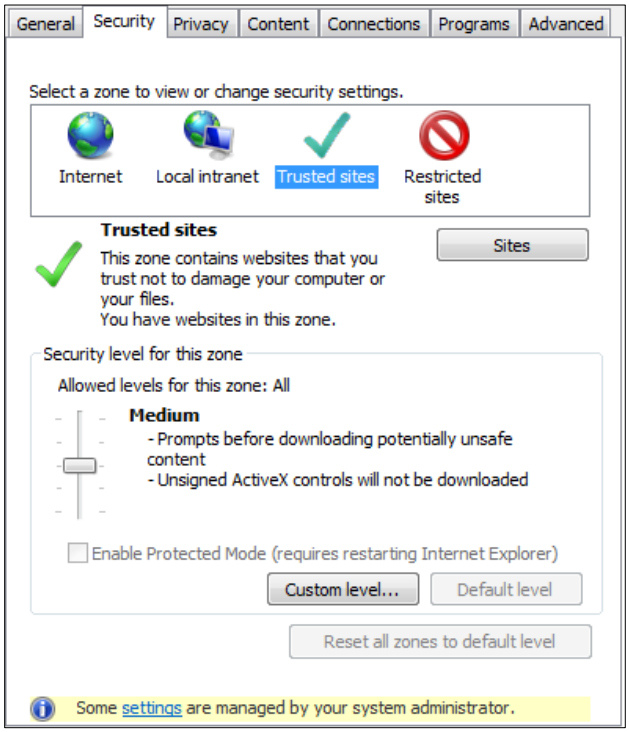
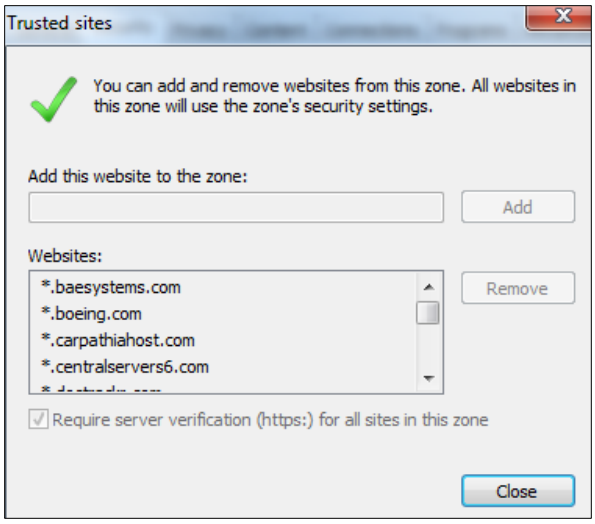
# FAQs: Digital Certificate Service

- **What is DCS?**
  - DCS stands for Digital Certificate Service. This services allows a user to install a Medium Level of Assurance Digital Certificate to their computer or to a token which then can be used to sign documents.
- **How do I obtain a hardware token?**
  - You will need to obtain a hardware token from your Organization Administrator.
- **Can I share my token with someone else?**
  - Tokens cannot be shared. Each user needs their own token.
- **Do I always have to use my Phone OTP credential to access my application?**
  - Yes, you will always need to access the DCS application using Phone OTP.
- **What is the difference between Medium Level of Assurance Hardware and Software?**
  - Software certificates are stored on a computer. Hardware certificates are stored on an external token that you will need to plug into your computer to use them.
- **How do I configure my browser settings for DCS?**
  - **Adding Exostar as a Trusted Internet Site (Required) Step Action**
    1. Launch Internet Explorer.
    2. From the Menu Bar, select **Tools** and click **Internet Options**. The Internet Option page opens. This page allows users view and modify Internet Explorer settings.
    3. Select the **Security tab** and then click **Trusted Sites**. Then click the **Sites** button on the right side of the panel.

