JOB AID
Multi-Factor Authentication

OVERVIEW

Multi-factor authentication (MFA) is a security provision that requires more than one method of verification of the user's identity for a system login. All State and CSRA remote users will be required to adhere to multi-factor authentication when accessing any NCTracks production or non-production resource using F5. F5 allows staff to access Silk Central, which is used to track defects and service tickets, as well as other applications and links.

Accessing NCTracks remotely requires permission. If you do not currently access NCTracks remotely, and your job function requires it, contact your manager or user administrator to request remote access permission.

OBJECTIVE

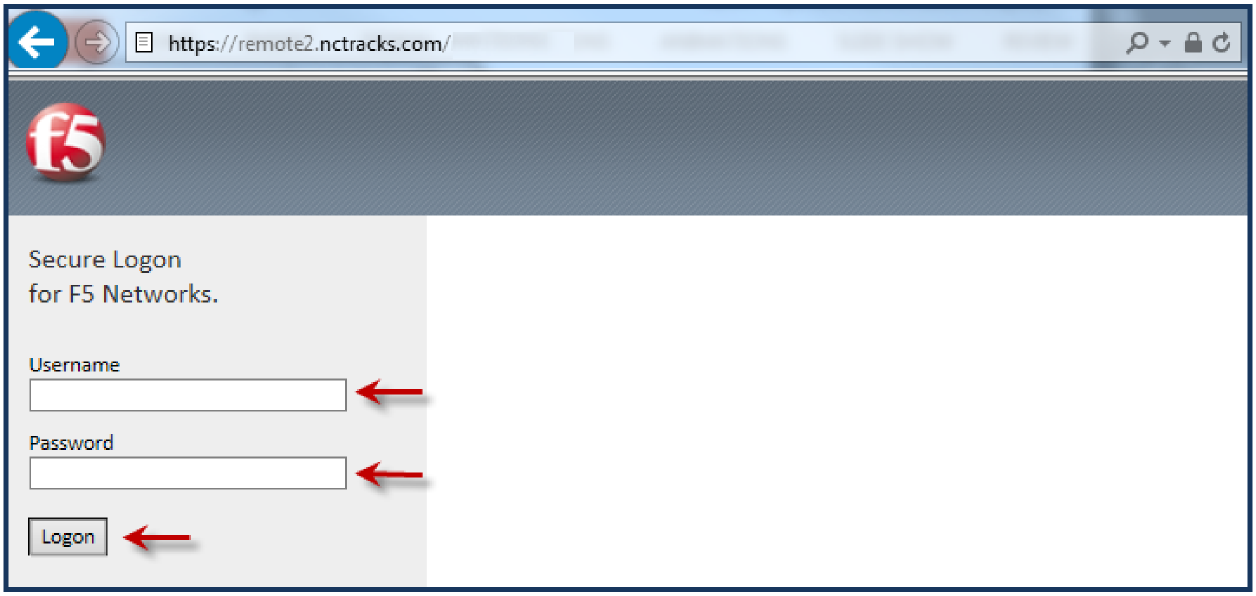
This Job Aid provides instructions for:

- Updating your profile in the Active Directory (AD) in order to confirm or update your email address. This email address will be used for prompt delivery of a One Time Password (OTP).
- The F5 login process for State and CSRA users.
- Troubleshooting technical issues.

