ASX Austraclear Release 3

TECHNICAL FAQ's

August 2011

Information provided is for educational purposes and does not constitute financial product advice. You should obtain independent advice from an Australian financial services licensee before making any financial decisions. Although ASX Limited ABN 98 008 624 691 and its related bodies corporate ("ASX") has made every effort to ensure the accuracy of the information as at the date of publication, ASX does not give any warranty or representation as to the accuracy, reliability or completeness of the information. To the extent permitted by law, ASX and its employees, officers and contractors shall not be liable for any loss or damage arising in any way (including by way of negligence) from or in connection with any information provided or omitted or from any one acting or refraining to act in reliance on this information. This document is not a substitute for the Operating Rules of the relevant ASX entity and in the case of any inconsistency, the Operating Rules prevail.

ASX Limited
ABN 98 008 624 691

20 Bridge Street, Sydney NSW 2000
PO Box H224
Australia Square NSW 1215

Telephone: +61 2 9227 0000
Facsimile: +61 2 9227 0859
Email: info@asx.com.au

Updated: August 2011
Version: 1.0

CONTENTS

Frequently Asked Questions

PC Infrastructure

What is the recommended PC hardware specification for the ASX Austraclear system?

The recommended specification is an Intel Core 2 3.16 GHz PC with 4GB RAM.

Where can we download the .Net Framework version Redistributable package from?

The .Net Framework can be obtained as a free download from the Microsoft web site. Going forward, Microsoft will include the .Net framework in service packs and new versions of Windows.

http://www.microsoft.com/downloads/en/resultsForProduct.aspx?displaylang=en&ProductID=de7bb609-3fd0-4b0f-865d-5ed2463ad5d0&nr=10&sortCriteria=Popularity&sortOrder=Ascending&stype=ss_sd

Is the ASX Austraclear Release 3 system is now a browser based software?

No. The ASX Austraclear Reelase 3 system is still a .Net Windows Form application which can either be launched by your web browser or installed as an application via File Deployment and launched from the Start menu.

What Operating System versions and related service packs will be required to enable us to deploy the ASX Austraclear Release 3 client prior to the IWT or live implementation date?

A published technical requirements can be retrieved from the link below:

https://www.asxonline.com/austraclear_system_release_3/index.htm

Please note that Release 2 and Release 3 minimum Technical Requirements are not the same.

What is the minimum MDAC version requirement on the client PC to support .Net framework and the ASX Austraclear Release 3 software?

MDAC is not required for the ASX Austraclear system.

Does the installation of .Net Framework affect the Active Directory?

No, the installation of the .Net Framework does not impact the Active Directory.

If we will be using the Internet to access the ASX Austraclear Release 3 system, is any sort of VPN client required to be installed on the clients to provide this access?

There is no VPN software required to access EXIGO. The client uses SSL encryption to connect to the servers.

Can the ASX Austraclear Release 3 system software be deployed and run in a CITRIX server / Windows Terminal server environment?

The deployment and execution of the new system software on a Citrix or Windows Terminal Server environment will have to be confirmed by Participants on an individual basis. This is the case as each Citrix-type configuration is likely to be unique to each individual Participant, and we are therefore not able to provide a generic confirmation regarding it's suitability for the ASX Austraclear system.

However, some Participant running a Citrix environment have been successfully deployed our Release 2 system since go-live.

If we will be running RITS / ACNZ on the same PC as the ASX Austraclear Release 3 system, how will the required Kea software be installed?

The Kea software and installation instructions will be provided by the ASX. Please contact the ASX Austraclear helpdesk to arrange installation.

Is Windows XP Service Pack 3 supported?

Yes. The ASX Austraclear Release 3 system will run on Windows XP SP 3

Why is the MSI Security Policy required?

The MSI Security Policy is required for the web-launcher process. It configures the trust relationship between the middle tier and the client PC.

What specific changes does the security policy make to the client's PC operating system and/or .Net Framework

It adds the OM Web launcher key to the .Net security configuration which allows the browser to use .Net to download the ASX Austraclear application.

How often will this file need to be changed (as Admin rights are require to install it) ?

This unique key does not change between versions of the web launcher.

Network (including Proxy Servers)

What specific configuration changes are required to our firewalls and proxy servers?

The required changes are described in detail in the Participant Technical Briefing Papers and the appropriate ASX Austraclear Release 3 Domain Names papers, for both ANNI and Internet users, which are available on the ASX Austraclear web site.

https://www.asxonline.com/austraclear_system_release_3/index.htm

If we do not have either a router or firewall configured, can you confirm that we therefore do not need to make any port configuration changes?

If the Participant does not use a router or firewall, no port configuration changes are required.

If TCP Port 900 is opened, what traffic will be going over TCP Port 900 eg http or https?

HTTP. TCP Port 900 is not used by the ASX Austraclear system

If our client PC's use private internal addresses and access the Internet via either a web proxy or NAT firewall, does access to the ANNI network work via Network Address Translation?