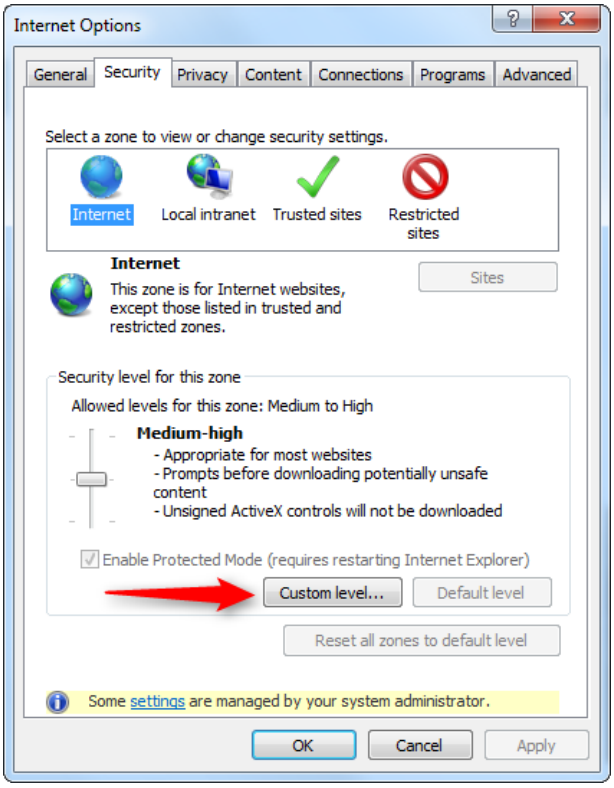



This opens the **Trusted Site** page:




4. In the **Add this web site to the zone** edit box, enter **https://*.exostar.com**. Click the **Add** button.
5. When finished, click the **OK** or **Close** to return to the **Internet Options Menu**. Note: If this website has been previously added, you may receive a message indicating it is already in the Trusted Site Zone.

- **Security Settings for ActiveX (Required)**
  1. On the **Internet Options page**, under the **Security tab**, select **Custom level**:



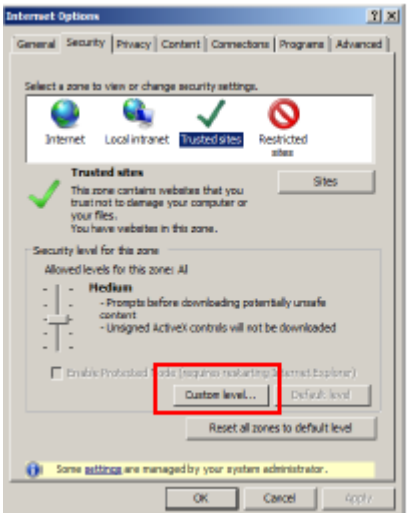
2. Verify the **Security Settings – Trusted Sites Zone** settings are as follows:

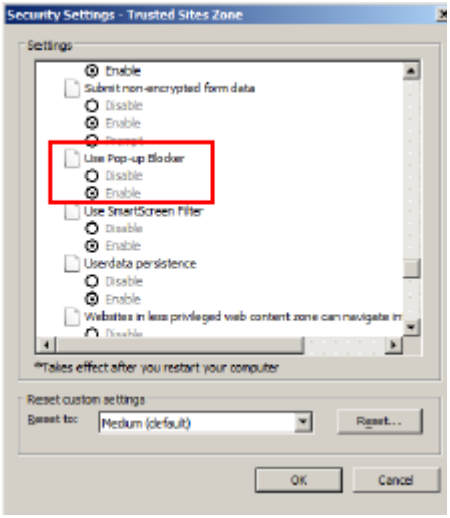
| ActiveX Controls and Plug-in Settings | Value |
|---|---|
| Allow previously unused ActiveX controls to run without prompt | Enable |
| Automatic prompting for ActiveX controls | Enable |
| Binary and Script behaviors | Enable |
| Download Signed ActiveX controls | Enable |
| Run ActiveX controls and plug-ins | Enable |
| Script ActiveX controls and plug-ins | Enable |

NOTE: Settings will take effect after you restart internet explorer.

3. Once settings are changed, click **OK** twice to save. Modifications will take effect after you restart Internet Explorer.

- **Popup Blocker (Required)**
  1. From the Internet Options page, select the Security tab, and click the **Custom level** for Security Level for this Zone.



