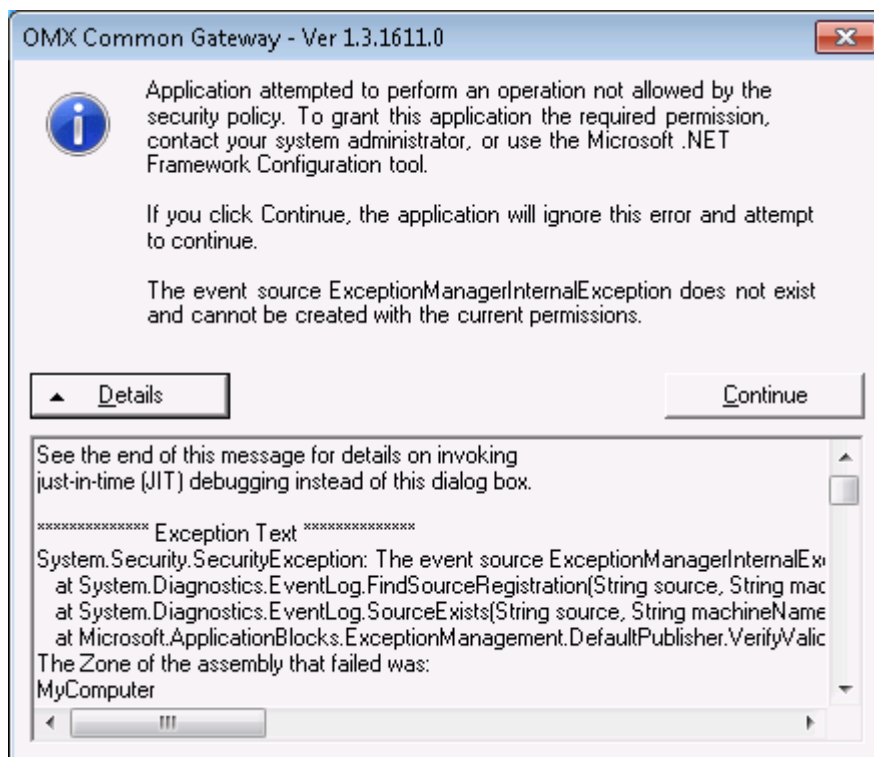




- [.NET error during logon to Common Gateway GUI or HTHL](#)
 - [A System Error has Occured. Information about the error has been logged in your event log.](#)
 - [A technical problem was experienced. Details: Operation Failed: Invalid client certificate details](#)
 - [A technical problem was experienced - Details: Operation failed: This version of the client application is not compatible with the server currently used.](#)
 - [A technical problem was experienced. Details of the problem have been captured in the application log for further analysis.](#)
 - [A technical problem was experienced while attempting to log in. Details: Operation failed: RSA SecurID passcode validation failed. Please check the passcode and try again.](#)
 - [Access is forbidden. Please check that certificates are valid.](#)
 - [Account is either disabled or password has expired](#)
 - [Blank page with text](#)
 - [Can't install Weblauncher MSI](#)
 - [Can't launch executable: Request for the permission of type 'System.Security.Permissions...](#)
 - [Could not establish trust relationship with the server](#)
 - [Digital ID could not be Installed](#)
 - [Invalid Client Certificate DetailsE](#)
 - [Login Error - System.Web.Services.Protocols etc.](#)
 - [Microsoft .NET - Unhandled exception has occurred in your application...Configuration system failed to initialize](#)
 - [Microsoft .NET - Unhandled Exception has occurred in your application...Attempted to read or write protected memory...](#)
 - [Missing or Incomplete menu option](#)
 - [No executable file to start or The application that you downloaded is not a valid application](#)
 - [One of the sub-systems has reported a critical error. Unable to continue...](#)
 - [Online Error status: 100a](#)
 - [Page cannot be displayed or access denied](#)
 - [Release 3.1 Expected error messages](#)
 - [The archive file that is downloaded to the local computer is not valid](#)
 - [The deployment manifest for the application requires a different version of the Weblauncher than is currently installed on the system](#)
 - [The Request Failed with HTTP status 401:Unauthorised](#)
 - [The request failed with HTTP status 403: Forbidden](#)
 - [Unable to establish a secure communication channel to the server \(Forbidden\)](#)
 - [Unauthorized to access the download page. Please check the login details and try again. Failed to get executable](#)
 - [Unauthorized to access the download page OR The system could not log you on](#)
 - [Verisign can't issue a certificate](#)
 - [When I click the link, Nothing happens](#)
-

.NET error during logon to Common Gateway GUI or HTHL



Application: Common Gateway GUI or HTHL client

Connectivity Type: ANNI or Internet

Deployment Type: File Deployment

Cause: It is an expected error message after a user made a mistake on entering their logon account to the Common Gateway GUI. Normally, the client will send a correct error message, If it followed by the .net error, meaning, the user's account has no security rights to modify the event log in the machine.

Incident Response: If they want to get away with this error message, they need to run the SWGUI.exe as an admin and then attempt to deliberately logon using an incorrect account.

Upon doing this, the GUI will create the log in the event log. Once created, the user will not receive the .net error anymore. It will use the CGWY log created in the Event Log from then on.

A System Error has Occured. Information about the error has been logged in your event log.

Application: Exigo GUI

Connectivity Type: ANNI or Internet PC

Deployment Type: Web browser or File deployment

Causes:

1. During logon to EXIGO, the connectivity timed out.
2. The user never used EXIGO for a long period of time
3. High memory usage in the machine

Incident Response:

After exiting from the login GUI, wait for 5 minutes and try the login process again.

If the error message still appears, please contact your IT support to check of any PC network issue or if connectivity is experiencing any performance issue. Also, try to restart the machine.

If the above did not resolve the problem, try to go to a machine where another user successfully logged on to EXIGO recently. In that machine, go to Documents and Settings\User Profile\Application Data\Local Settings\SECUR. Under SECUR folder, there are files with a very long File names like example below:

OM.SECUR.PI.BSO.InstrumentClass, OM.SECUR.PI.BSO, Version=6.5.0.235, Culture=neutral, PublicKeyToken=8941f02d31442b70, Host=ASX Austraclear

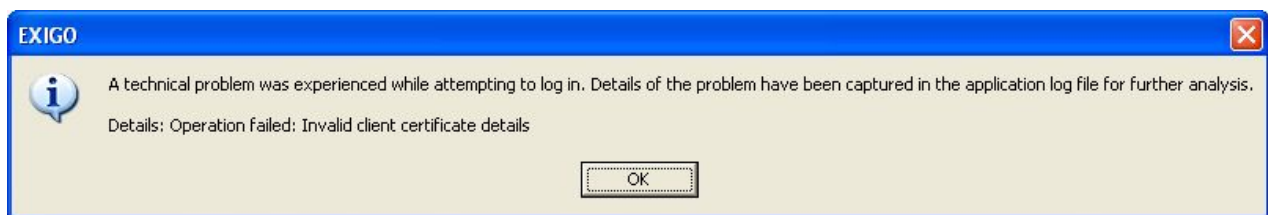
There will be at least 3 files in that directory with long file names like this. Their IT should copy all those files and transfer it to the affected machine under the same directory.

If it is still didn't work, please request your IT to recreate your user profile in the machine.

Escalation:

Run the Compatibility Checker, and send the log report it to Austraclear Helpdesk, together with the screenshot of the error message and the Event Log.

A technical problem was experienced. Details: Operation Failed: Invalid client certificate details



Application:
Weblauncher

Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web Browser or File deployment

Cause:
Invalid certificate details, Expired Certificate, Certificate without private key.

Incident Response:

- Make sure that the certificate that you are using is paired with your Austraclear user id
- Make sure that the certificate is not expired
- Check that your certificate has a private key or exportable. To check this, you need to perform the following:
 - Launch Internet Explorer.
 - Go to Tools->Internet Options->Content->Certificates
 - Highlight the certificate->Click Export->next
 - Make sure that the option 'Yes, export the private key' can be ticked or it is not grayed out.
 - If you can't ticked the option 'Yes', it means that your certificate was installed without the private key or the certificate gone corrupted. to correct this, you need to uninstall this certificate and re-import your backup certificate. If you do not have a back up certificate, you need to request to revoke this certificate and apply for a new one.

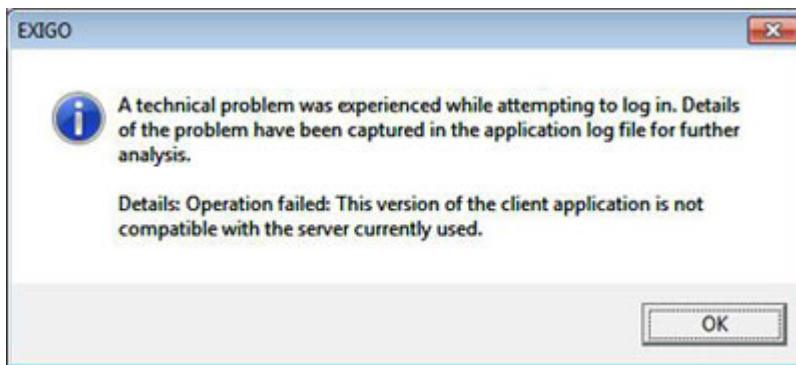
Related Document : https://www.asxonline.com/intradoc-cgi/groups/participant_services/documents/participantapplicationkitsfe/asx_038038.pdf

Escalation:

Please provide the following to Austraclear Helpdesk:

- 1) Screenshot of the error message and the screenshot of the certificate to proving it has a private key.
- 2) Compatibility checker
- 3) Exigo log

A technical problem was experienced - Details: Operation failed: This version of the client application is not compatible with the server currently used.



