

Two-Factor Authentication User FAQ's

Table of Contents...

[What is Two-Factor Authentication \(2FA\)?](#)

[What does Symantec Validation and ID Protection \(VIP\) do?](#)

[I don't have a smartphone, what is my alternative?](#)

[How many devices can I register?](#)

[What type of mobile devices can I install Symantec VIP on?](#)

[Does the Symantec VIP Application use my mobile data plan?](#)

[I lost/replaced my device with my registered credential, what do I do?](#)

[Removing a registered credential](#)

[I am unable to log into a KBR application that requires two-factor authentication \(2FA\)](#)

[I do not have my registered credential in my possession; can I get a temporary code?](#)

[Can I use this Credential ID and Security Code outside of KBR?](#)

[I am getting an error when I select send temporary security code using SMS or Voice Call from the 'Confirm Your Identity' window](#)

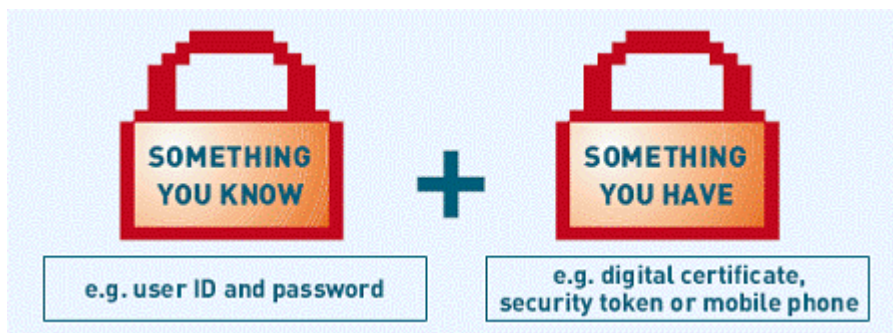
[How many times can I enter the 6-digit VIP Security Code incorrectly before I am locked?](#)

[I am being prompted for multiple logins and cannot open Office files within SharePoint](#)

What is Two-Factor Authentication (2FA)?

To strengthen KBR information security and safeguard company data, Information Technology will implement two-factor authentication for remote access to Outlook Web Access (OWA), Citrix, and VPN.

Two-factor authentication (2FA) provides identification of users by pairing two different components for enhanced security, to protect access to networks and websites. These components may be something the user has (a security code), and something the user knows (a password).



A good example of this is how an ATM card works. You can withdraw money from an account with a bank card (something the user has), and a PIN (something the user knows). Only the correct combination of these two items allows the transaction to be completed.

[Table of Contents...](#)

What does Symantec Validation and ID Protection (VIP) do?

Symantec VIP helps to protect networks, applications and data against unauthorized access, as part of a comprehensive information protection program.

There are a variety of credential forms available. KBR's preferred method is Symantec VIP for your mobile device. A desktop version is also available for employees without a mobile device.

Once you have installed the Symantec VIP application on your mobile device or computer, you will use it to access networks or applications which utilize two-factor authentication, such as Citrix, OWA or VPN. You will be prompted for a VIP security code which the Symantec VIP application provides.

[Table of Contents...](#)

I don't have a smartphone, what is my alternative?

KBR's preferred method for installing and registering for two factor authentication is a smartphone or mobile device. In the event you don't have a smartphone or mobile device, you may install the Desktop Version on your laptop or desktop computer.

For more information regarding how to install the desktop version, visit the Two-Factor Authentication (2FA) User Registration instructions on the [2FA Support Portal](#).

If neither the mobile device nor desktop versions are options for you, please send an email to the KBR IT 2FA Support mailbox at kbrit2fasupport@kbr.com for assistance.

[Table of Contents...](#)

How many credentials can I register?

You are able to register up to 3 credentials

[Table of Contents...](#)

What type of mobile devices can I install Symantec VIP on?

Symantec VIP is available on most devices, including:

- iPhone and iPad running iOS 7.0 and higher
- Android running v4.0 and higher
- Windows phone running 7.5, 8, and 8.1
- Blackberry 10 and higher

For a full list of devices, see <https://m.vip.symantec.com/supportedphones.v>

[Table of Contents...](#)

Does the Symantec VIP Application use my mobile data plan?