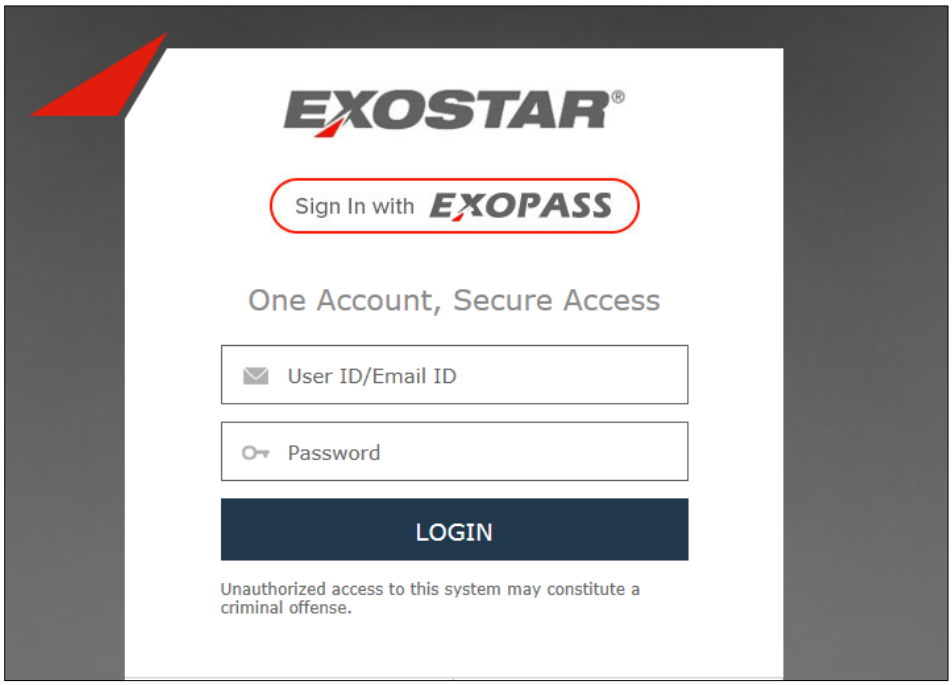




2. Verify that the following **Security Settings – Trusted Sites Zone** are set as follows:

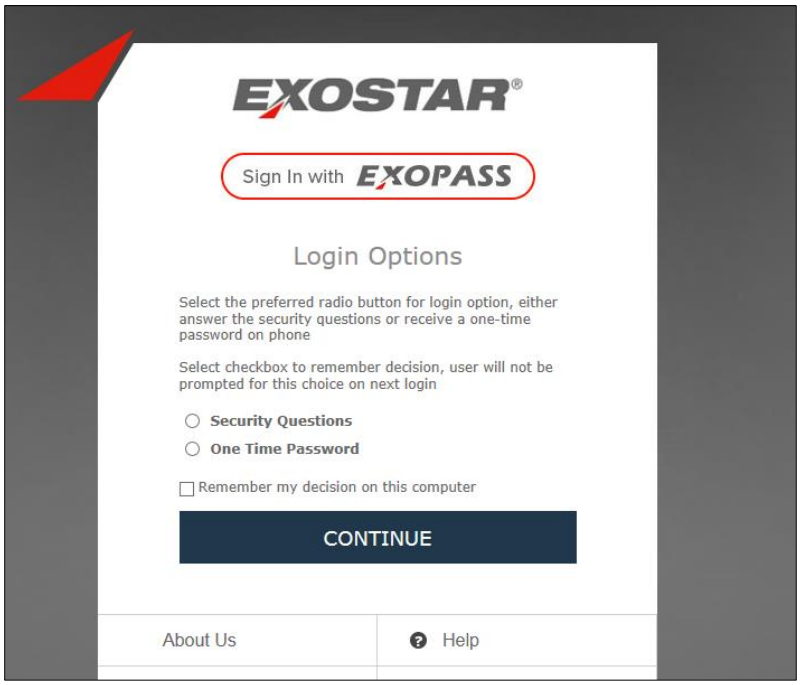
| Miscellaneous Settings | Value |
|---|---|
| Use Popup Blocker | Disable |

The **Use Popup Blocker** setting will disable popup blocking for all web sites in the Trusted Internet zone. Once settings are changed, click **OK** twice to save. Modifications will take effect after you restart Internet Explorer.

