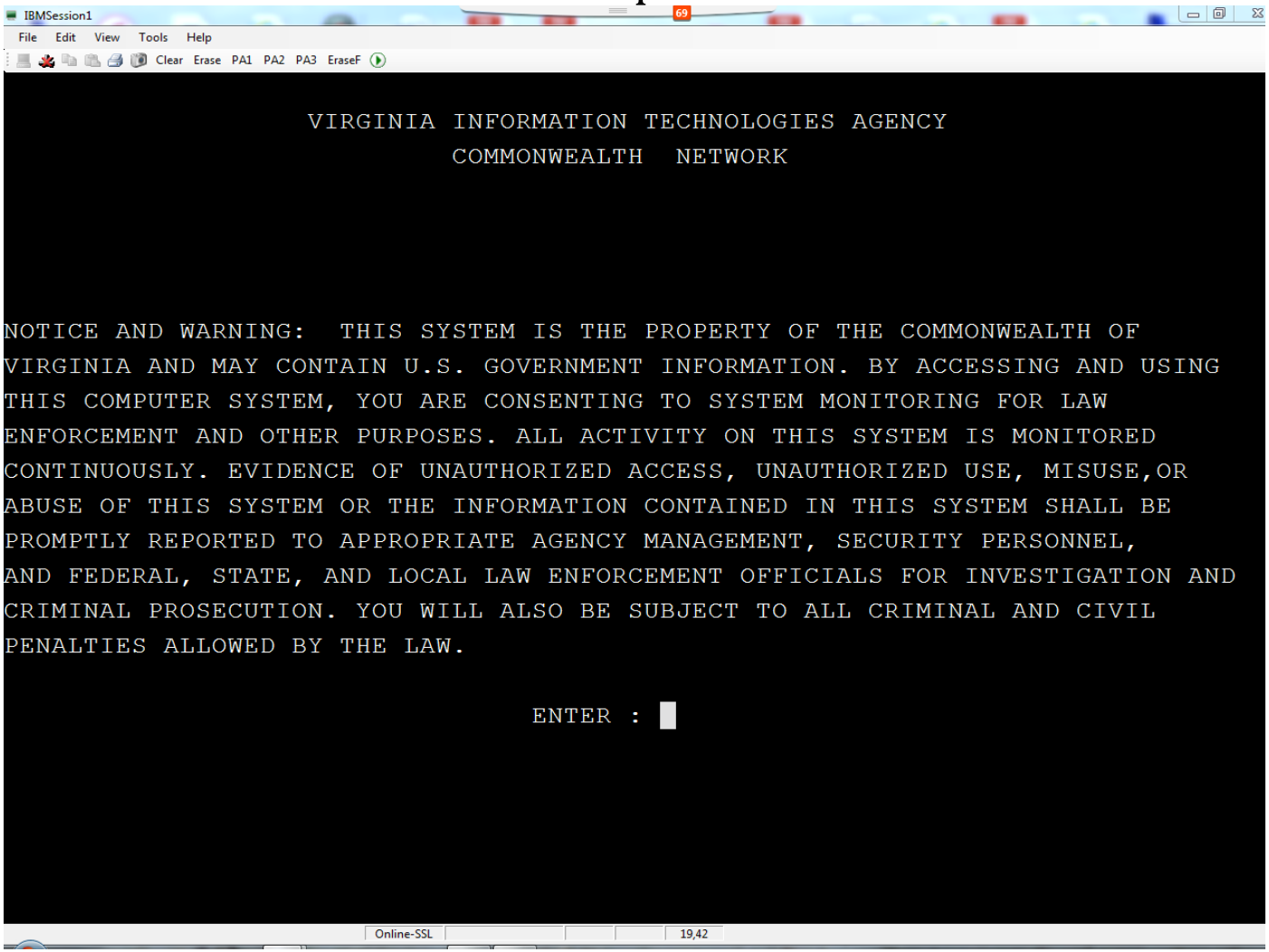


Tips on final VCCC Authentication:

- 30 minutes free to complete authentication and access process
- User is on the mainframe "Splash Screen" before calling the VCCC
- VCCC phone number (866) 637-8482
- VCCC will provide a temporary password
- User sign onto mainframe to verify access while on the phone with VCCC
- User changes temporary password to new password and re-accesses the mainframe

PROCESS FLOW

Mainframe “Splash Screen”



Appendix A

VITA network access request form instructions

Purpose:

The VITA network access request form is used for Commonwealth of Virginia (COV) localities, government departments, authorized vendors and non-executive branch agencies to request access through the COV network to access the Dept. of Motor Vehicles (DMV), Virginia Employment Commission (VEC), and Dept. of Social Services (DSS) applications on the VITA mainframe.