Application:

Exigo GUI

Connectivity Type:

ANNI or Internet PC

Deployment Type:

File deployment

Cause:

Current EXIGO version is not correct (user is still trying to use the previous version of the GUI).

Incident Response:

Install the correct version for File Deployment.

Exigo User can obtain the new version by calling the Austraclear Helpdesk.

A technical problem was experienced. Details of the problem have been captured in the application log for further analysis.

Application:

Exigo GUI

Connectivity Type:

ANNI or Internet PC

Deployment Type:

Web browser or File deployment

Cause:

Bad install of the Weblauncher; High Memory usage in the machine; .Net version is incorrect

Incident Response:

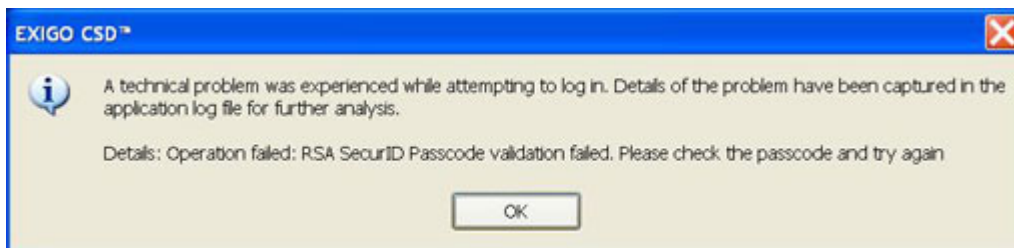
- Uninstall/Re-install Weblauncher. Related document:
http://www.asx.com.au/images/settlement/9.4_Web_Launcher_3_1_Installation_Guide.pdf
- Restart your machine, and check with your IT support any network degradation issue.
- Run the compatibility checker and check the log report of any inconsistencies with the .net version

Escalation:

Send the following logs and information to Austraclear Helpdesk

1. Compatibility Checker Log
2. Screenshot of the actual error message
3. EXIGO Log file
4. Event System and Application Log

A technical problem was experienced while attempting to log in. Details: Operation failed: RSA SecurID passcode validation failed. Please check the passcode and try again.



Application:
Exigo GUI

Connectivity Type:
Internet PC

Deployment Type:
Web browser or File deployment

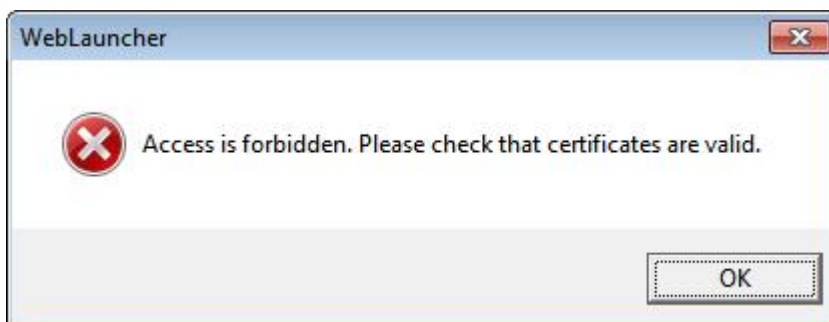
Cause:
Invalid RSA SecurID PIN or Passcode

Incident Response:

1. Close existing EXIGO login session and make sure that the correct RSA pin + token is being entered.
2. Call Austraclear Helpdesk to check if the RSA pin and token is enabled.

Austraclear Helpdesk can reset the PIN if the identified workaround doesn't solve the problem.

Access is forbidden. Please check that certificates are valid.



Application:
Exigo GUI

Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web browser or File deployment

Causes:

1. EXIGO user is using a corrupt certificate or a certificate without private key.
2. EXIGO user certificate private key gone missing
3. EXIGO user certificate does not match with their EXIGO user account.

Incident Response:

1. Check that you are using the certificate that is paired with the EXIGO username and password
2. Check that the certificate has not expired.
3. Check that the certificate is not corrupted. If the certificate is corrupted, a valid certificate must be re-installed.
4. Open the certificate and ensure that the 'yes' export the private key is not greyed out. Otherwise, you will need to re-install the certificate.

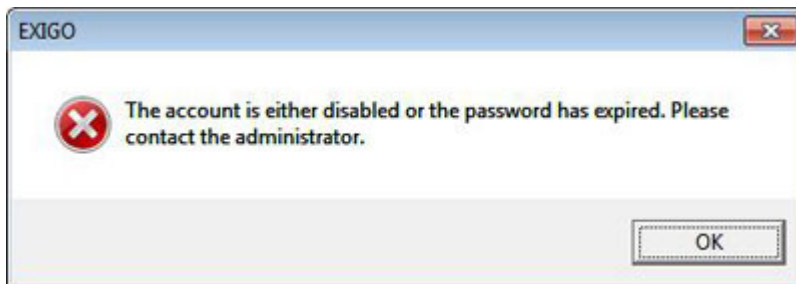
Make sure that the option 'Yes, export the private key' can be ticked or it is not grayed out. If you can't ticked the option 'Yes', it means that your certificate was installed without the private key or the certificate gone corrupted. to correct this, you need to uninstall this certificate and re-import your backup certificate. If you do not have a back up certificate, you need to request to revoke this certificate and apply for a new one.

Related Document : https://www.asxonline.com/intradoc-cgi/groups/participant_services/documents/participantapplicationkitsfe/asx_038038.pdf

Escalation:

If the steps above do not resolve the issue, it may be necessary to call the Austraclear Helpdesk and ask them to check if the certificate has been revoked.

Account is either disabled or password has expired



Application:
Exigo GUI, Weblauncher, Common Gateway GUI

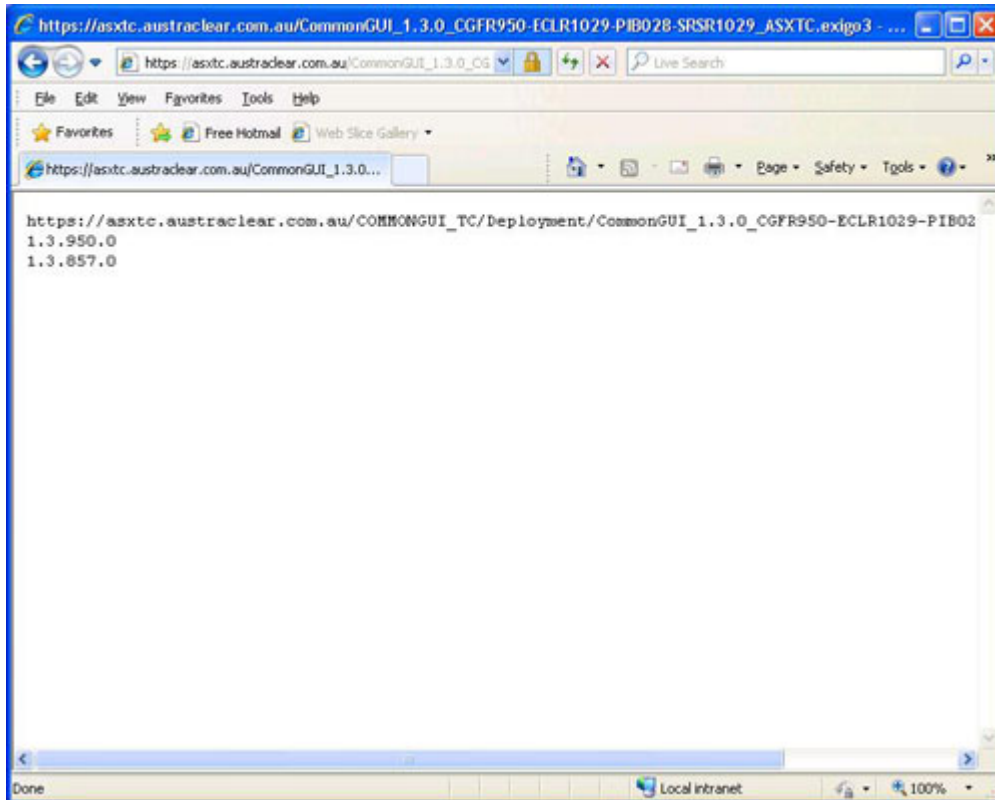
Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web browser or File deployment

Cause:
EXIGO user account must be locked.

Incident Response:
Ask your Austraclear administrator to unlock user account.

Blank page with text



Application:
Weblauncher

Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web browser

Cause:
No Weblauncher Installed

Incident Response:
Install the latest Weblauncher. Please make sure that the install will be done by someone's account with admin rights.