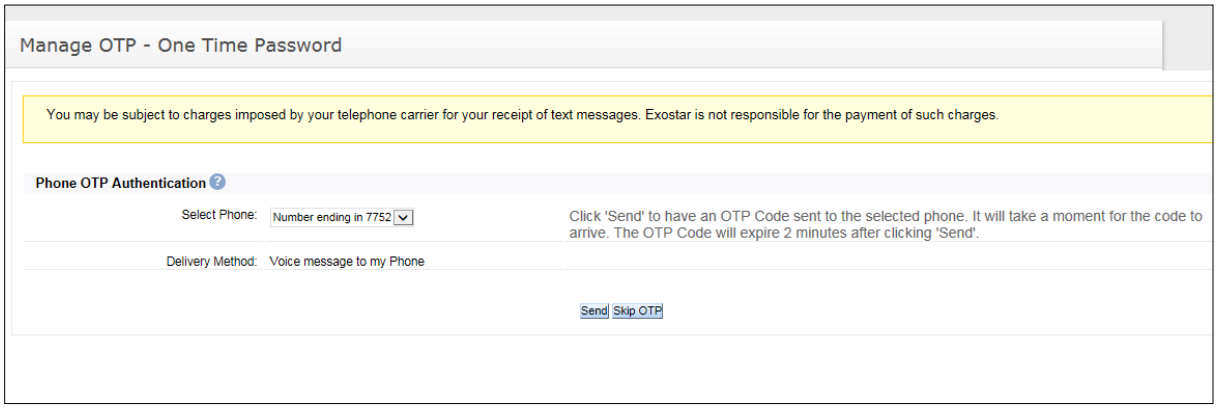
- **How do I log into my Exostar Secure Access Management (SAM) account with my Phone OTP credential?**
    1. Launch Internet Explorer.
    2. In the URL bar, enter https://secureaccess.exostar.com.
    3. You will be presented with the login screen where you will need to enter your user id and password. Click **Login**.



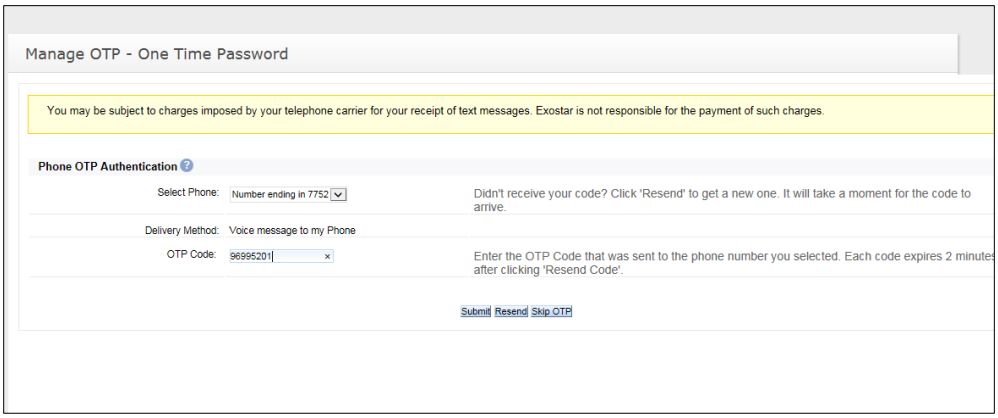

    4. After you have clicked **Login**, you will be presented with a login options screen. Select the **One Time Password** radio button and click **Continue**.



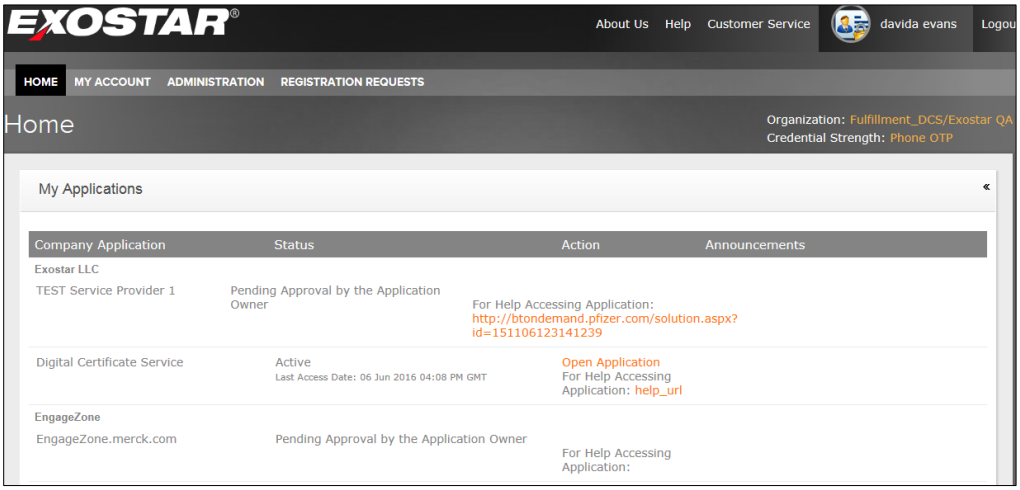

5. You will be prompted to enter the One Time Password associated with the phone you registered on your account. Select the phone code to be sent to and click **Send**.