UPDATING THE ACTIVE DIRECTORY

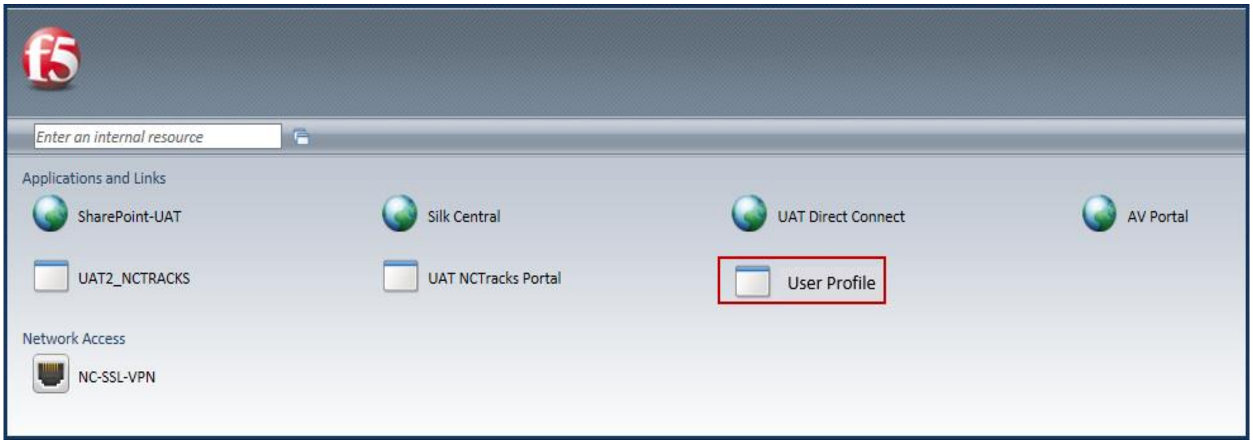
State and CSRA users will have the option to update their profile in the AD beginning May 20, 2018 and ending June 2, 2018. The F5 multi-factor authentication requirements will be implemented June 3, 2018. The email address in the AD will be used for the delivery of the OTP that will be used at each login request. If the AD is not updated, the default email address will be the email address currently listed in the AD.

To access NCTracks remotely, the user will navigate to the F5 login screen at https://remote2.nctracks.com, enter their Username and Password, and select **Logon**.



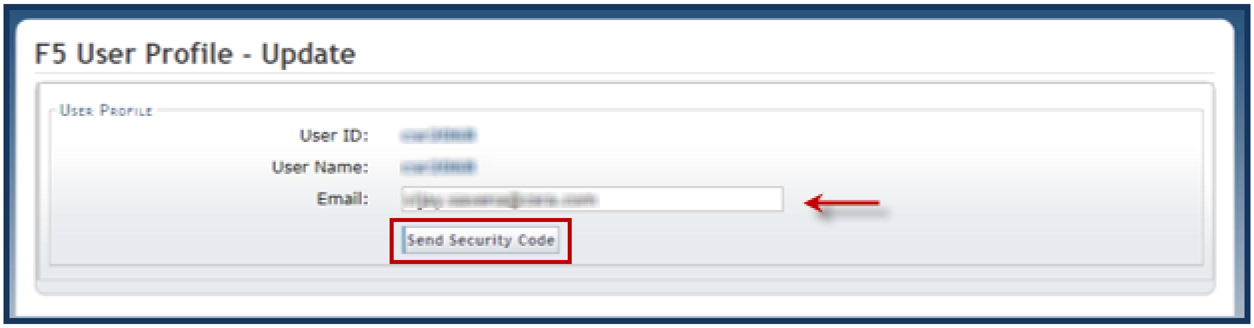
Once the user has entered their credentials, the following screen will display allowing the user to update their profile by selecting “User Profile”.

Note: F5 menu options vary based on the user’s access permissions.



The following message will be displayed at the bottom of the page to remind users of the new login process. Once the MFA enhancement has been implemented, the message will no longer be present.

“Attention F5 Users: Beginning June 3, 2018, you will be required to use a stronger authentication method to access your account. During each subsequent login, after entering your username and password, you will receive a new, one-time use security code via email. You will then have to enter that one-time security code to access your account. The email address that will be used for this is maintained via the “User Profile” link on the landing page. Please navigate to that application and verify and/or update your email address before June 3rd, so you will be able to login once this change has been implemented.”