Related Document: http://www.asx.com.au/images/settlement/9.4_Web_Launcher_3_1_Installation_Guide.pdf

Can't install Weblauncher MSI



Application:
Weblauncher

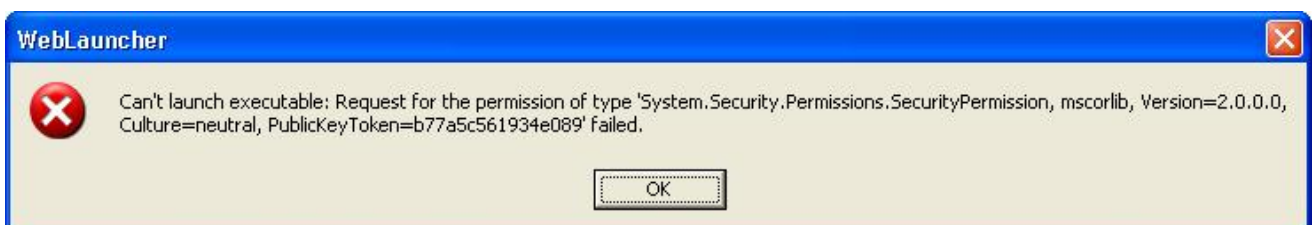
Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web browser

Cause:
Corrupt User's Profile

Incident Response:
Re-create the users profile. Please make sure that your IT support perform this.

Can't launch executable: Request for the permission of type 'System.Security.Permissionsns...



Application:
Weblauncher

Connectivity Type:
ANNI or Internet PC

Deployment Type:

Web browser

Cause:

1. The weblauncher was installed by someone without admin rights.
2. Security permissions requirement.

Incident Response:

Re-install the weblauncher while using an account with admin rights.

Make sure that the local directory has no lockdown policy.

Escalation:

Run the compatibility Checker and send the log and error screenshots to Austraclear Helpdesk.

Related Document: http://www.asx.com.au/images/settlement/9.4_Web_Launcher_3_1_Installation_Guide.pdf

Could not establish trust relationship with the server



Application:

Weblauncher

Connectivity Type:

ANNI or Internet PC

Deployment Type:

Web browser

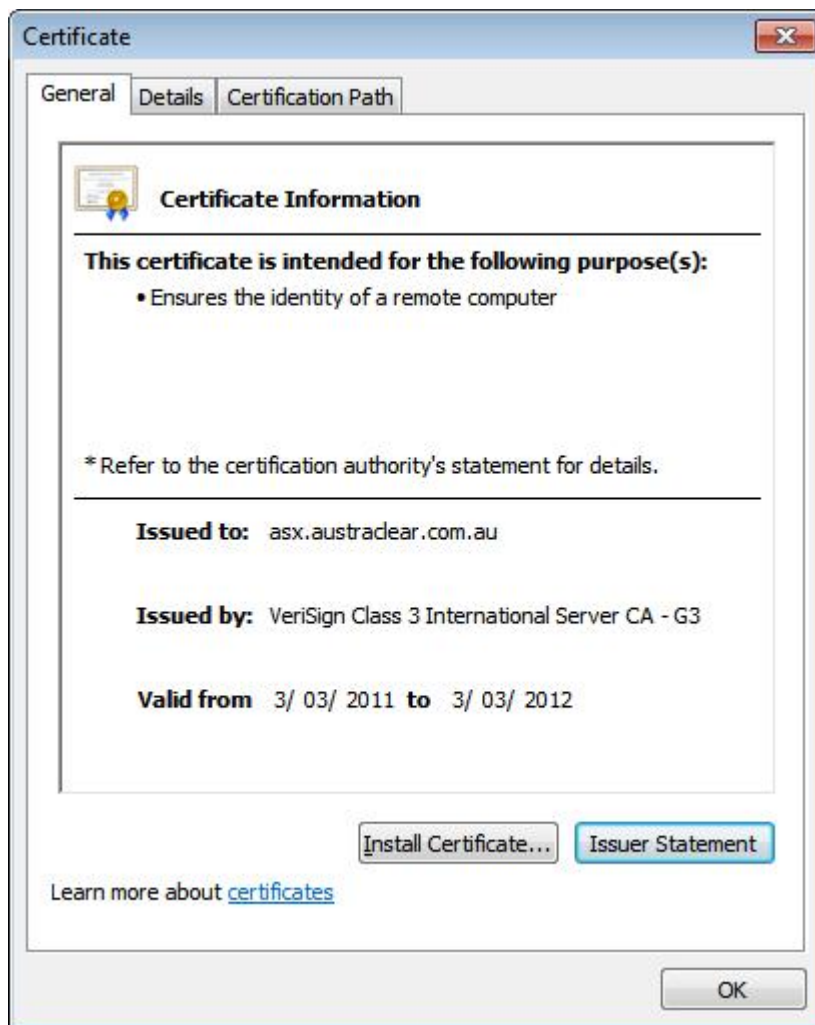
Cause:

Not using the current VeriSign CA

Incident Response:

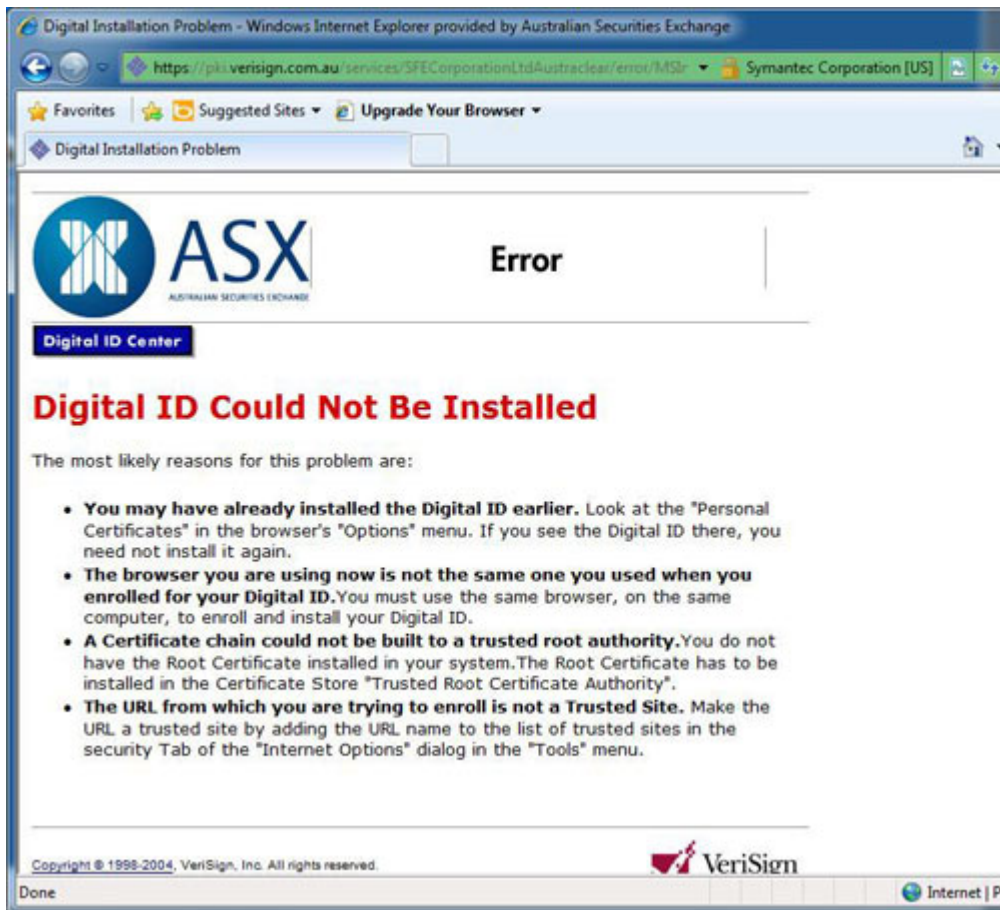
Check if the PC has the current VeriSign cert installed.

1. At the IE browser, type <https://asx.austraclear.com.au>
2. Then go to Safety->Security Reports->View certificate
3. The certificate must be clean or without any X. Example of a working cert:



If the cert does not appear as above, install the certificate into Trusted Root Certification. Your IT support can help you with this. Any questions, please ring Austraclear Helpdesk.

Digital ID could not be Installed



Connectivity Type:
ANNI or Internet PC

Cause:
In Windows 7, there is some instance that the SFE CA is not properly installed.







The result of this would be, the Certificate that you enrolled will not be saved in your machine and instead, an error message will appear (as above) after enrolment.