6. You will receive the One Time Password to the phone number you selected. Enter the code you received and click **Submit**.

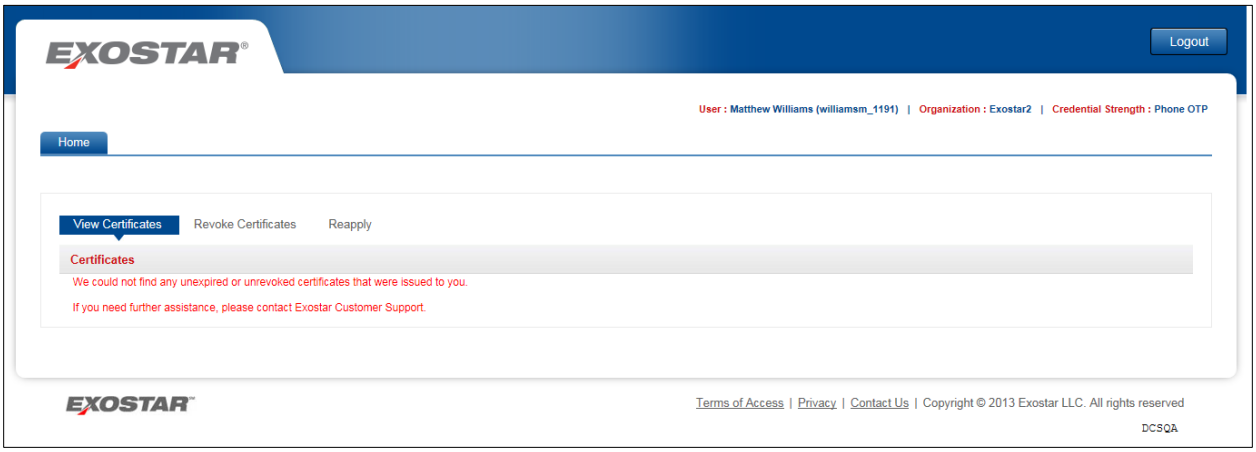



7. You will now be logged into your SAM account with your Phone OTP. The **Credential Strength** should say **Phone OTP** (located in the right hand corner).