Customers should already have a mainframe identifier (3-letter identifier), a current VITA mainframe account and assigned mainframe access coordinator(s).

Only the localities information security officer (ISO), IT manager or approved mainframe access coordinator (MAC) may submit this request.

Instructions:

1) Download the VITA network access request form
2) Locate the type of access required in bold (see below)
3) Complete the form, as shown
4) Email the form to the VITA Customer Care Center (VCCC), as shown

1. How to download the VITA network access request form:

- Click or copy this link into your internet browser: https://www.vita.virginia.gov/media/vitavirginiagov/services/docs/MainframeAccess-FirewallRuleRequest-Localities.xlsx
- Open the document in Microsoft Excel
- Select the "Firewall Requested" tab

2a. Request DMV and VEC mainframe access via the VITA internet secure portal:

Enter the requester's source public IP address in the YELLOW cells. Customers may have a primary and secondary (backup) public IP.

Access requested	Firewall / Portal IP	Source DNS name (Optional)	Source public IP address
DMV mainframe (Primary)	166.67.70.224		
DMV mainframe (Secondary)	166.67.70.224		

Access requested	Firewall / Portal IP	Source DNS name (Optional)	Source public IP address
VEC mainframe (Primary)	166.67.70.224		
VEC mainframe (Secondary)	166.67.70.224		

Note: Only four-octet IPs (123.456.789.123/32) and three-octet (123.456.789.0/24) with 24-bit masks are permissible.

2b. Request DOA/CIPPS mainframe access via the VITA internet secure portal:

For DOA CIPPS access: Enter the requester's source public IP Address in the YELLOW cells. Customers may have a primary and secondary (backup) public IP.

Access requested	Firewall / Portal IP	Source DNS name (Optional)	Source public IP address
DOA/CIPPS (Telnet) DOA/CIPPS (FTP)	166.67.70.223 166.67.65.11		

Note: Only four-octet IPs (123.456.789.123/32) and three-octet (123.456.789.0/24) with 24-bit masks are permissible.

2c. Internet supplier provider (ISP) change instructions:

- Enter the current IP that is to be removed in the "Current Public (Primary) or (Secondary) YELLOW cell
- Enter the new IP replacing the existing in the "New Public IP" cell

Access Requested	Firewall / Portal IP	Source DNS name (Optional)	Source public IP address
ISP change	**Current Public IP**		**New Public IP**

Note: If you do not want the current IP to be turned off right away, especially if the organization is migrating users over time, do not use this section. Use section 2a. or 2b. to add your new ISP IP(s).

After migration to the new IP is complete or the current IP is inactive, please submit a second "mainframe access firewall rule request template form" to remove the retired public IP, per example below.

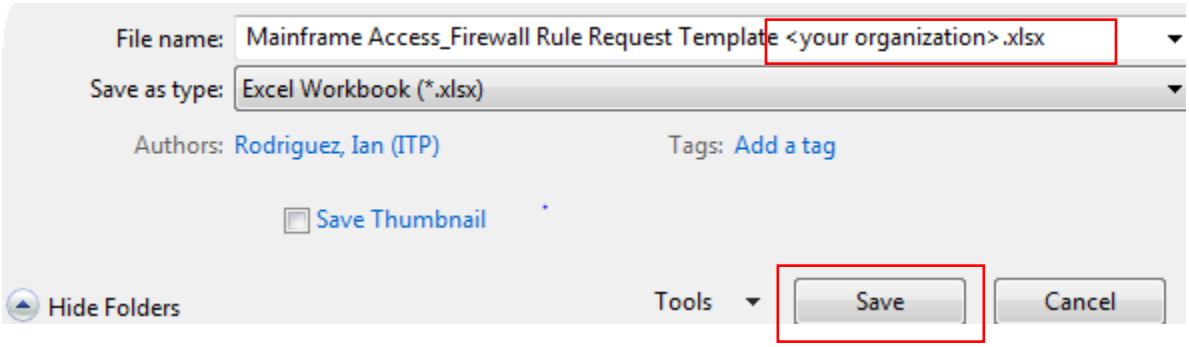
Access requested	Firewall / Portal IP	Source DNS name (Optional)	Source public IP address
ISP change	**Current Public IP** xxx.xxx.xxx.xxx (remove)		**New Public IP**

3a. Enter local contact information in the event the firewall team needs additional or clarification of entered information.