Incident Response:
To test the validity of CA, Go to Digital Certificate enrolment Page,

Click Install CA

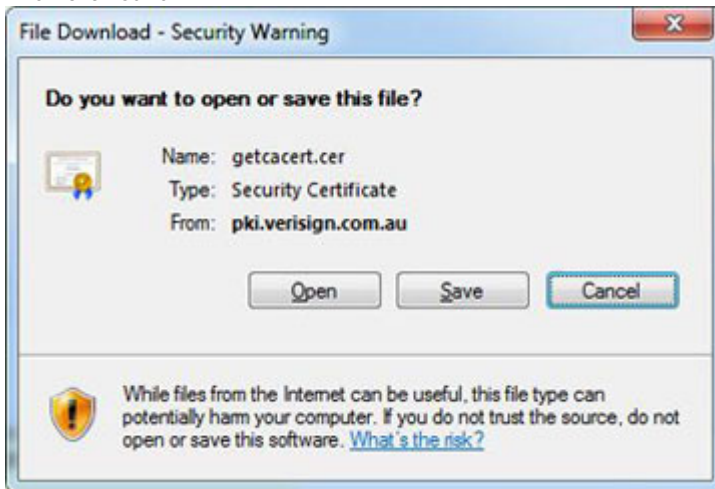


SFE Corporation Ltd Austraclear Digital ID Center

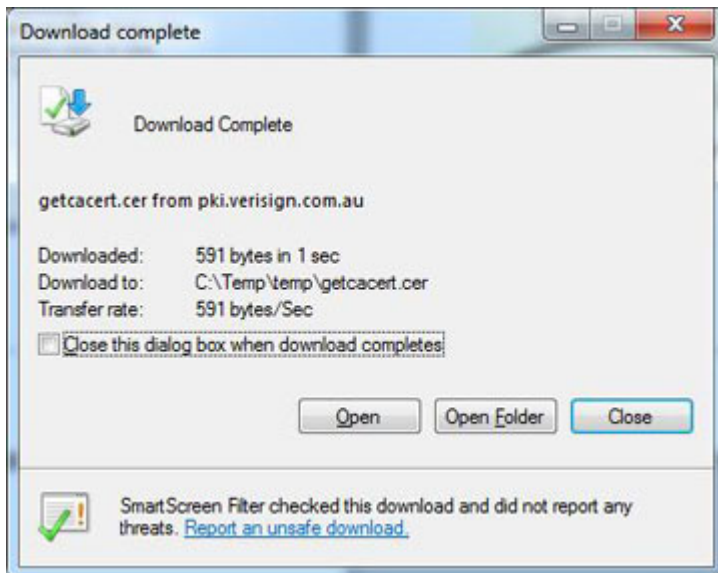
-  **ENROLL**
Choose this option to enroll for a client Digital ID.
-  **PICK UP ID**
Choose this option if you enrolled for a Digital ID but did not pick it up.
-  **SEARCH**
Choose this option to search for a Digital ID. This function is useful for determining whether a Digital ID is valid, expired, or revoked. You may also download IDs from this option.
-  **RENEW**
Choose this option to renew a Digital ID which is expiring or which has already expired. You should generally start renewing your Digital ID at least one month before your Digital ID is due to expire.
-  **REVOKE**
Choose this option to revoke your Digital ID. Digital IDs should be revoked immediately for any suspected compromise, including lost or stolen private keys, corrupted key pairs, change in site ownership, or suspected fraud.
-  **INSTALL CA**



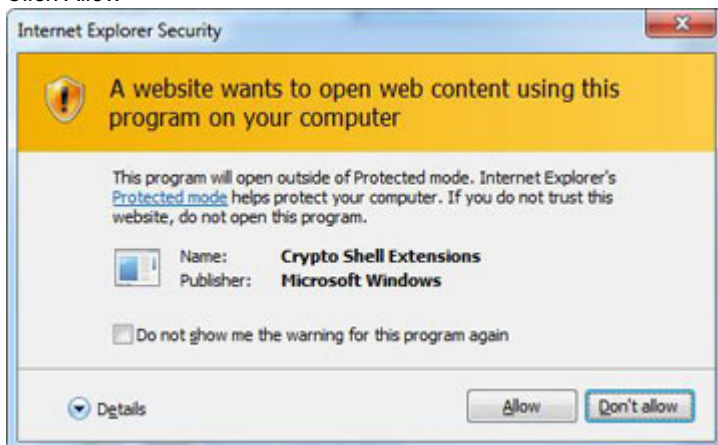
Then click save



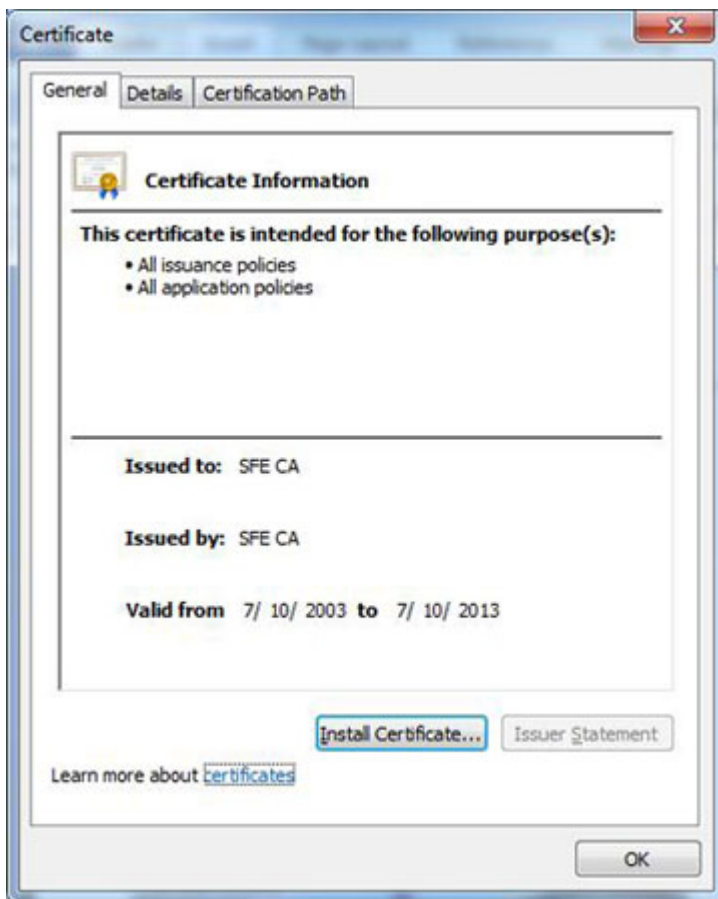
Then click open



Click Allow



This will appear if the CA is valid



If the certificate is showing a RED X Mark, it means that the certificate is not trusted, the following must be done:

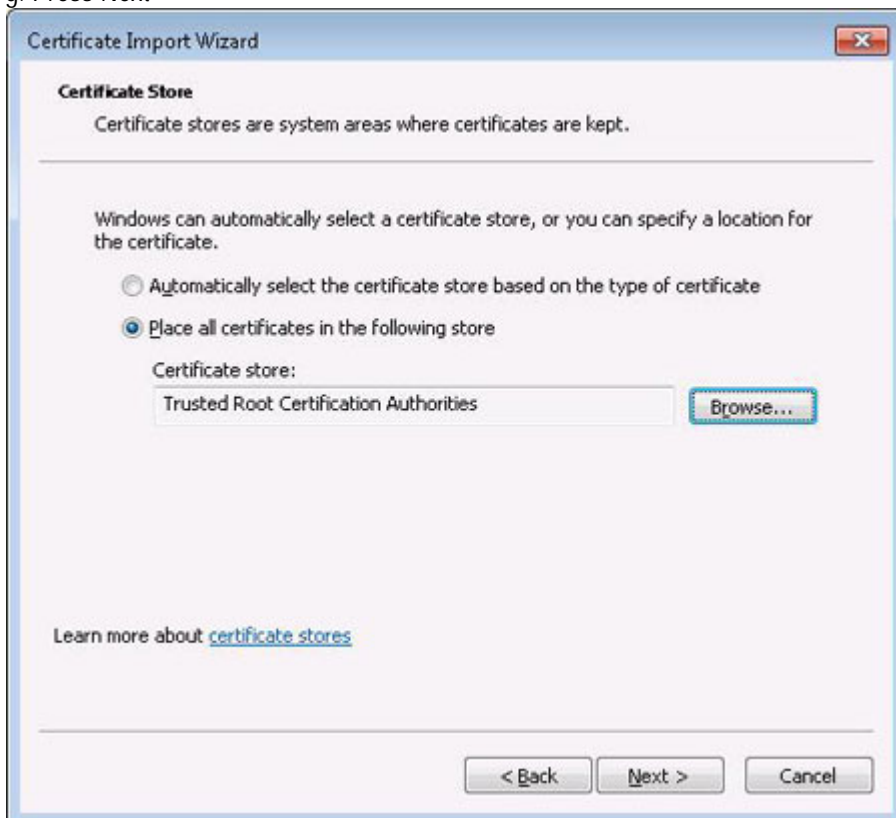
a. On the same window, Press Install Certificate



- b. Click NEXT
- c. Select Place All Certificates in the following Store
- d. Click Browse
- e. Select Trusted Root Certification Authority



- f. Press OK
- g. Press Next



- h. Then finish

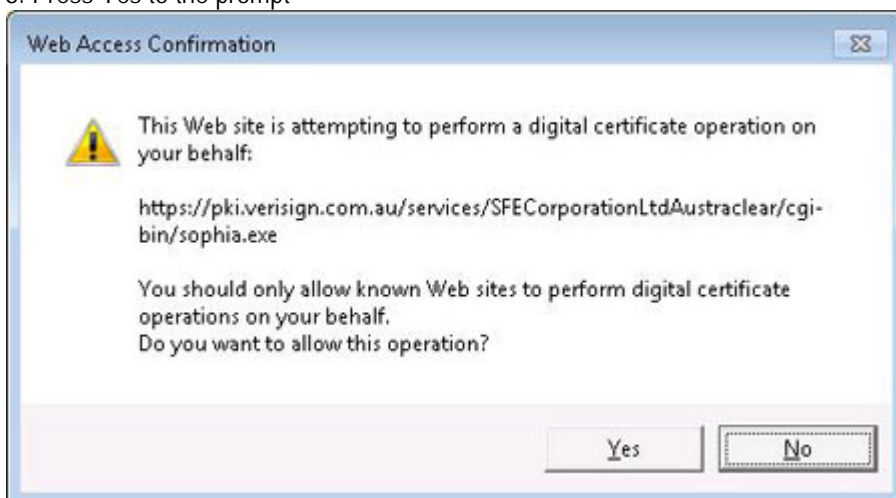
To pick up the previously enrolled certificate, the following must be done.