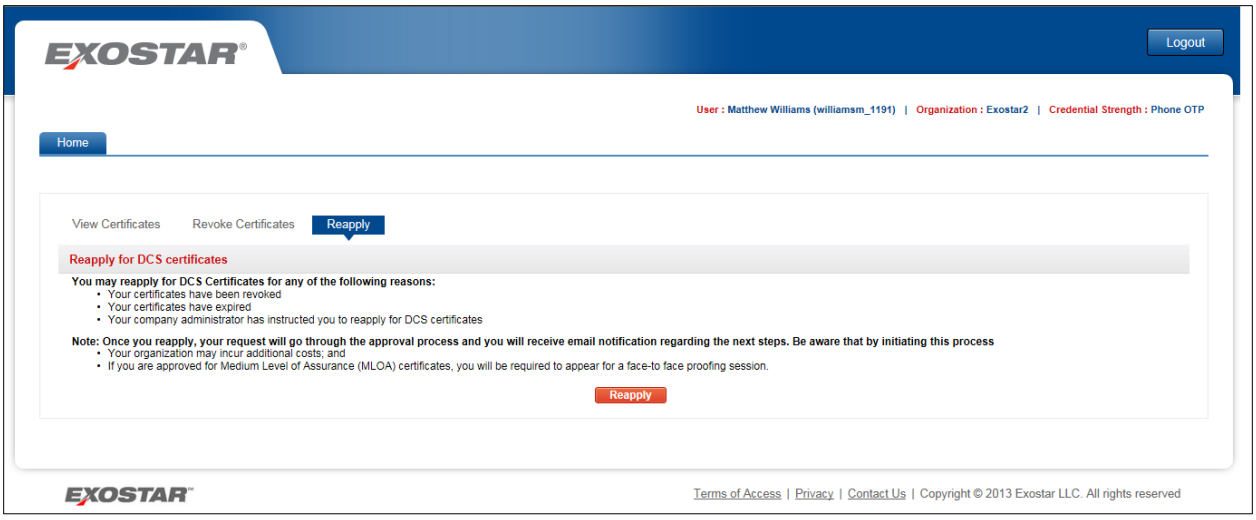



- **How can I determine if my computer is configured properly to download the certificate?**
    - You will need to run the system check. This diagnostic check will ensure that your computer is configured properly and that there are no hidden issues. You can access the system check at http://myexostar.com/systemcheck/?persona=dcs.
- **I am trying to download the certificates and receive an error message: "The ActiveX Control is not installed or is not running. You need to install it or run it before you can proceed". Why am I receiving this error and what should I do?**
    - This error will be displayed when you attempt to download the digital certificates and the Exostar ActiveX control is being blocked/cannot be downloaded. The most common causes for this error are Internet Explorer settings and/or system level permissions that are not set correctly and therefore do not allow the download and use of Exostar's ActiveX control.

- **Why don't I see the Enroll option in DCS to obtain Medium Level of Assurance certificates?**
    - If you previously had certificates installed or revoked, the **Enroll** button will be unavailable.

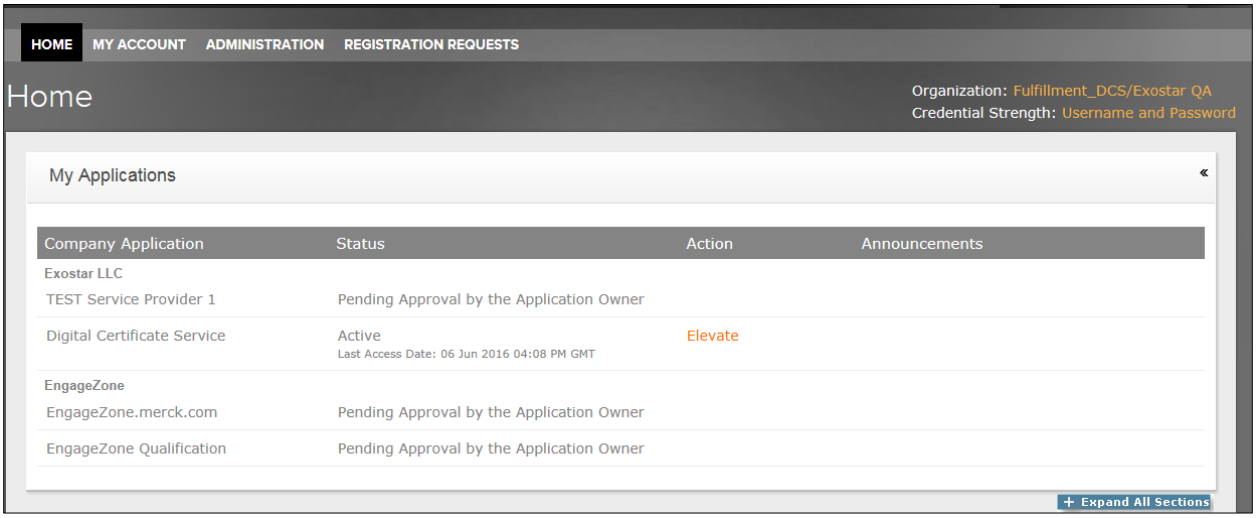



    - To obtain certificates, you will need to click **Reapply** to request new certificates. Select the certificate type, validity period and the reason why you are requesting the certificate. If you are unsure of what to enter, select **Unknown**. This information can be modified by the DCS Administrator.