When installing the Symantec VIP Application on your mobile device, you will need to be connected to either your mobile data or a secured Wi-Fi connection. After the application is installed, mobile data or Wi-Fi is no longer necessary for the application to function.

[Table of Contents...](#)

I lost/replaced my device with my registered credential, what do I do?

If you have lost/replaced a device that you previously registered a Symantec VIP credential from, you will need to register the new credential that appears on the device before you can authenticate with KBR applications that require two-factor authentication.

If the old registered device is not in your possession due to replacement or the device being misplaced, you will need to request a temporary code to log into the registration portal.

1. Go to <https://2fa.kbr.com/>.

The screenshot shows the Symantec VIP Self Service Portal sign-in page. At the top left is the Symantec logo and the text 'VIP SELF SERVICE PORTAL'. At the top right is the KBR logo. Below the header is a yellow bar. The main content area has a dark header with 'Sign In'. Below this is a form with two input fields: 'User Name' with the value 'hbay736' and 'Password' with masked characters. Below the password field is a small logo for 'Symantec Validation & ID Protection' and a yellow 'Sign In' button.

2. Log in with your [KBR Network User ID and Password](#).

3. Select 'Trouble signing in?'

To Complete Your Sign-in

For your protection, first confirm your identity by entering a security code from your credential that has **already been registered** to your account.

Confirm Your Identity

Enter a security code from this credential:

Credential Name: **My Phone**

Credential ID: **VSTZ**

Credential Type: **VIP Credential**

Security Code:

[What is a Security Code?](#)

4. Select the appropriate option which fits your needs, to request a temporary security code, to confirm your identity.

Symantec | VIP SELF SERVICE PORTAL (hbay736) Sign Out
KBR

To Complete Your Sign-in

Request a temporary security code to help confirm your identity.

Confirm Your Identity


How would you like to receive your security code?

Email Address: Ma*****@kbr.com

SMS* (Text Message): 128*****59

Voice Call: 171*****69

5. Enter the 6 digit code that was sent via the means selected in step 4, into the 'Security Code' field and select 'Sign In.'

 A temporary security code has been sent to Ma*****@kbr.com.

Enter Your Temporary Security Code

Confirm Your Identity


Security Code:

6. You may now manage your registered credentials listed. To remove the old credential, follow the instructions listed in [Removing a registered credential](#).
7. To register a new credential, visit the [2FA Support Portal](#) for registration instructions.

[Table of Contents...](#)

Removing a registered credential

1. Go to <https://2fa.kbr.com/>.


 Symantec. | VIP SELF SERVICE PORTAL **KBR**

Welcome to the Symantec® VIP Self Service Portal
To access the Self Service Portal, enter your user name and password, and click Sign In.