F5 User Profile - Update

User Profile

User ID: [redacted]

User Name: [redacted]

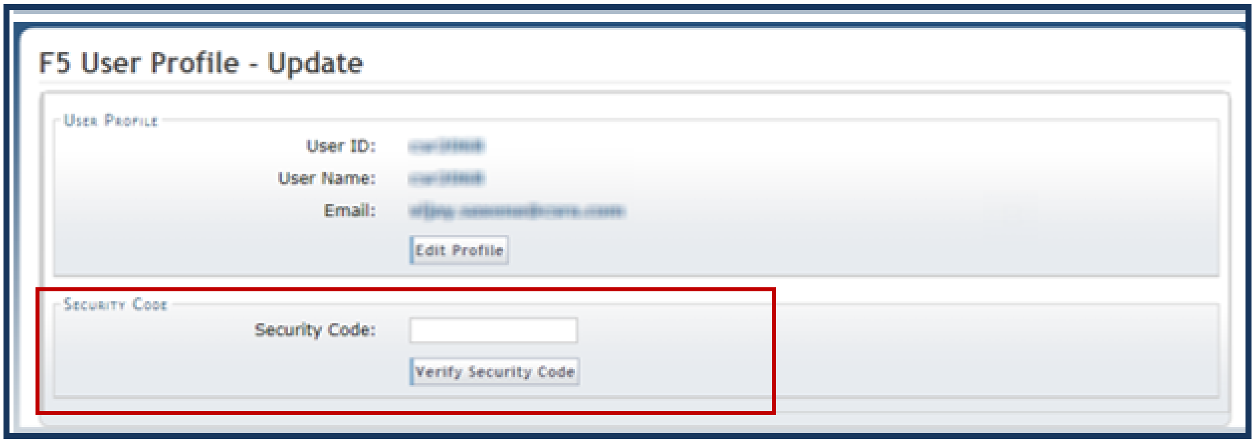
Email: [redacted]

Review the default email address. If this is the address to be used for the delivery of OTPs, no updates are required. If the email address needs to be changed, make the appropriate changes and select **Send Security Code**.

Note: For the purposes of F5 MFA, the terms Security Code and OTP are synonymous.

A security code will be sent to the email address to authenticate the profile update changes.

Navigate to your email system and find the email containing your security code.



F5 User Profile - Update

User Profile

User ID: [redacted]

User Name: [redacted]

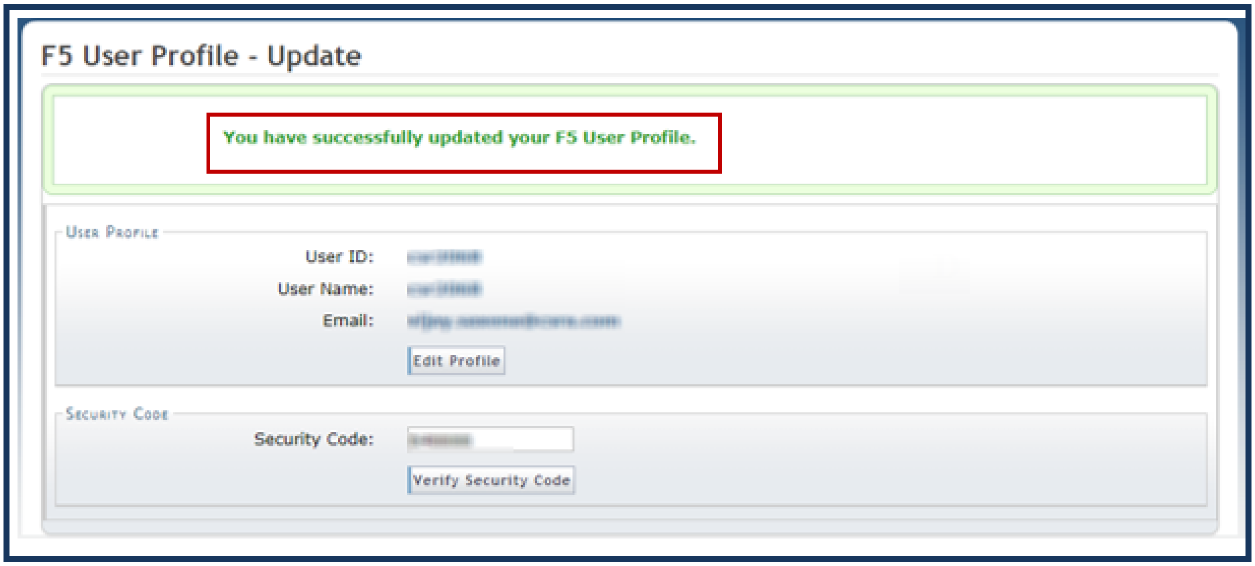
Email: [redacted]