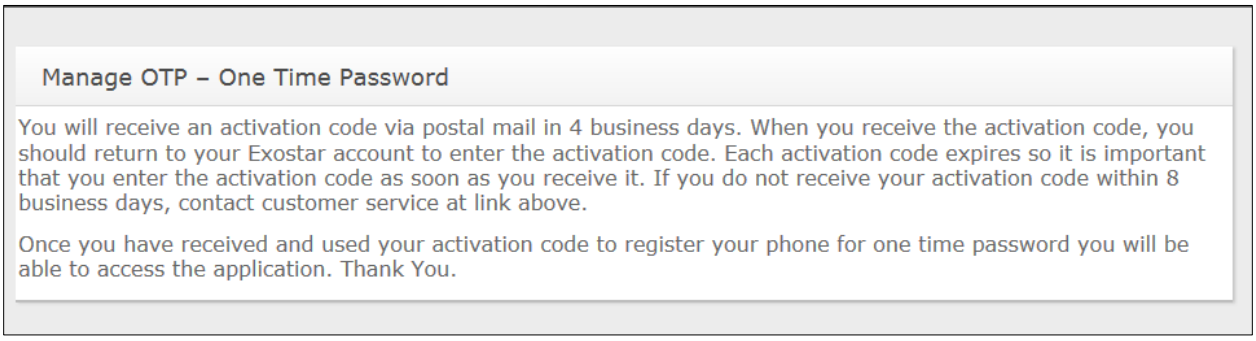



- **What if I see elevate under the actions column next to DCS?**
    - If you do not see **Open Application for DCS** but see **Elevate**, click **Elevate** to upgrade your credential strength from **username and password** to **Phone OTP**.
        - You will be prompted to log in with the Phone OTP credential to upgrade your credential strength to **Phone OTP**.

- Once you successfully log in with your Phone OTP, your credential strength will change from username and password to Phone OTP. Elevate will change to **Open Application**:




- **Why was I directed to the mail option during my Phone OTP activation process?**
  - If you do not answer the questions correctly but Experian can locate you, you will receive your activation code via postal mail in four business days.

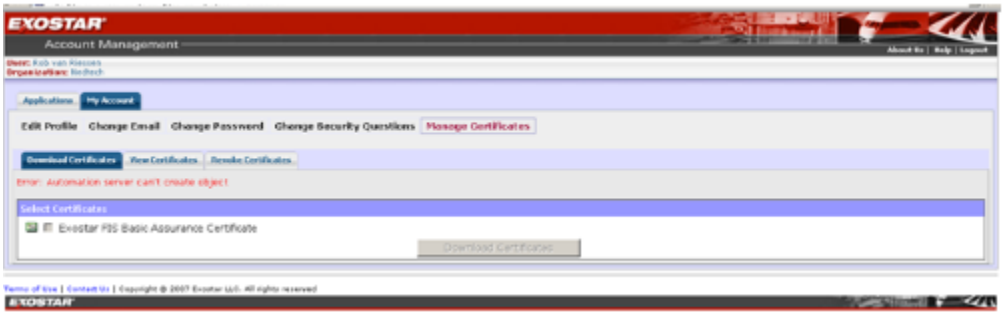



- **I get an error screen with only 'Yes' or 'No' options when I attempt to download the certificates? What happens when I click on 'No'?**

  Due to a known Microsoft issue (documented in the Microsoft Knowledge Base article # 940275), the dialog box appears as shown above and does not contain the intended informational message that is supposed to be displayed. When you encounter this error, select "Yes".

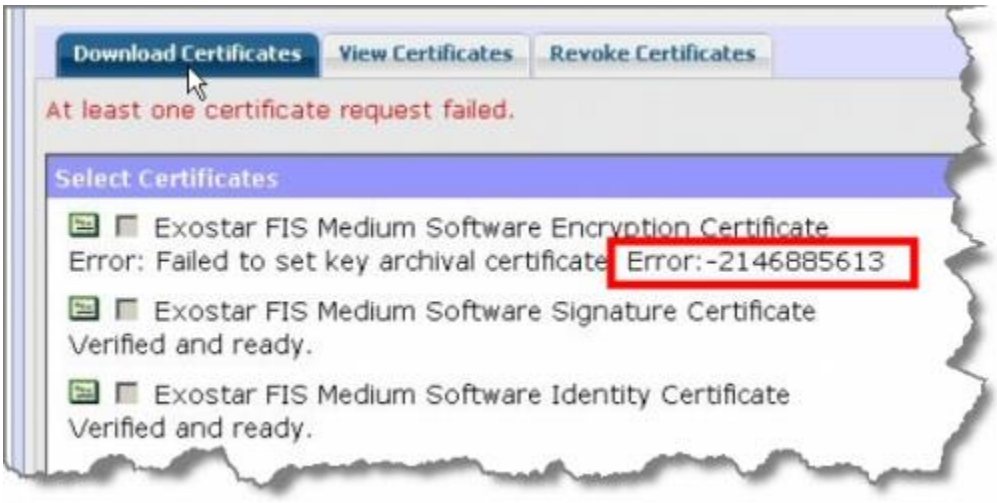
  - If you click on "No", you will receive the following message and will need to restart the download process: "**Error! Filename not specified**."