Contact information of requester	
Name:	
Locality name:	
Position:	
Phone:	
Email:	

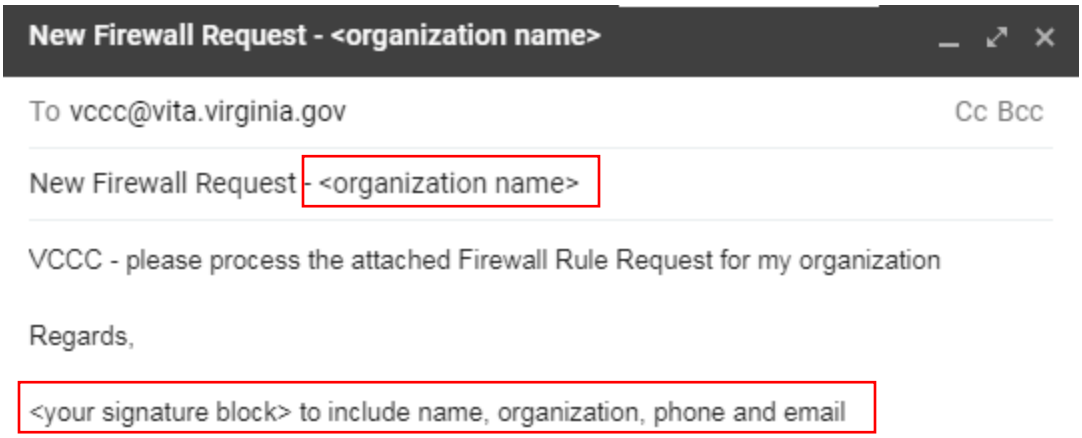
Note: The VITA and requested DMV/VEC Chief Information Security Officers (CISO) office may contact the requester to verify the network access request.

3b. Perform a "save as" and save request to your local computer.



4. Email the request to the VITA Customer Care Center (VCCC).

Fill out an email from your organizations email service, per example below:



Send email with attachment.

You will receive an email response from the VCCC that your email was received. You may receive a service ticket number - CALLnnnnnn and/or REQnnnnnnnn.

When resolved, you may receive a response that REQnnnnnnnn is **Resolved**. The request is expected to be complete within 10 business days, which includes VITA and agency CISO approval plus firewall engineering team fulfillment.

For questions or status, especially after 10 business days has passed, please call the VCCC at (866) 637-8482. Please have your CALL or REQ number to reference.

If you do not have a CALL or REQ number nor have any indication of resolution from the VCCC, please email the VITA locality customer liaison with your contact information: customeraccountmanager@vita.virginia.gov

Please include the date of your initial email and any additional information supplied by the VCCC.

Other Tabs:

Instructions: Additional detail and guidelines for firewall requests (e.g. format, nomenclature, notations).

Site to Site VPN Modification: In some cases, localities and vendors use site-to-site virtual private network (VPN) tunnels. This section is to modify or remove this VPN Tunnel, as needed. Please contact the VITA locality customer liaison for any questions.

04-06-2021

COV Network Access Request for VITA Mainframe Access

My locality / organization requests access to the VITA mainframe via the internet using encrypted TN3270 software. As Information Security Officer (ISO) or Locality Mainframe Access Coordinator, as undersigned, I hereby request assistance and coordination necessary for the creation of the connection.

Please indicate the purpose for this Security Firewall Request (check all that apply):

☐ New VITA Mainframe customer / locality, first-time request.

Existing VITA Mainframe customers, check boxes that apply:

☐ New public IP due to Internet Service Provider (ISP) change replacing current Public IP, please indicate the current IP Address: Click or tap here to enter text.

☐ Remove current IP address (no longer active or operating) or,

☐ The current IP address will remain active; do not disable until date: _____

☐ Adding a secondary IP for backup, do not remove the existing primary IP Address.

☐ Other (please indicate): _____

VITA Firewall Request Information

- New Customer Source IP (xxx.xxx.xxx.xxx/32):
- Destination DNS or IP: s0221.vita.virginia.gov
- VITA Public IP (Secure FTP): 166.67.70.224
- Protocol: Secure TN3270 Telnet, Port 992

Local technical Point of Contact for questions, coordinating implementation, and testing:

- Name: Click or tap here to enter text.
- Email: Click or tap here to enter text.
- Phone:

Requestors Contact Information (Organization Information Security Officer/Manager or Access Coordinator)

- Name:
- Title:
- Email:
- Phone:

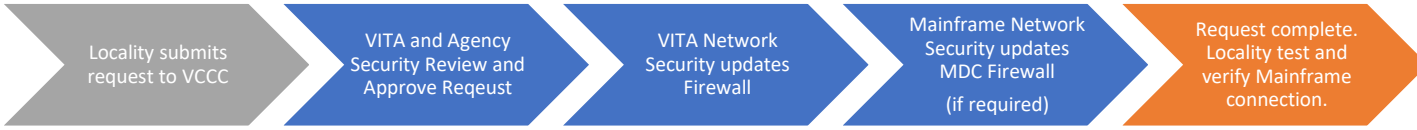
Access Coordinator Responsibilities

FORM INSTRUCTIONS

New customer / locality: This form is to be submitted after the following steps have been completed by the locality:

1. Agency (DMV / VEC) approval to access agency databases on the VITA mainframe
2. Locality has submitted the ACTREQv2 form and VITA Billing has completed new customer on-boarding and provided the 3-letter designator to the locality.
3. Locality has submitted the "VITA Access Coordinator Letter" and VITA has completed updates of assigned Access Coordinator on the VITA mainframe.