Security Code

Security Code:

Enter the security code in the **Security Code** field and select **Verify Security Code**.

Upon successful completion of these steps, a confirmation page will display.



F5 User Profile - Update

You have successfully updated your F5 User Profile.

User Profile

User ID: [redacted]

User Name: [redacted]

Email: [redacted]

Security Code

Security Code: [redacted]

RECEIVING SECURITY CODE/OTP VIA TEX MESSAGE

While all Security Codes are sent out via email, users that would prefer to receive Security Codes via text can use an SMS-to-email gateway. Most major cell carriers provide an SMS-to-email gateway. In order to use this, users must provide the email address that corresponds to their cell number and carrier. This email address is the 10-digit cell number followed by the @ symbol and the carrier-specific SMS gateway domain. Here are the SMS gateway domains for some of the leading cell carriers.

Mobile carrier	SMS gateway domain
Alltel	sms.alltelwireless.com
AT&T	txt.att.net
Boost Mobile	sms.myboostmobile.com
Cricket Wireless	sms.mycricket.com
MetroPCS	mymetropcs.com
Project Fi	msg.fi.google.com
Republic Wireless	text.republicwireless.com
Straight Talk	vtext.com
Sprint	messaging.sprintpcs.com
T-Mobile	tmomail.net
U.S. Cellular	email.uscc.net
Verizon Wireless	vtext.com
Virgin Mobile	vmobl.com

For example, if your carrier is AT&T and your cell number is (919) 555-1212, the email address that you would use would be 9195551212@txt.att.net.

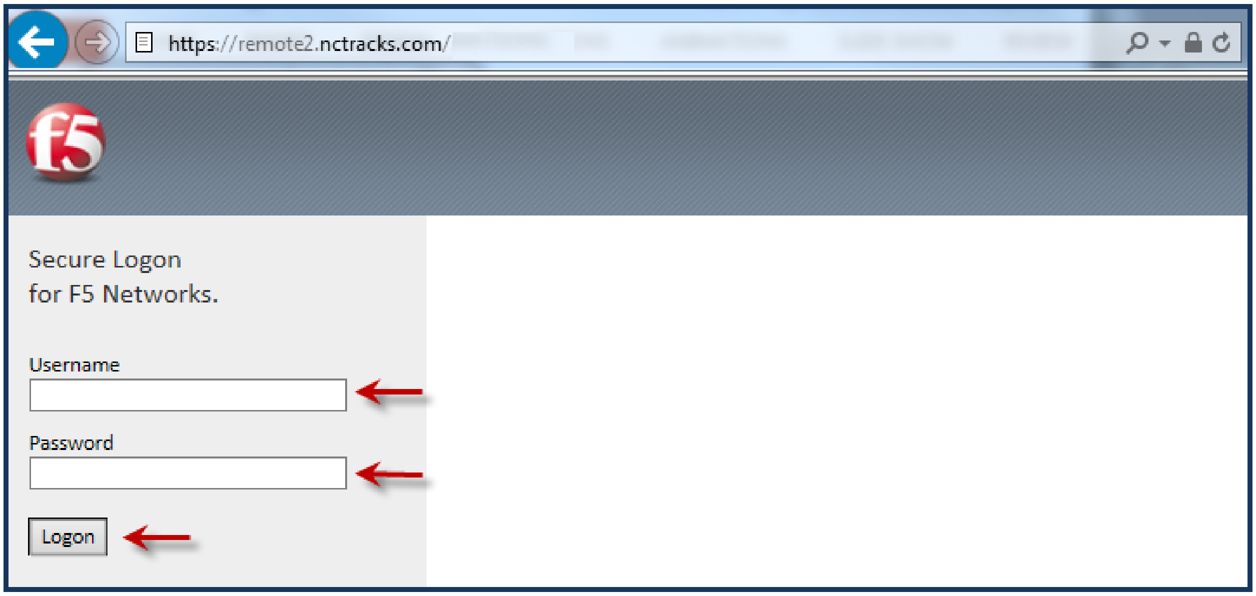
Notice in this example that the email address is the telephone number expressed as 10 (ten) digits [without the country code, (1), dashes or any separator characters] and the SMS gateway domain. The country code is not needed. The 10-digit telephone number with the email domain are sufficient to send the email from any location in the world.