Make sure that you are using the same machine where you enrolled your certificate.

1. Go to Digital Certificate Enrolment Page
2. Press SEARCH
3. Enter the email address associated with your certificate
4. Choose from the valid certificate in the list
5. Press Download
6. Select the ID format as 'My ID for Microsoft Internet Explorer/Outlook Express/Outlook'



7. Press Submit
8. Press Yes to the prompt

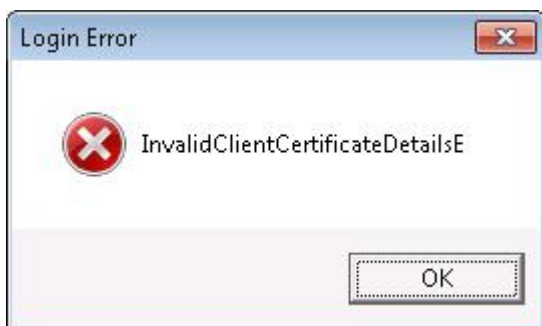


9. Then the success page must display:



10. The Certificate is now successfully enrolled and downloaded.

Invalid Client Certificate DetailsE



Application:
Common Gateway GUI

Connectivity Type:
ANNI or Internet PC

Causes:
Invalid certificate details, expired certificate, or certificate without private key.

Incident Response:
User must enter a correct username that matches with their certificate.
Close the application and try to log in again.

1. Check if you are using a valid certificate that match with your account
2. Check if your certificate has not expired
3. Check if your certificate has a private key. To check, try to export your certificate, the option "yes, export the private key" should not be greyed out.

Related Technical Document: https://www.asxonline.com/intradoc-cgi/groups/participant_services/documents/participantapplicationkitsfe/asx_038038.pdf

Escalation:

If your certificate has expired or does not have the private key (and no back up) you will need to request a new one by contacting the Austraclear Helpdesk.

Login Error - System.Web.Services.Protocols etc.



Application:
Common Gateway GUI

Connectivity Type:
ANNI or Internet PC

Cause:

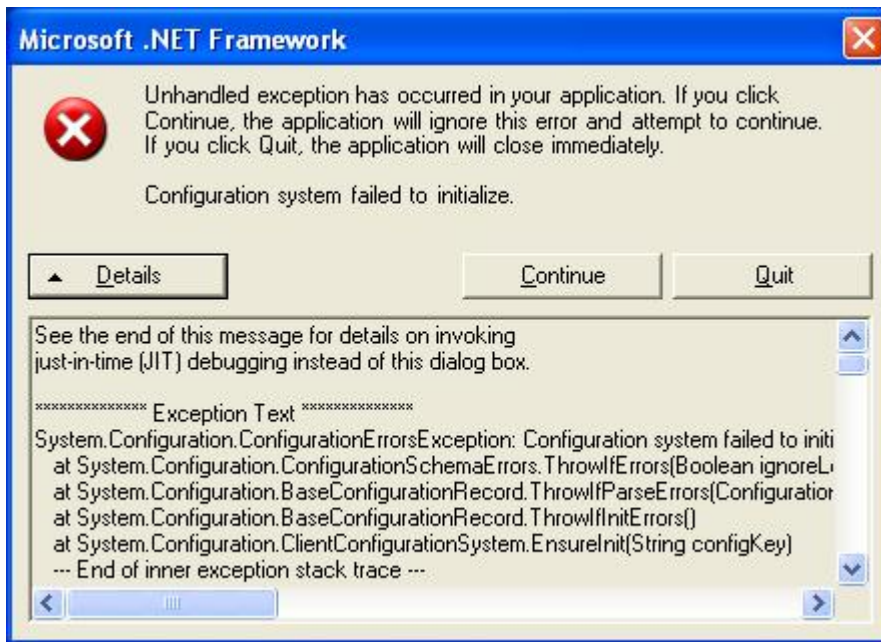
1. Common Gateway GUI user is not entering the correct RSA pin or token number.
2. RSA token is currently disabled
3. RSA token require a re-sync.

Incident Response:

User must close any Common Gateway GUI session before attempting to log in.

1. Make sure that the user is entering their RSA pin and token during login
2. Call Austraclear Helpdesk to check if the RSA token is currently disable
3. Call Austraclear Helpdesk to check if the RSA need to be re-synchronised.

Microsoft .NET - Unhandled exception has occurred in your application...Configuration system failed to initialize



The error message happened after the login to the Weblauncher.

Application:
Weblauncher

Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web browser

- Cause:
1. Weblauncher was installed by someone without admin rights.
 2. Bad install of the Weblauncher
 3. Incorrect Version of .net

- Incident Response:
1. Check if you are using the correct version of .net 2.0 by running the compatibility checker
 2. If 1 is true, uninstall the Weblauncher and install, this time with someone with admin rights.

Related http://www.asx.com.au/images/settlement/9.4_Web_Launcher_3_1_Installation_Guide.pdf Technical Document:

Escalation:
Send the Compatibility log to Austraclear Helpdesk. If you can't run the compatibility checker, you can download the manual version from here. (You need to unzip the content and install it on your machine).

Microsoft .NET - Unhandled Exception has occurred in your application...Attempted to read or write protected memory...



The error message happened after clicking the link.

Application:
Weblauncher, Common Gateway GUI

Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web browser

Causes:

1. Weblauncher was installed by someone without admin rights.
2. Bad install of the Weblauncher
3. Incorrect Version of .net
4. .Net is corrupted or affected by other applications

Incident Response:

1. Check if they are using the correct version of .net 2.0 by running the compatibility checker
2. If 1 is true, uninstall the Weblauncher and install, this time using someone's account with admin rights.
3. If point 1 and 2 did not resolve the problem, replace or reset user's profile (This is applicable to Cause number 4 above). Please consult your IT support before attempting to do this.

Related

Technical

Document:

http://www.asx.com.au/images/settlement/9.4_Web_Launcher_3_1_Installation_Guide.pdf

Escalation:

Run the Compatibility Checker and send the compatibility log to Austraclear Helpdesk.

Missing or Incomplete menu option

Application:
Exigo GUI

Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web browser or File deployment

Causes:

1. After logon to EXIGO, the client did not load all functionality in a timely fashion
2. High memory usage in the machine

Incident Response:

After exiting from the login GUI, wait for 5 minutes and try the login process again.

If the error message still appears, please contact your IT support to check of any PC network issue or if connectivity is experiencing any performance issue. Also, try to restart the machine.

If the above did not resolve the problem, try to go to a machine where another user successfully logged on to EXIGO recently. In that machine, go to Documents and Settings\User Profile\Application Data\Local Settings\SECUR. Under SECUR folder, there are files with a very long File names like example below:

OM.SECUR.PI.BSO.InstrumentClass, OM.SECUR.PI.BSO, Version=6.5.0.235, Culture=neutral, PublicKeyToken=8941f02d31442b70, Host=ASX Austraclear

There will be at least 3 files in that directory with long file names like this. Their IT should copy all those files and transfer it to the affected machine under the same directory.

If it is still didn't work, please request your IT to recreate your user profile in the machine.

Escalation:

Run the Compatibility Checker, and send the log report it to Austraclear Helpdesk, together with the screenshot of the error message and the Event Log.

No executable file to start or The application that you downloaded is not a valid application



During the download of the EXIGO GUI, the above error message appeared, then followed by either of the error messages below:

The application you downloaded is not a valid application. OR No Executable file to Start

Application:
Weblauncher

Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web browser

Cause:

- It took time to download the GUI (over 10 minutes) and the connectivity to Austraclear timed out.
- EXIGO zip that was downloaded was incomplete.
- Local PC Security setting account is causing the issue.

It took time to download the GUI (over 10 minutes) and the connectivity to Austraclear timed out.

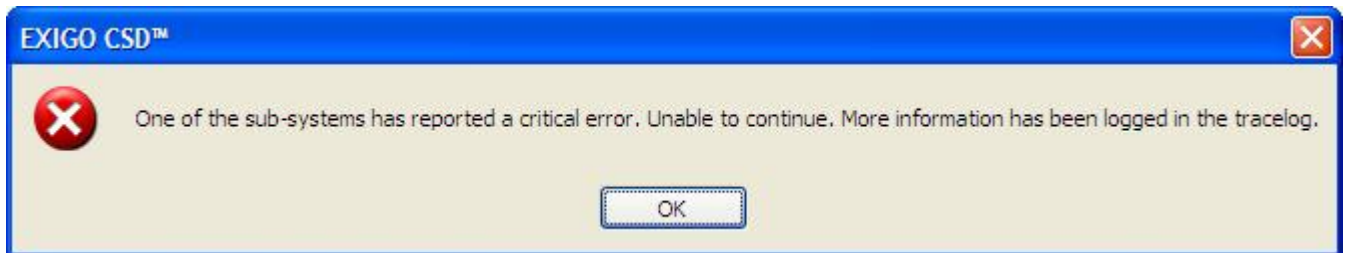
Incident Response:

1. Delete any zip file in C:\Users\- 2. Contact your IT support to check that there's no network degradation in your PC connectivity.
- 3. Contact your IT support to check if you have restriction applied on file download to your PC.