- **I have a digital certificate. I am trying to download the certificates and receive an error message: “Automation server can't create object”**




  - This error will be displayed when you attempt to download the digital certificates and the Exostar ActiveX control is blocked or cannot be downloaded. The most common causes for this error are Internet Explorer settings and/or system level permissions that are not set correctly and therefore do not allow the download and use of Exostar's ActiveX control. Refer to the Certificate Download Requirements document.

- **I am attempting to download my Medium Level of Assurance Certificates. I receive the following error message with error code # 2146885613**




  - This error message is received when either the Exostar Certificate Revoke List URL is blocked by the proxy/corporate policies. To confirm the issue, try to access the following two sets of URLs. If either of these URLs fails, then you need to contact IT Support within your organization to ensure that the host name is added to the list of "allowed" URLs. FIS/DCS URLS: (Host URL: http://www.fis.evincible.com)
    - FIS Root CA 2.crl
    - FIS Root CA 2.p7c
    - FIS Signing CA 2.crl
    - FIS Signing CA 2.p7c
    - DCS Signing CA 1.crl
    - DCS Signing CA 1.p7c

- **How do I backup my DCS Certificates?**
  - Please see the How to Backup Your Certificate guide under the DCS section on www.myexostar.com.

- **How do I import my MLOA/BLOA certificates to a Windows Vista machine (exported from Windows XP or older versions)?**
  - Microsoft has identified an issue with importing certificates to Windows Vista machines (exported from Windows XP or Windows 2000). To successfully use the certificates backed-up from an older version to Vista, follow the steps below:

    **1.** Download the Microsoft patch to the Windows Vista machine and follow the details provided under the Resolution section. Please review all information on the site to appropriately download the patch: http://support.microsoft.com/kb/970730

**2**. Download the exported certificates to your Windows Vista machine. Refer to the How to Backup Your Certificate guide under the DCS section on www.myexostar.com.

- **How do I enable strong private key protection for Medium Level of Assurance Certificates?**
    - If you have existing certificates for which you would like to enable strong authentication, you need to back-up and import the certificate. Refer to the How to Backup Your Certificate guide under the DCS section on www.myexostar.com.
    - **IMPORTANT:** Please note that for MLOA certificates, you need to ensure that you back-up your certificate appropriately. If the certificate is corrupted/lost during this process, you will need to re-apply for the certificate.

- **How can I use my MLOA digital certificates to digitally sign my email?**
    - Refer to your email client documentation for details. e.g., Microsoft Outlook.

- **Can I use my digital certificates after leaving my job at my current employer?**
    - Your certificate contains attributes that uniquely associate you to your employer. If you leave this employer, the certificate information will not be valid.

- **How can my organization designate multiple FIS administrators?**
    - During the DCS subscription process, one user can be assigned the DCS Administrator role. To add an additional DCS Administrator, the Organization Administrator can upgrade a user account as follows:

1. Designate a user to assign the DCS Administrator role and access their SAM details page by going to the Administration tab.
2. If the user has an existing SAM account, you will need to search for the user. When the users appears, click on the hyperlinked user id.
4. Scroll to the Application to Administer section and select "Application Admin" from the Role drop-down list.
3. An application list is now available for selection. Select Digital Certificate Service (DCS).
4. Click Continue and then review the changes you have made.
5. Click Submit to save the changes.

The user will receive an email providing information that their account has been upgraded to the DCS Administrator role. This process may be utilized to upgrade a user to an administrator role for any other application.

**NOTE:** The Organization Administrator can also set-up a new user account with the administrator roles by selecting the appropriate role from the Role drop-down list. Refer to the Secure Access Manager (SAM) Admin Training Guide section "*Adding New Users"* for detailed step-by-step information.