If your carrier is not listed and you still wish to receive Security Codes via text, please contact your carrier to get their SMS gateway domain.

F5 LOGIN PROCESS FOR STATE AND CSRA USERS

Additional steps have been added to the F5 Virtual Private Network (VPN) login process for all remote users (State and CSRA). An additional authentication will be required in order to gain access to all production and non-production resources, applications, and various environments.

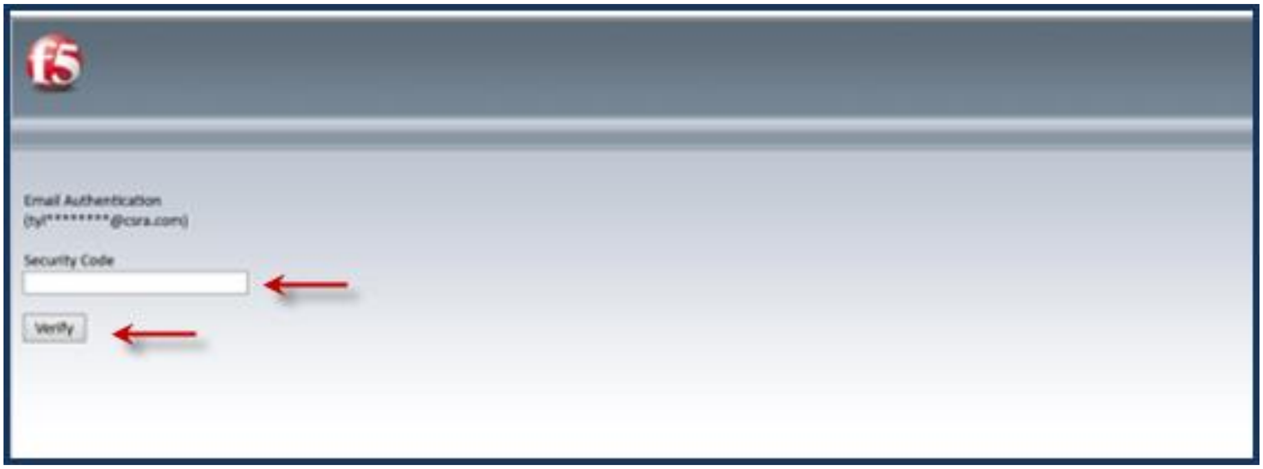
The user will navigate to the F5 login screen at https://remote2.nctracks.com, enter their Username and Password, and select **Logon**.



Once your initial credentials are entered, an email containing an OTP will be sent to the email address in the AD.

Navigate to your email system and find the email containing your security code.

Enter the OTP in the **Security Code** field and select **Verify**.