Escalation:

If the problem persists, run the Compatibility Checker and escalate to Austraclear Helpdesk with the log file generated from Compatibility Checker, Error Screen Shot and the Event Log.

One of the sub-systems has reported a critical error. Unable to continue...



Application:

Exigo GUI

Connectivity Type:

ANNI or Internet PC

Deployment Type:

Web browser or File deployment

Causes:

1. During logon to EXIGO, the connectivity timed out.
2. The user never used EXIGO for a long period of time

Incident Response:

After exiting from the login GUI, wait for 5 minutes and try the login process again.

If the error message still appears, please contact your IT support to check of any PC network issue or if connectivity is experiencing any performance issue. Also, try to restart the machine.

If the above did not resolve the problem, try to go to a machine where another user successfully logged on to EXIGO recently. In that machine, go to Documents and Settings\User Profile\Application Data\Local Settings\SECUR. Under SECUR folder, there are files with a very long File names like example below:

OM.SECUR.PI.BSO.InstrumentClass, OM.SECUR.PI.BSO, Version=6.5.0.235, Culture=neutral, PublicKeyToken=8941f02d31442b70, Host=ASX Austraclear

There will be at least 3 files in that directory with long file names like this. Their IT should copy all those files and transfer it to the affected machine under the same directory.

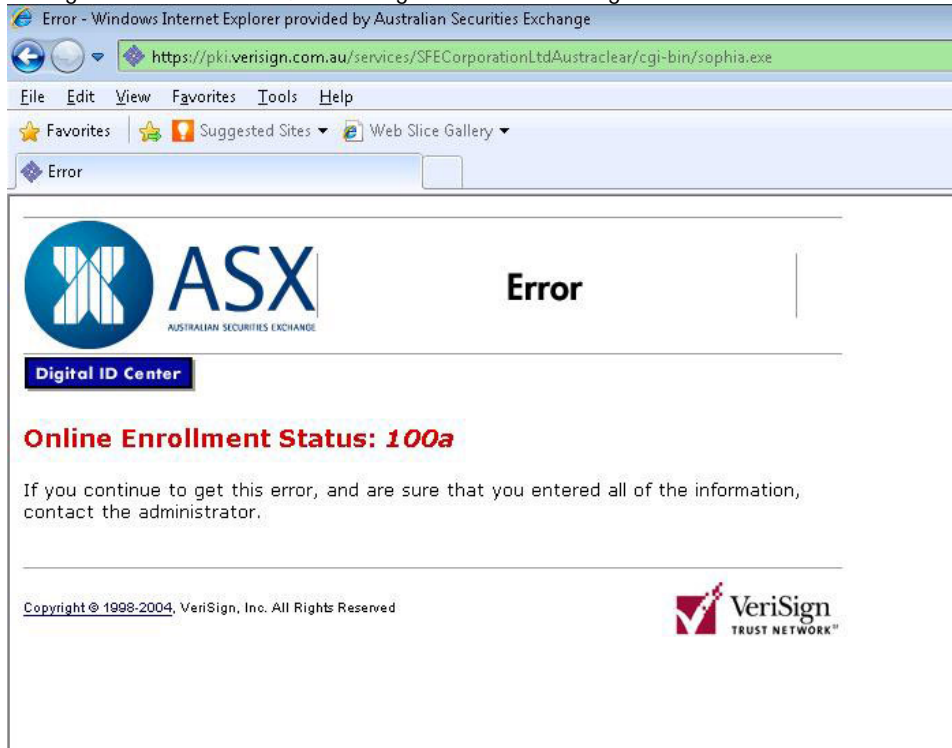
If it is still didn't work, please request your IT to recreate your user profile in the machine.

Escalation:

Run the Compatibility Checker, and send the log report it to Austraclear Helpdesk, together with the screenshot of the error message and the Event Log.

Online Error status: 100a

During Certificate Renewal, the user got this error message.

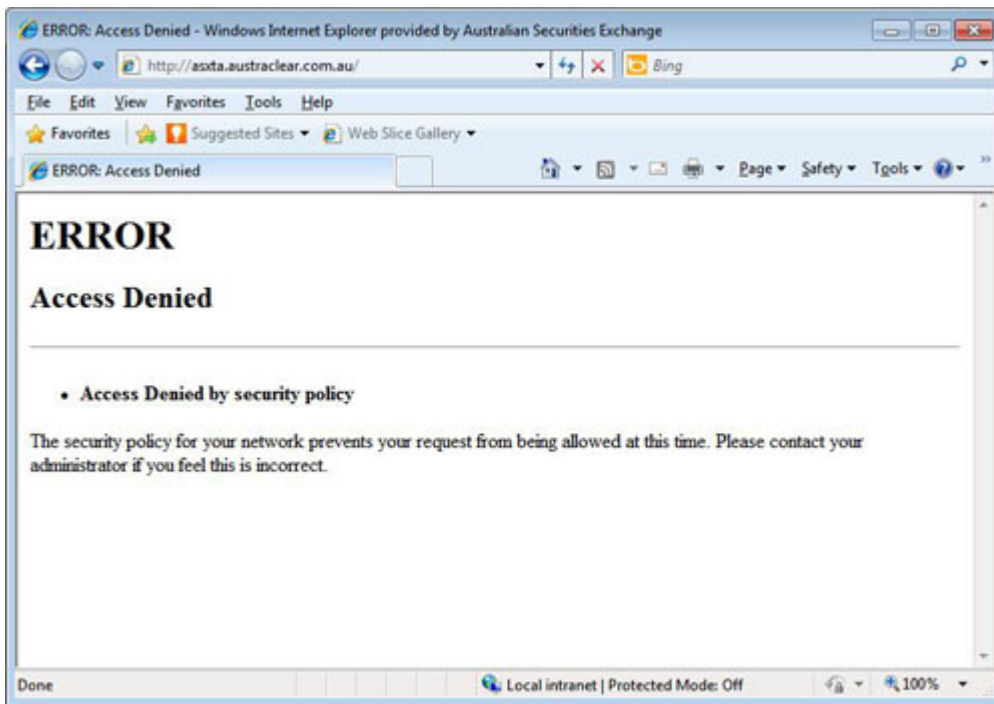


Connectivity Type:
ANNI or Internet PC

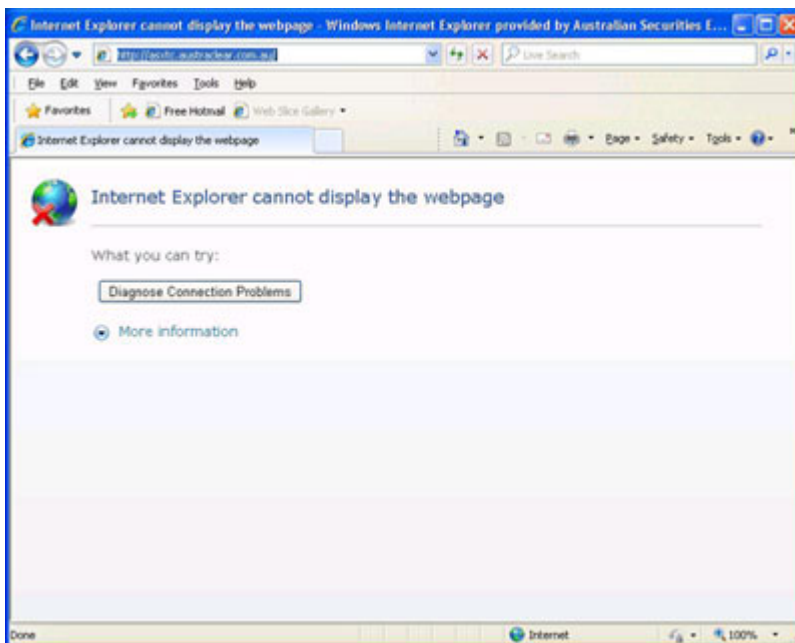
Cause:
You are trying to renew a certificate that already past the expired date.

Incident Response:
Please enroll for a new certificate rather than using the renew option.

Page cannot be displayed or access denied



OR



Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web browser

Causes:

1. No Connectivity to EXIGO
2. Not using https
3. Misspelled url
4. Certificate not valid

Incident Response (for cause 1-3):

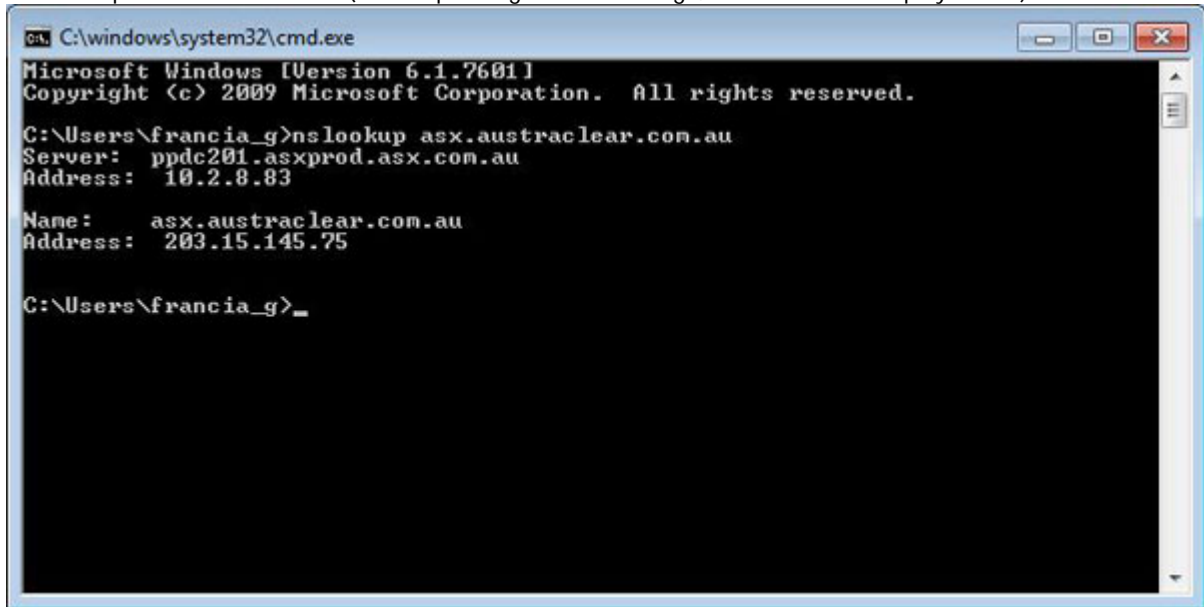
1. Check if the webpage typed in the browser is: <https://asx.austraclear.com.au>
2. Call your IT to check if you have a connectivity to EXIGO.