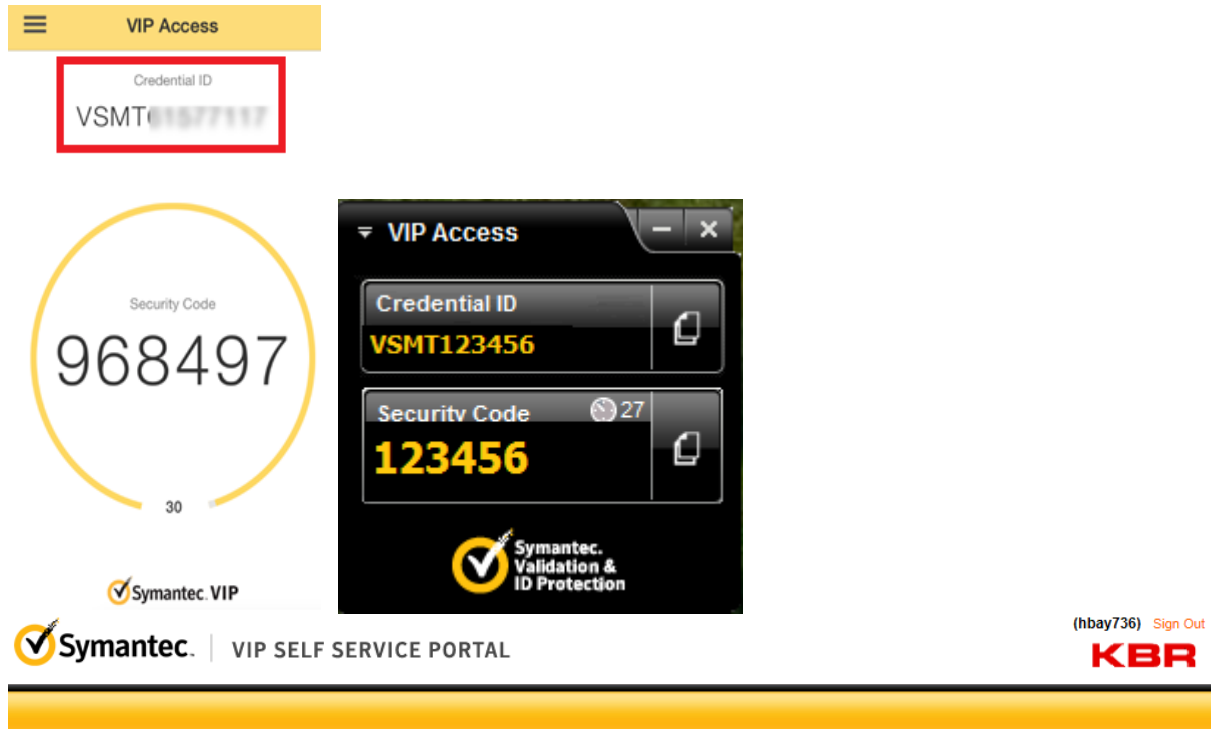
Sign In

User Name:

Password:

Enabled by: 

2. Log in with your **KBR Network User ID and Password**.
3. Enter in the security code from your registered credential into the **'Security Code'** field on your web browser.



To Complete Your Sign-in

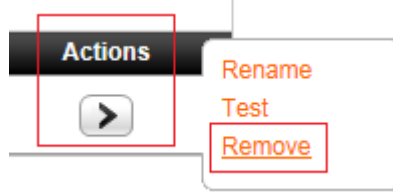
For your protection, first confirm your identity by entering a security code from your credential that has **already been registered** to your account.

The image shows a 'Confirm Your Identity' dialog box. It contains the following fields and text:

- Enter a security code from this credential:
- Credential Name: **Mary's Phone**
- Credential ID: **VSTZ**
- Credential Type: **VIP Credential**
- Security Code: (This field is highlighted with a red box)
- What is a Security Code? (link)
- Cancel (button)
- Continue (button)
- Trouble signing in? (link)

NOTE: If the Credential ID listed in the web browser does not match what is listed as the Credential ID on the device in your possession, the Security Code will not work and the credential that is your possession will need to be properly registered.

4. Within the device manager, you will be able to do the following:
 - a. Remove your registered credential.
 - o Select the arrow (>) next to 'Actions' and select 'Remove'



- o Select the 'Remove' button to successfully remove the credential



VIP SELF SERVICE PORTAL

(hbay736) Home | Sign Out



Remove Credential

Are you sure you want to remove credential **Mary's Phone** ?

Note: Once your credential has been removed, it can no longer be used unless it is registered again.



NOTE: Once the credential has been removed, it can no longer be used unless it is registered again.

[Table of Contents...](#)

I am unable to log into a KBR application that requires two-factor authentication (2FA)

When logging into a KBR application that requires two-factor authentication, you will be required to provide your KBR Network User ID and Password, Domain and a 6-digit Security Code which is provided by the credential you have registered (smartphone, desktop version, hardware token card).

NOTE: The domain is **not** necessary when logging in, unless specifically asked, such as with Citrix. Enter only your User ID, password and 6 digit security code to gain access.

1. Go to the KBR application you wish to access (Citrix, OWA, VPN, SharePoint), which will prompt you for two-factor authentication.

A screenshot of a login form with a grey background. It contains four input fields: 'User name:' with the value 'hbay736', 'Password:' with masked characters, 'Domain:' with a dropdown menu showing 'corp.kbr.com', and 'VIP Security Code:' with masked characters. A 'Log On' button is located at the bottom right of the form.

- In the 'User Name' field, enter your KBR Network User ID. Do **not** enter the domain information in the User ID field.
 - In the 'Password' field, enter your KBR network password.
 - In the 'Domain' field, select the appropriate domain (when applicable).
 - In the 'VIP Security Code' field, enter the 6-digit security code provided on the device that contains the credential that was previously registered (smartphone, desktop version).
2. If all of the fields above are entered correctly, you will be granted access to the specific application successfully.
- NOTE:** If you have not entered correct information in any of the fields, the return error message will display that your credentials are incorrect.