Email Authentication
(tyl*********@csra.com)

Security Code

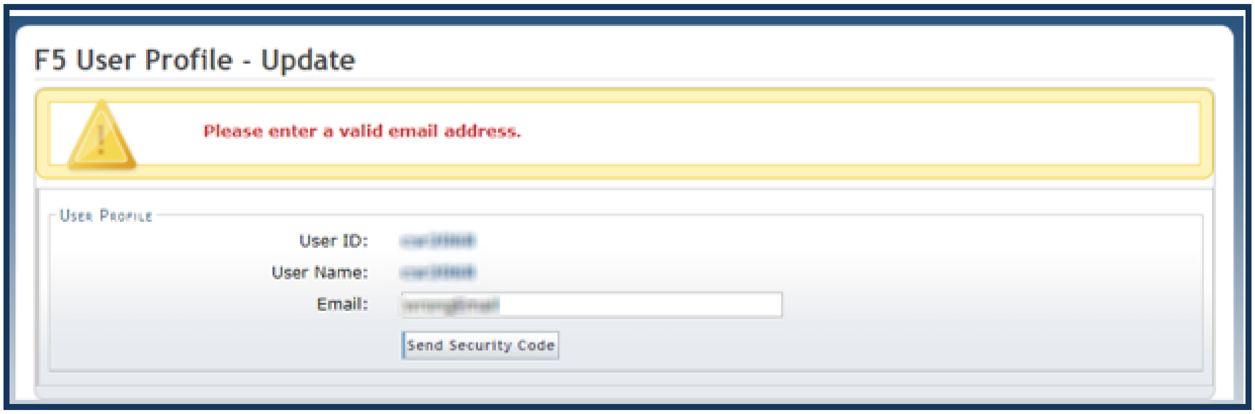
Once the Security Code/OTP has been confirmed, access to F5 VPN will be granted.

TROUBLESHOOTING TECHNICAL ISSUES

Following are examples of circumstances and resources to assist with troubleshooting technical issues.

Invalid Email Address

It will be very important to confirm or update your email address prior to the implementation of this enhancement on June 3, 2018. Users will have the option of updating their profile in the AD beginning May 20, 2018 and ending June 2, 2018. If the email address on file is invalid, you will receive the following error message.



F5 User Profile - Update

Please enter a valid email address.

User Profile

User ID: [redacted]

User Name: [redacted]

Email: [redacted]

Once the MFA process is implemented, if you **DO NOT HAVE** access to the email address on file, you will not be able to update the email address using the User Profile button on the F5 page. You will need to contact your security administrator to have them submit a ticket to update the email address.

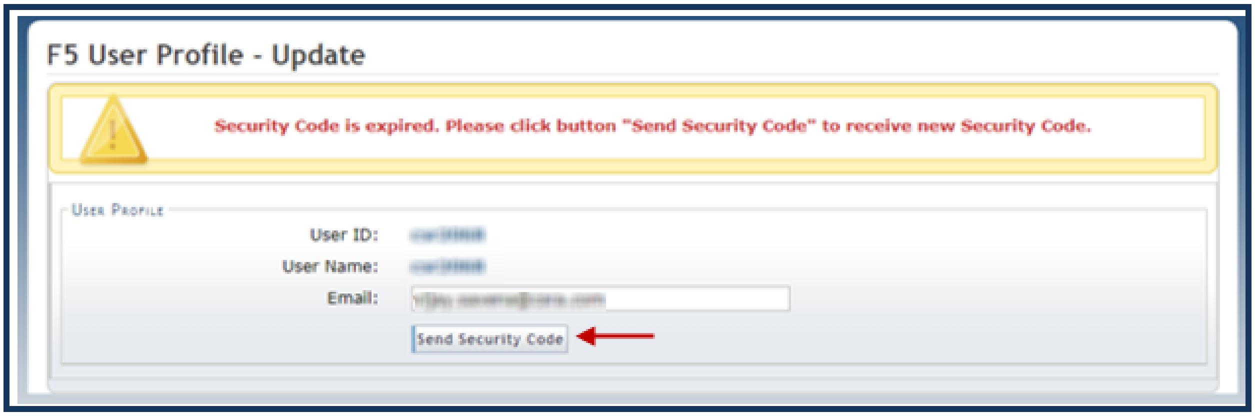
Once the MFA process is implemented, if you **DO HAVE** access to the email address on file, you will continue to be able to update the email address using the User Profile button on the F5 page.