The following test must be done to check the EXIGO connectivity:

1) NSLOOKUP

At the command prompt type: nslookup asx.austraclear.com.au

Result as per screenshot below (note depending on their settings, the IP address display differs).



```
C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\francia_g>nslookup asx.austraclear.com.au
Server: ppdc201.asxprod.asx.com.au
Address: 10.2.8.83

Name: asx.austraclear.com.au
Address: 203.15.145.75

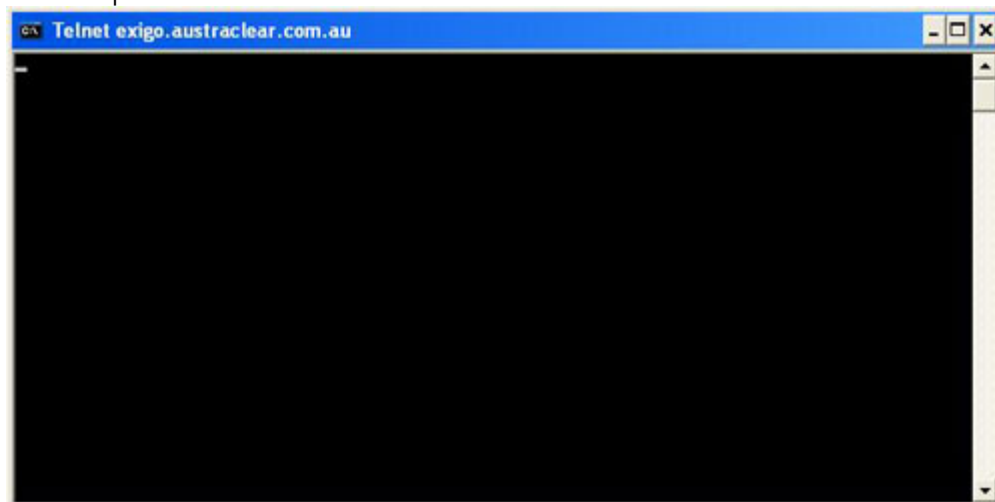
C:\Users\francia_g>_
```

If this can't be done or if the command did not give the expected result, go to point number 2:

2. TELNET

At the command prompt, type, telnet asx.austraclear.com.au 443

Result as per screenshot below:



```
Telnet exigo.austraclear.com.au
```

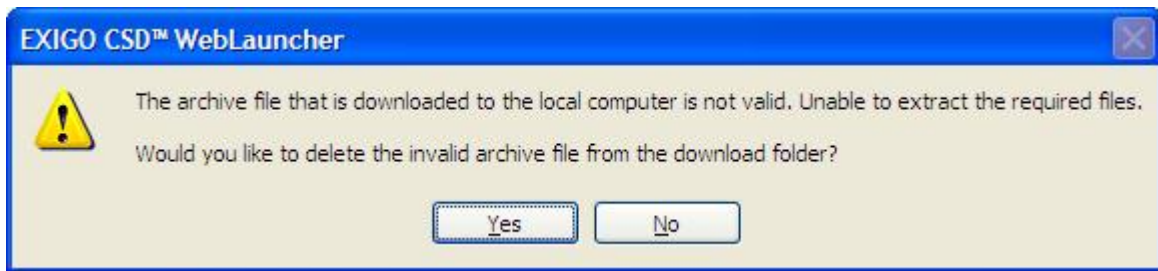
Escalation:

If the test can't be done or if the command did not give the expected result, escalate to Austraclear Helpdesk.

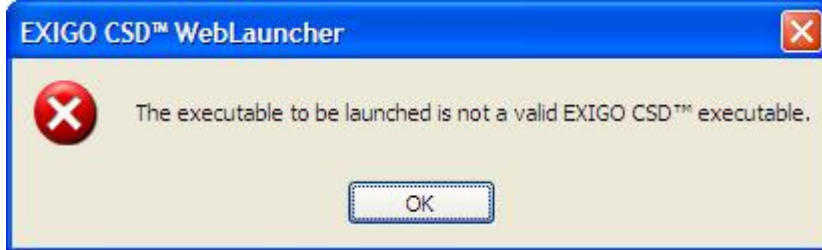
Release 3.1 Expected error messages

Please see the document for common [Release 3 error messages](#) (PDF 184KB)

The archive file that is downloaded to the local computer is not valid



Then it could be followed by (after pressing No to delete the corrupt file) the error message below



Application:
Weblauncher

Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web browser

Cause:

It took time to download the GUI (over 10 minutes) and the connectivity to Austraclear timed out. EXIGO zip that was downloaded was incomplete.

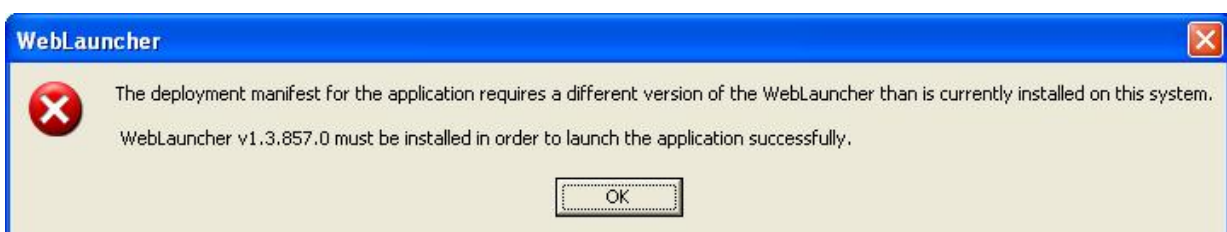
Incident Response:

1. Delete any zip file in C:\Users\- 2. Redownload The GUI

Escalation:

If the problem persists, run the Compatibility Checker and escalate to Austraclear Helpdesk with the log file generated from Compatibility Checker, and the Event Log.

The deployment manifest for the application requires a different version of the Weblauncher than is currently installed on the system



Application:
Weblauncher

Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web browser

Cause:
Wrong version of Weblauncher being used.

Incident Response:

1. Advise the user to uninstall the old version and install the new version of the Weblauncher

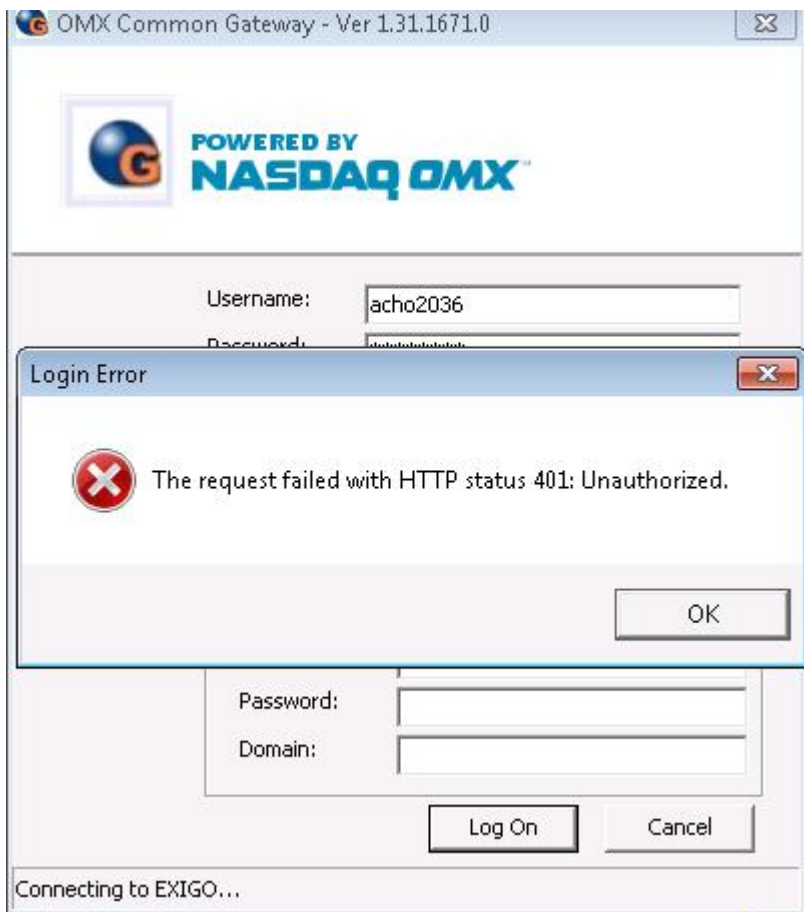
Related

Technical

Document:

http://www.asx.com.au/images/settlement/9.4_Web_Launcher_3_1_Installation_Guide.pdf

The Request Failed with HTTP status 401:Unauthorized



Application:
Common Gateway GUI

Connectivity Type:
ANNI or Internet PC

Cause:
Wrong password or password has expired

Incident Response:

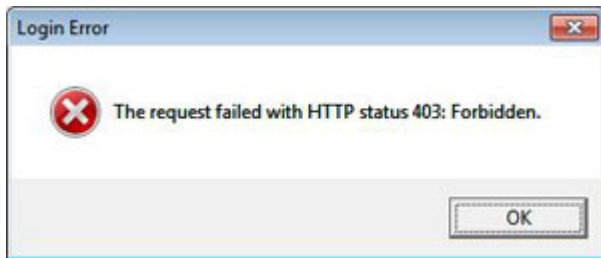
1. Check if you are entering the correct password and user ID pair

2. Check if your password has expired
3. Check any spaces or special character that were typed in the user id or password.