Existing customer / locality: Submit this form at any time to add / change / remove Public IP address for CoV Network access to the VITA mainframe.
Submit this form via email to the VCCC: vccc@vita.virginia.gov The sender / requestor should receive a ticket number indicating the VCCC has started the form processing. Ticket will be either a CALLxxxx or REQxxxx.
NOTE: Allow up to 10 business days for completion of the security firewall request.
Form Processing



Form instructions:
Complete "Name of county/city/organization". "County of …" or "City of ….." or "Dept of …." or "Office of ….." or other designator.
Purpose of this CoV Network Firewall Request: Check the applicable box. If new IP is replacing the existing IP, please indicate the existing or old IP Address. Show date the current address will no longer be active so it can be removed from the VITA Firewall.
Enter the Public IP address. This is the full IP address of all local traffic from the locality location to the internet.
Enter contact information for a technical POC. Usually the IT Manager or IT Resource with knowledge of the local firewall(s) configuration.
Enter contact information of Requestor. This will an Access Coordinator as indicated on the "VITA Access Coordinator Letter" form or a Locality / Organization Officer.

Local network configuration requirements:

- Local network / firewall must allow Port 992, Port 990, Port 50000-50099 bidirectional traffic.
- All 992, 990, 50000-50099 internal network traffic must be routed to the local Public IP.

Access Coordinator Responsibilities

- If using DNS (not required), set s0221.vita.virginia.gov to resolve to 166.67.70.224/32 and route to public IP

TN3270 Emulator requirements

- Supports DNS addresses
- Supports TLSv1.2 security

TN3270 Setup

- Mainframe IP: 166.67.70.224 or, if DNS used, s0221.vita.virginia.gov
- Port: 992
- Security set at TLS1.2 and/or 256-bit encryption

If this request is not complete within the 10 day processing or if the requester has not received an indication the request is complete, please contact the VCCC for an update. Please have your ticket number available. If no progress or no ticket number, please contact the Locality Liaison.