You will need to contact the NCTracks Operations Contact Center at 800-688-6696. The call center agent will need a valid email address in order to create a service ticket to manually update the AD. Once the AD has been manually updated, you will be contacted to confirm completion of the request.

Expired Security Code

The Security Code/OTP is a numeric code that will expire if not verified within 5 minutes. If the code entered has expired, you will receive the following message and will need to request a new security code by selecting **Send Security Code**.

The new code will be delivered to the email address on file. Please retrieve and enter the new security code.



F5 User Profile - Update

Security Code is expired. Please click button "Send Security Code" to receive new Security Code.

User Profile

User ID: [redacted]

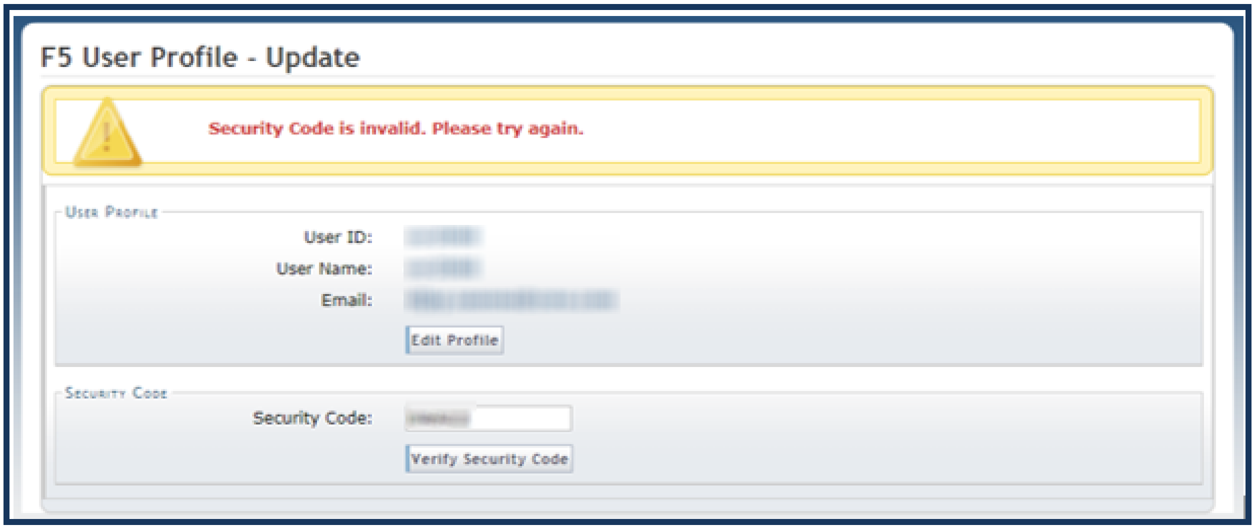
User Name: [redacted]

Email: [redacted]

Invalid Security Code

The numeric security code received in your email should be entered in the **Security Code** field. If an error message is received indicating that the security code is invalid, confirm that you have entered the code correctly and re-enter if necessary.

If the system is unable to verify the code, you can request that a new code be sent by selecting the **Edit Profile** button. You will be given the option to have another security code emailed to the email address on file.



F5 User Profile - Update

Security Code is invalid. Please try again.

User Profile

User ID: [redacted]

User Name: [redacted]

Email: [redacted]

Security Code

Security Code: [redacted]

Note: If you are not able to successfully log in to your email, you should follow the same help desk procedure that you currently follow for your organization.