VITA Virginia Information Technologies Agency

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		
VEC mainframe (Primary)	166.67.70.224		
VEC mainframe (Secondary)	166.67.70.224		

VITA network access request form instructions

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)	166.67.70.223		
DOA/CIPPS (FTP)	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**

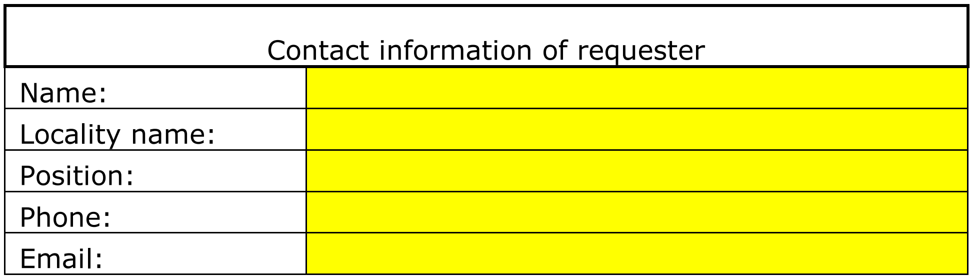
Note: If you do not want the current IP to be turned off right away, especially if the organization is migrating users over time, do not use this section. Use section 2a. or 2b. to add your new ISP IP(s).

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**		**New Public IP**
	xxx.xxx.xxx.xxx (remove)		

VITA network access request form instructions

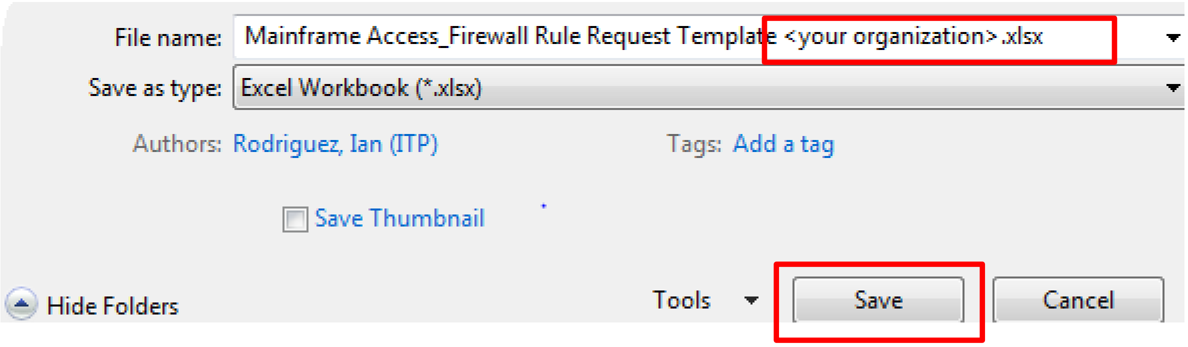
3a. Enter local contact information in the event the firewall team needs additional or clarification of entered information.



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.



File name: Mainframe Access_Firewall Rule Request Template <your organization>.xlsx

Save as type: Excel Workbook (*.xlsx)

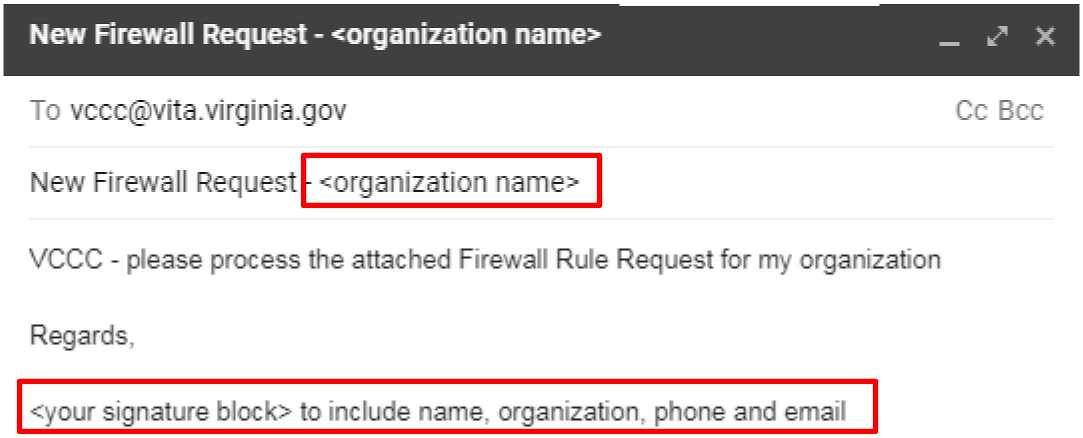
Authors: Rodriguez, Ian (ITP)

Tags: Add a tag

□ Save Thumbnail

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

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



New Firewall Request - <organization name>

To vccc@vita.virginia.gov

New Firewall Request - <organization name>

VCCC - please process the attached Firewall Rule Request for my organization

Regards,

<your signature block> to include name, organization, phone and email

VITA network access request form instructions

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 (customeraccountmanager@vita.virginia.gov) with any questions.