VITA Locality Customer Liaison can be contacted at

customeraccountmanagers@vita.virgininia.gov

Or contact

VCCC/Service Desk

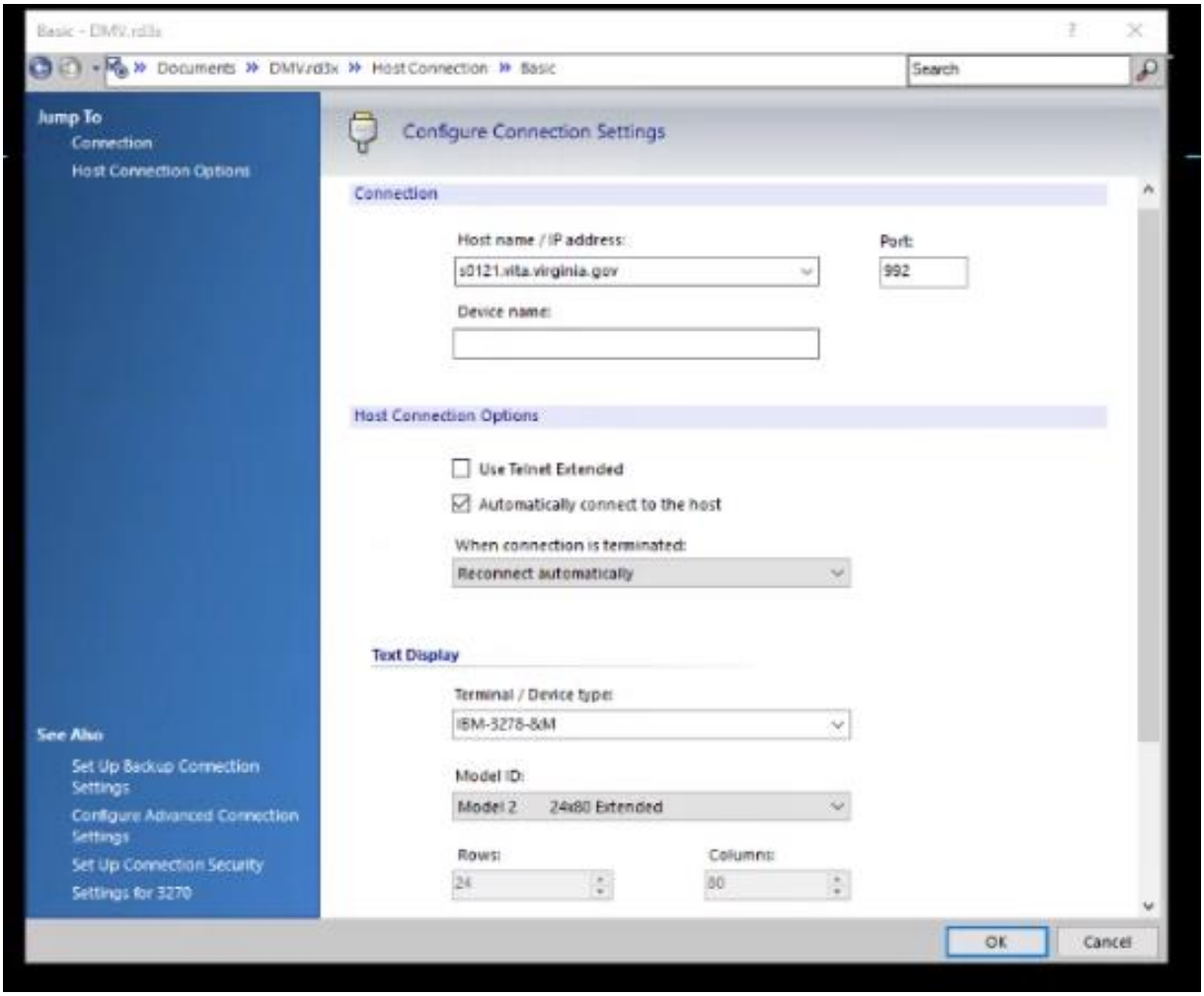
vccc@vita.virginia.gov

(866) 637-8482

Attachmate Reflections 2014 - TAX Mainframe User

This process is to make changes and verify the settings on your DMV mainframe access emulator, Attachmate Reflections meets VITA Security requirements.

1) Open your DMV connection to the mainframe using the icon on your desktop.
2) If the session connects to the VITA sign-on page, disconnect the session.
3) Open the FILE dropdown in the ribbon along the top
4) Select and click the “Setting” icon button - do not select any of the three menu items that appear on the left of the Setting button.
5) Select the Connection Configuration, the window below swill appear:



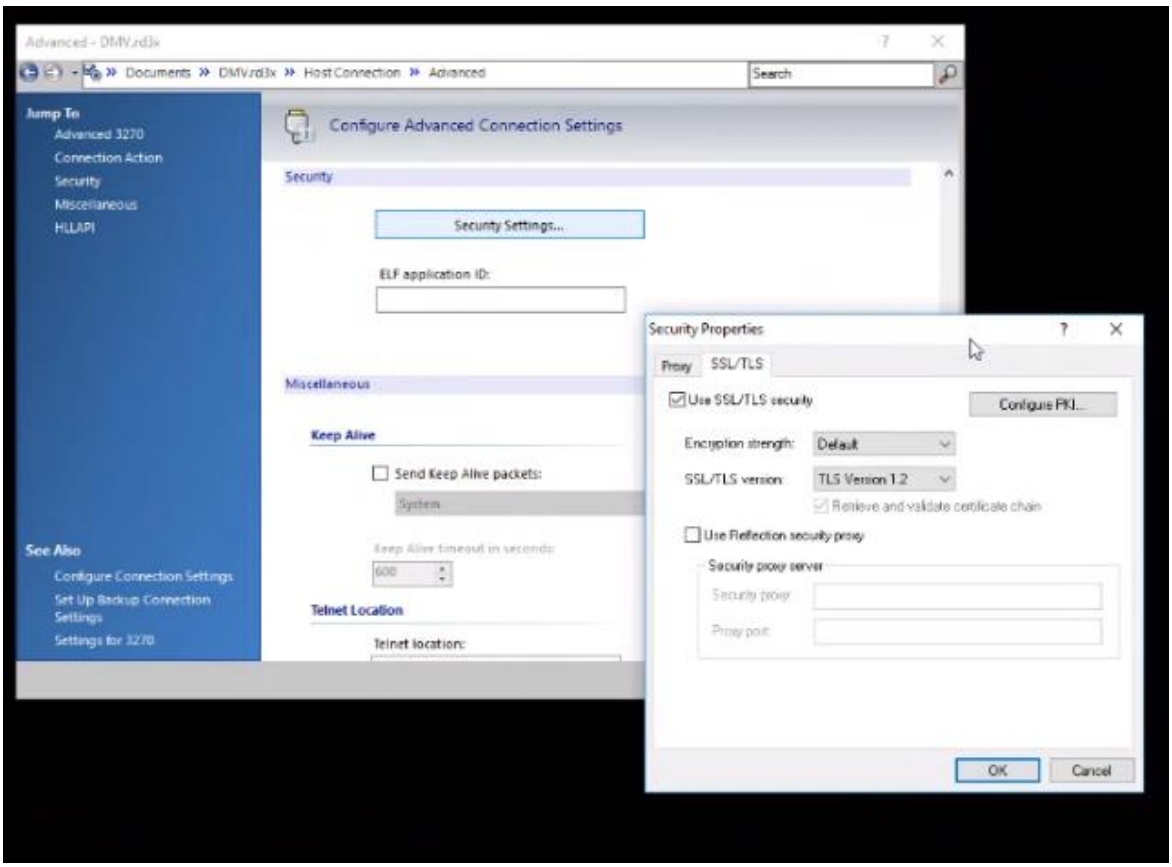
6) Under Connection=>Hostname / IP Address:
   If the entry is s0101.vita.virginia.gov or s0100.vita.virginia.gov change by typing over the following: s0121.vita.virginia.gov