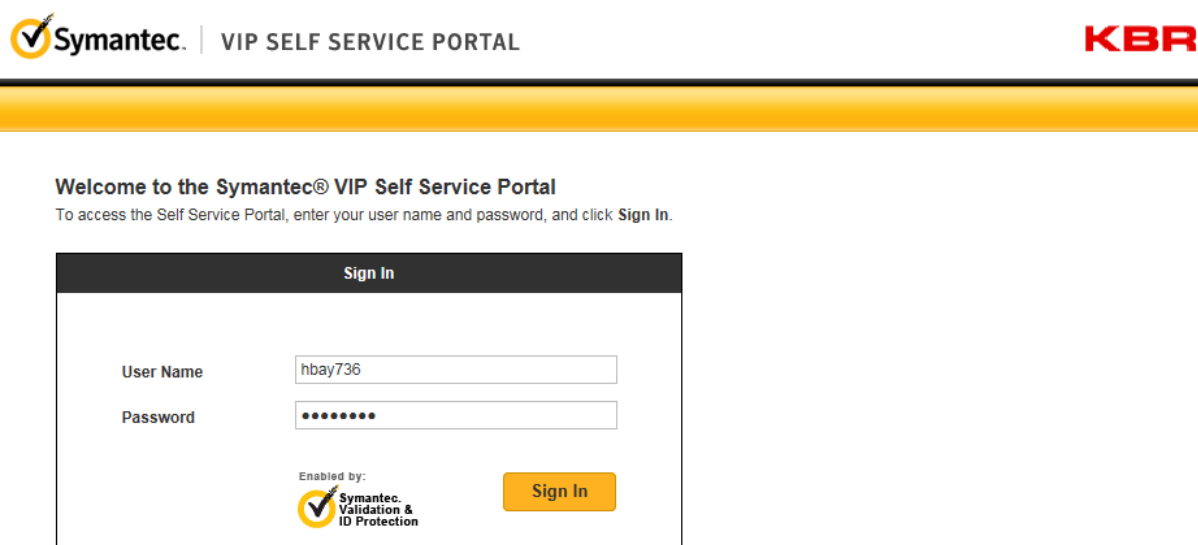
[Table of Contents...](#)

I do not have my registered credential in my possession; can I get a temporary code?

If you are attempting to access a KBR remote application that requires two factor authentication and do not have your registered credential, contact the Global Service Desk.

If you need a temporary code to log into the two factor authentication self-service portal to manage your credentials, follow the instructions:

1. Go to <https://2fa.kbr.com/>.



The screenshot shows the Symantec VIP Self Service Portal Sign In page. At the top left is the Symantec logo and the text "VIP SELF SERVICE PORTAL". At the top right is the KBR logo. Below the logos is a yellow horizontal bar. The main content area has a dark header with "Sign In" in white. Below the header, there are two input fields: "User Name" with the value "hbay736" and "Password" with masked characters. Below the password field, there is a small logo for "Symantec Validation & ID Protection" and a yellow "Sign In" button.

2. Log in with your **KBR Network User ID and Password**.
3. Select **'Trouble signing in'** at the bottom of the 'Confirm Your Identity' window.

To Complete Your Sign-in

For your protection, first confirm your identity by entering a security code from your credential that has **already been registered** to your account.

Confirm Your Identity

Enter a security code from this credential:

Credential Name: **My Phone**

Credential ID: **VSTZ**

Credential Type: **VIP Credential**

Security Code:

[What is a Security Code?](#)

4. Select the appropriate option which fits your needs, to request a temporary security code, to confirm your identity.

To Complete Your Sign-in

Request a temporary security code to help confirm your identity.

Confirm Your Identity

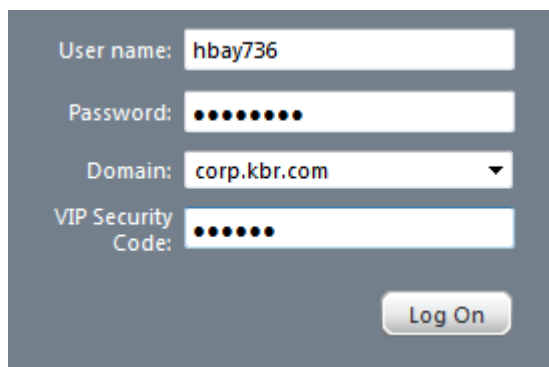
How would you like to receive your security code?