Escalation:

Contact Austraclear Helpdesk.

The request failed with HTTP status 403: Forbidden



Application:
Common Gateway GUI

Connectivity Type:
ANNI or Internet PC

Cause:
Common Gateway user is using either:

1. Invalid certificate
2. Corrupt certificate
3. Certificate with no private key
4. Expired certificate

Incident Response:

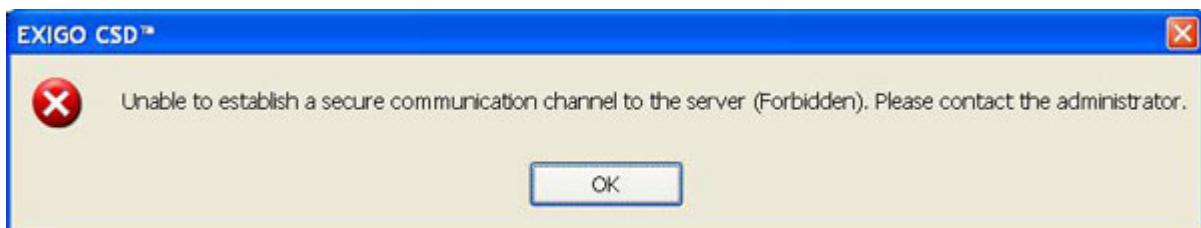
1. Check if you are selecting the correct digital certificate
2. Check if you are using a valid certificate (not expired or certificate must have a private key).
3. Check if your certificate has a private key. To check, try to export your certificate, the option "yes, export the private key" should not be greyed out.

Related Technical Document: https://www.asxonline.com/intradoc-cqi/groups/participant_services/documents/participantapplicationkitsfe/asx_038038.pdf

Escalation:

If your certificate has expired or does not have the private key (and no back up) you will need to request a new one by contacting the Austraclear Helpdesk.

Unable to establish a secure communication channel to the server (Forbidden)



Application:
Weblauncher

Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web browser

Cause:

1. EXIGO user is using a corrupt certificate or a certificate without private key.
2. EXIGO user certificate private key gone missing
3. EXIGO user certificate does not match with their EXIGO user account.

Incident Response:

Ask the user to:

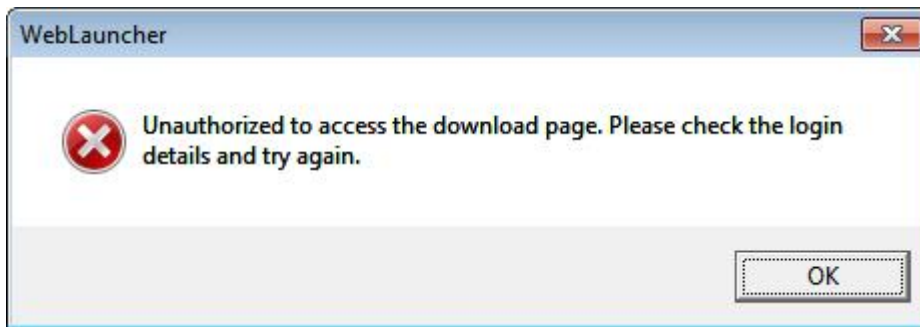
1. Check if they are using the Certificate that was paired with their Exigo password
2. Check that their Certificate has not expired.
3. Check that the Certificate is not corrupted. If the Certificate is corrupted, a valid Certificate must be re-installed.
4. Check if your certificate has a private key. To check, try to export your certificate, the option "yes, export the private key" should not be greyed out.

Related Technical Document: https://www.asxonline.com/intradoc-cgi/groups/participant_services/documents/participantapplicationkitsfe/asx_038038.pdf

Escalation:

If your certificate has expired or does not have the private key (and no back up) you will need to request a new one by contacting the Austraclear Helpdesk.

Unauthorized to access the download page. Please check the login details and try again. Failed to get executable



Error above followed by 'Failed to get executable'

Application:
Weblauncher

Connectivity Type:
ANNI or Internet PC

Deployment Type:
Web browser

Cause:

Incorrect username, password or digital certificate. Or the EXIGO user account has been locked out.

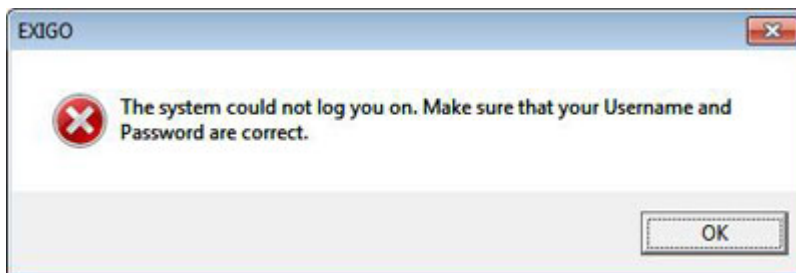
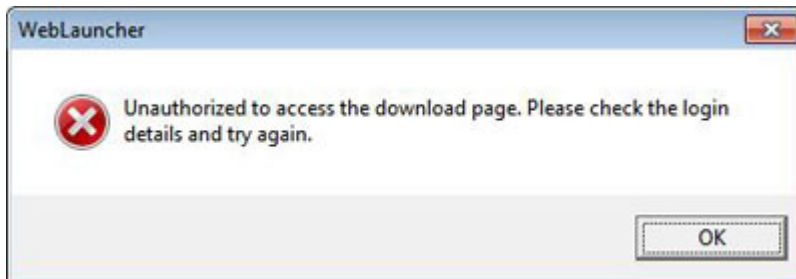
Incident Response:

1. Check if the user entered the correct username and/or password and/or using a valid certificate during login to EXIGO GUI.

Escalation:

Escalate to Austraclear Help Desk to check if the EXIGO user account is locked.

Unauthorized to access the download page OR The system could not log you on



Application:

Exigo GUI and Weblauncher

Connectivity Type:

ANNI or Internet PC

Deployment Type:

Web browser or File deployment

Cause:

User entered a wrong user name or password.

Incident Response:

Close EXIGO and launch it again. User must enter the correct credentials and the correct password.

Verisign can't issue a certificate

During Certificate Renewal, the user got this error message from Verisign.

'Online Enrollment Status - Thank you for requesting a Digital ID. Unfortunately, we cannot issue a certificate because an error occurred while processing your request. Please try again. If you continue to get this error, please contact your administrator.'

Connectivity Type:

ANNI or Internet PC

Incident Response:

1. <https://pki.verisign.com.au> is added as a Trusted Site (TOOLS > INTERNET OPTIONS > SECURITY > TRUSTED SITES > SITES)

2. The default Security Level of your Internet settings to "LOW" (TOOLS > INTERNET OPTIONS > SECURITY > DEFAULT LEVEL > LOW)

3. Your ActiveX settings are enabled (this should happen automatically if your security settings are set to "LOW")

You can check this at the following screen TOOLS > INTERNET OPTIONS > SECURITY > CUSTOM LEVEL - Check "ActiveX" are set to "Enabled"

Once this is done, please try to renew.

If this doesn't work, please try to export your digital certificate (in PFX format) to a network drive as per section 5.4 of our technical documents:

https://www.asxonline.com/intradoc-cgi/idcplg?IdcService=ASX_COLLECTION_DISPLAY&hasCollectionID=true&dCollectionID=887&SortField=dInDate&SortOrder=Desc

Then try to renew on another PC running Windows XP.

When I click the link, Nothing happens

Application:

Weblauncher

Connectivity Type:

ANNI or Internet PC

Deployment Type:

Web Browser

Cause:

The user 'saved' the file instead of 'Opening' it after clicking the Austraclear Client Link.

Some Participant's PC policy enforce to confirm the download of a certain file types.

When a user sees this, sometime they click 'SAVE' instead of 'Open'. If this is the case, the weblauncher will not launch the application

Incident Response:

2. User to click the Austraclear client link again
3. If prompted (see screen below), click OPEN



If the prompt does not have the option OPEN, please contact your IT support to enforce the OPEN option for the File Types.