Access Coordinator Responsibilities

NOTE: This change does is to migrate all Agency mainframe users to a single DNS, this does not change the location or mainframe destination IP.

7) Press OK.

8) On the menu screen, select the “Security Settings”, the screen should look like this:



9) Press “Security Settings” bar, the next window (right) will appear.

10) Ensure the “Use SSL/TLS security” is checked (as shown)

11) Ensure Encryption Strength is “Default” (As shown)

    a. If not, use the dropdown to select “Default”

12) Ensure SSL / TLS version is “TLS Version 1.2” (As shown)

    a. If not, use the dropdown to select “TLS Version 1.2”

13) Leave all other settings as shown

14) Press OK.

15) Close Attachmate Reflections.

16) Restart Reflections to verify connectivity

Access Coordinator Responsibilities

Mochasoft TN3270 Setup Procedure for initial setup

Access to VITA Mainframe for DMV/VEC/DOA CIPPS/SCB Systems

Mocha TN3270 meets the VITA security requirements in supporting secure telnet, port 992, and TLSv1.2 encryption. This software is compatible with Windows Operating Systems up to Windows 10, as of this date. This software is a one-time purchase where there is no annual license fee. Each mainframe user must have a copy of this software installed on their computer.

Mochasoft also provides free lifetime upgrades.

As of this date, Mocha TN3270 can be purchased individually or unlimited copies for the entire organization (company license), depending on your needs.

To download the software, type the following in your browser search: **Mocha TN3270**

Go to http://www.mochasoft.dk/tn3270.htm

Select the “Buy Now” button to purchase either a single or company license, or

Select the “Download” button to download a single free 30-day version.

NOTE: A company license has specific restrictions, please review those as the price-point for a company license may be more favorable for offices requiring 10 or more software copies.

Download the software and install per the instructions. Generally, no custom modification are required.

Once completely installed, proceed to the next section for set-up

Before a connection is successful, confirm with VITA that your organization has been set-up in the VITA Secure Internet Portal. A firewall rule should be in-place with VITA to allow your organization’s public IP allowed access to the CoV Network.

Mocha TN3270 Setup – Localities accessing the VITA Mainframe using the VITA Secure Internet Portal

Use the following procedure to set up MochaTN3270 for the first time after downloading either the purchased version or the free 30-day version. This procedure should be accomplished after connectivity to the mainframe has been confirmed by VITA.

1. When installing the software for the first time, the install process will place a shortcut on your desktop:

2. Double-click this short cut to open the Mocha TN270 application.

3. A black box will appear (see below) on the desktop and will attempt to connect. Since the connection is not set up yet, it will fail. Allow it to fail (within 20 seconds) and stop until a pop-up appears, below. This is expected for a first-time setup.