Email Address: Ma*****@kbr.com

SMS* (Text Message): 128*****59

Voice Call: 171*****69

5. Enter the 6 digit code that was sent via the means selected in step 4, into the Security Code field or the KBR application you are attempting to log in to (OWA, Citrix, VPN, SharePoint).



The screenshot shows a login interface with the following fields and values:

- User name: hbay736
- Password: [Redacted]
- Domain: corp.kbr.com
- VIP Security Code: [Redacted]

A "Log On" button is located at the bottom right of the form.

[Table of Contents...](#)

Can I use this Credential ID and Security Code outside of KBR?


Use your VIP credential at any participating organization within the Validation and ID Protection Network as listed in the below site.

<https://idprotect.vip.symantec.com/desktop/wheretouse.v>

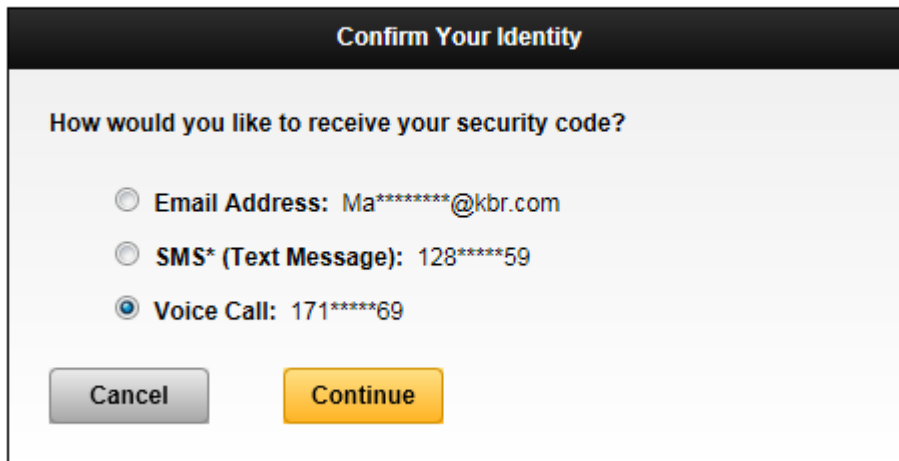
Important: Be sure to **register** your VIP credential at each VIP Participating Organization where you have an online account before you use the credential. Then your participating organizations will be able to recognize your VIP credential ID. Look for the Validation and ID Protection logo at VIP Participating Organization for instructions.

[Table of Contents...](#)

I am getting an error when I select send temporary security code using SMS or Voice Call from the 'Confirm Your Identity' window

 Unable to send temporary security code to 171*****69.

Request a Temporary Security Code



Confirm Your Identity

How would you like to receive your security code?

Email Address: Ma*****@kbr.com

SMS* (Text Message): 128*****59

Voice Call: 171*****69

This error is due to incorrect formatting of the phone numbers that are listed in your Outlook Properties (OPROPS).

The short term solution to this error is to select to have your temporary security code sent to your email address.

The long term solution is to update your phone numbers within Outlook Properties by going to <https://oprops.corp.kbr.com/>.

Please ensure your listed phone numbers are formatted correctly:

- No dashes –
- No period .
- No parenthesis ()
- May contain one space between numbers
- Must contain + followed by country code

Example Formatting:

Americas Region: +1 713 753 1234

Europe: +44 1372 86 1234

Australia: +61 8 9278 1234

Singapore: +65 62 10 1234

UAE: +971 4 313 1234

If you are unable to connect to Outlook Properties or are having difficulty updating your Outlook Property information, please contact the KBR Global Service Desk for assistance.

[Table of Contents...](#)

How many times can I enter the 6-digit VIP Security Code incorrectly before I am locked?

Ten (10)

If you are trying to log into a KBR application that is prompting for two-factor authentication, such as Citrix, OWA or VPN, and you enter the 6-digit security code incorrectly, you can enter the code incorrectly up to 10 times before your Symantec VIP account will be locked.

If you have locked your Symantec VIP account due to entering your 6-digit code incorrectly 10 times, you must contact the KBR Global Service Desk to unlock the account.

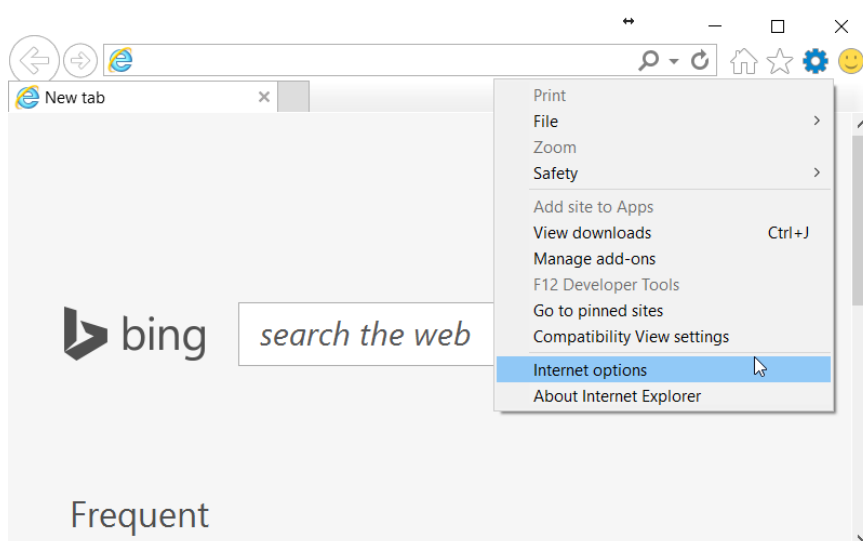
[Table of Contents...](#)

I am being prompted for multiple logins and cannot open Office files within SharePoint

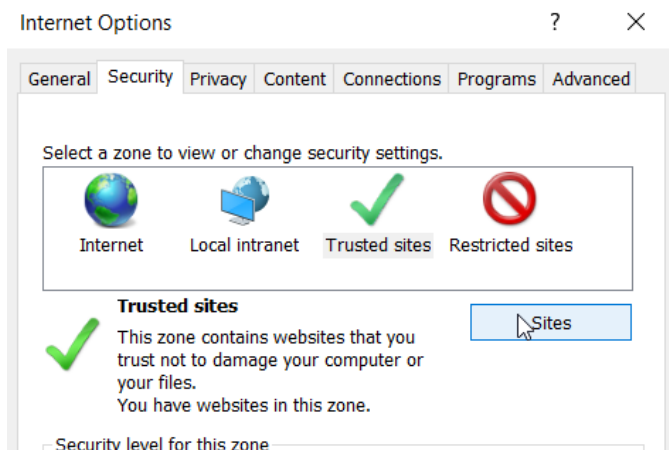
The problem occurs because of a security feature within Microsoft Windows. In the default configuration, Windows does not allow persistent cookies to be shared between the web browser and Office applications ([Microsoft KB932118](#)). The user

To resolve the problem, you must add *.kbr.com as a “Trusted Site” within Internet Explorer so the Office apps will use the same login session cookies as the browser.

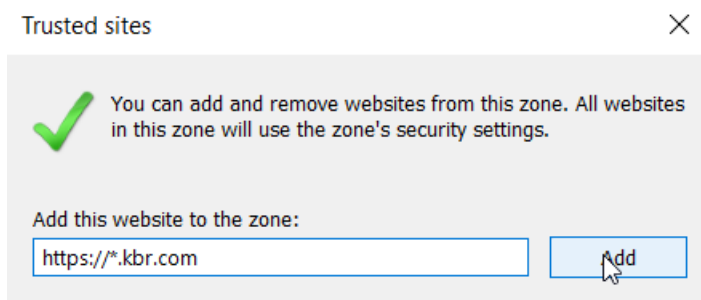
1. Open **Internet Explorer**.
2. Click on the **Tools** menu (gear icon) and select **Internet Options**.



3. Select the **Security** tab



4. Click on the Trusted Sites icon, then click the *Sites* button. In the **Add this website to the zone:** box, enter **https://*.kbr.com** and click **Add**, then **Close**.



5. Close the browser and re-try access to the application.

NOTE: The problem is evident no matter which web browser (Internet Explorer, Chrome, or Firefox) is being used. The change must be made in Internet Explorer to resolve the problem.

[Table of Contents...](#)