4. Press the “OK” button in the Mocha tn3270 white box. It will disappear, leaving the large black box remaining.

Mochasoft TN3270 Setup Procedure for initial setup 24 July 2020 Access to VITA Mainframe for DMV/VEC/DOA CIPPS/SCB Systems

5. See the ribbon along the top of the box – “File”, “Edit”, “View”, “Tools”, and “Help”.

6. Select “File”, a drop-down will appear, as follows:

7. Click the “Edit/New Session” entry. The “Edit/New Session” box will appear, as follows:

Mochasoft TN3270 Setup Procedure for initial setup 24 July 2020 Access to VITA Mainframe for DMV/VEC/DOA CIPPS/SCB Systems

8. In the “Edit/New Session” box, enter the following (per the illustration below):

a. **Name:** This is the name of your session; you can call it whatever you like, that makes sense to you (e.g. DMV Mainframe, DMV Look-up, Sue, Bill, Go Redskins, etc.)

b. Mainframe IP Address: enter 166.67.70.224 **(unless directed to use a different entry)**

c. Port: enter 992

d. SSL/TLS box: Checked

e. **TN3270E:** Checked

f. All other boxes and fields should remain unchecked or empty.

g. **Connect to this IBM Mainframe to program start:** Checked – if you want the software to immediately connect when you start it up (double-click the icon), or Uncheck – if you prefer to manually connect to the mainframe by pressing the “Connect” button every time you open the software. This is changeable anytime.
Mochasoft TN3270 Setup Procedure for initial setup 24 July 2020 Access to VITA Mainframe for DMV/VEC/DOA CIPPS/SCB Systems

Press the “Apply” button to save the set-up.

10. Press the “Connect” button to connect to the mainframe. A successful connection will look like this – NOTE the “Online TLS1.2” message at the bottom of the screen. It is a little cut-off, but should look like this.

Jolly Giant: QWS3270 SECURE

NOTE: The customer must have QWS3270 **SECURE ,** not QWS3270 PLUS or QWS3270 or WIRE.

The **SECURE** version is the only Jolly Giant product that supports the TLSv1.2 security requirement. The caller/user should be directed to upgrade their Jolly Giant version to QWS3270 SECURE, then use the setup/configuration described below.

The next three screens should be set up as shown below:

CONNECTION: HOST SETTINGS

QWS3270 SECURE Screenshots

Host Name or IP Address:

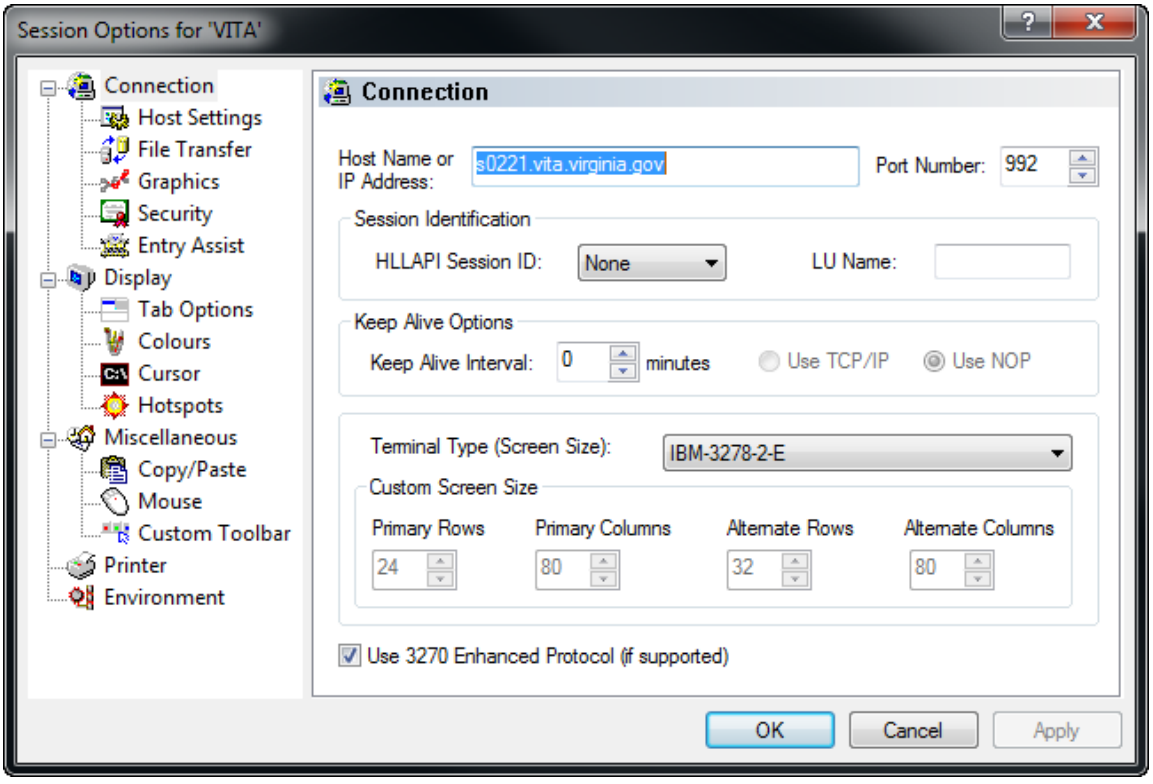
Locality: 166.67.70.224 (All localities are directed to use SYS2B portal)

Agency: 's0121.vita.virginia.gov' (SYS1B) or 's0221.vita.virginia.gov' (SYS2B)

NOTE: Either host name works equally as well, some agencies use SYS1B and others use SYS2B for load balancing purposes. For purposes of getting a user up and running, either works.

Port Number: 992 (as shown)

Terminal Type: IBM-3278-2-E (as shown)



Access Coordinator Responsibilities

Security / Encrption Settings:

Click on the ‘Security’ tab on the left side of the window.

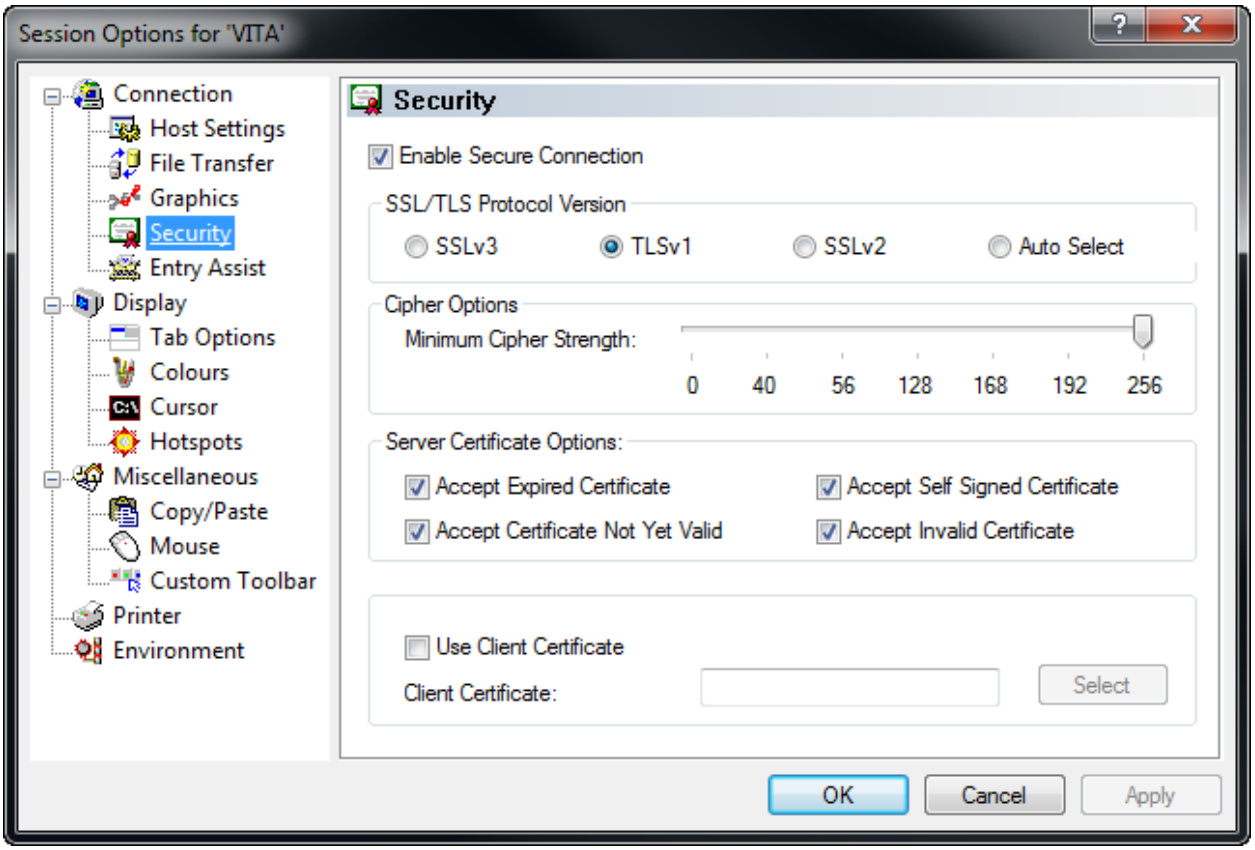
Check the Enable Secure Connectoin box (as shown)

Click the TLSv1 button (as shown)

Move or Leave the Cipher Strength slider at “256” (as shown)

Note: This setting forces QWS3270 to TLSv1.2.

Certificates – check all boxes (as shown)



File Transfer

File Transfer Program Name: IND$FILE (default)

Host Type: CMS (as shown)

Transfer Mode: WSF (as shown)