Yes it does.

If we utilise 'destination NAT'ing' does the ASX need to know our original source IP address?

Yes. This information is required to enable the ASX to configure our routers with the appropriate Network Address Translation information.

Is the DNS access for a publicly accessible DNS zone, or is it only accessible by authenticated clients? i.e. Can DNS be resolved via our internal forwarders?

Yes, DNS can be resolved by your internal forwarders.

(Internet Access) Will the DNS entries be added to the public Internet DNS system?

Yes. The details have been published. Note that the Internet DNS cannot be used by ANNI users. ANNI users must resolve from the ANNI DNS.

How do we configure TCP with the ASX DNS IP address?

Either the Participant workstations or the Participant DNS server should be configured to point at the ASX DNS servers. On workstations this is done through control panel/network settings.

With regards to DNS, does the application require TCP and UDP port 53 open from the client to the specified Internet addresses?

Yes. DNS uses port 53 for both UDP and TCP traffic. It uses TCP mainly for zone transfers, but can fall back from UDP to TCP for regular DNS queries if UDP responses are truncated. In addition some debugging tools use TCP by default for talking to servers. While DNS clients and servers use mainly UDP for query / response traffic, the ASX requests that TCP / UDP port 53 is allowed through Participant firewalls.

How will we connect to RITS/ACNZ going forward? Will the existing Keaterm sessions still be required for RITS/ACNZ?

Yes, the existing Kea session will still be required to access RITS/ACNZ and the method of connecting to these systems will remain the same.

If we are running a stand-alone PC for the ASX Austraclear system who is responsible for connection of the PC to the router?

The Participants are responsible for setting up their own internal network infrastructure. ASX can provide technical assistance if required

Why does port 53 need to be open, and what sort of traffic is going via port 53?

Port 53 is used by DNS (Domain Name Server). The Participant's local DNS server will need to communicate with the ASX DNS servers. This is required to facilitate fail over from primary ASX production site to the ASX Backup site.

Deployment (File and Browser)

Do we need to upgrade to the ASX Austraclear Release 3 system, or can we simply continue using the existing Austraclear Release 2 system?

In order to continue using ASX Austraclear after the live implementation date, you will need to have upgraded to the ASX Austraclear Release 3 system. The existing Austraclear Release 2 system will be decommissioned once the replacement Austraclear Release 3 system has been implemented.

How do you install and configure the software onto the PC?

Release 3 deployment methods are still the same. There are two methods available for deployment. The first method is the Browser model which uses .Net zero deployment.   You access the ASX Austraclear homepage and click on the appropriate link initiating the web launcher, which manages the software download and execution.

The alternative method is the File deployment model in which an installation file can be downloaded from ASX website. You are then able install the system by executing the file. Using this method would allow you to package the system for rollout to multiple PC's. Detailed information regarding each method is available on the ASX Austraclear website.

Is the software that is downloaded for the ASX Austraclear system specific to the current user or the local machine?

Using the Browser Deployment model the downloaded files are stored in the user's profile directory in the local machine. Thus, the user can transfer to a different PC anytime, as long as the PC requirements are met by the local machine i.e. .Net framework, Security Policy and other requirements as explained in the Technical Briefing Papers (This is true if roaming profiles are used).

Using the File deployment model the initial installation file (compressed file) needs to be saved into a local directory. However, once executed, the application will be saved in the local machine's "Program Files" directory.

How is the ASX Austraclear software actually launched?

Under the Browser deployment model the system is installed as a .Net Windows Forms application via a .Net feature known as ".Net zero deployment". This model enables users to launch and access the system via the browser, i.e. Internet Explorer 7.

Under the File Deployment model, the software is launched from the Start menu or by using a desktop shortcut.

What is the 'Web Launcher' and what does it do?

The web launcher is only used in the Browser Deployment model and is responsible for performing the deployment and providing feedback to the user in terms of a progress bar and details of each activity it performs. If an application download is required it will also indicated the size of that download. Once the application is downloaded to the client PC the web launcher will launch the application. A splash page will be displayed followed by the login prompt.

Is there a new version of Weblauncher for Release 3?

Yes, there will be a new version of Weblauncher for Release 3.

How do I authenticate to the application

If you are an Internet user, the application will prompt you to enter your SecurID details when you enter your user name and password. You must also have a valid digital certificate installed on your PC

Can we package still the ASX Austraclear Release 3 system software as part of our standard method of rolling out the SOE to PC's?

Using the File deployment model it would be possible to package the software and do a rollout to multiple PC's. However, the Participant then assumes responsibility for ensuring that their users have the most recent version of the software available.

Does the installation of the trust file (security policy) need to be repeated with each new release of software?

No, the installation of the trust file is a one-off, which is performed the first time a user logs into the new system. This step would only need to be repeated if a user needs to access the system from a new or different PC.

What is the difference between File and Browser deployment model?

The File deployment method does not maintain automatic version control, and the software will need to be manually updated when there is a new release. The software is password protected and available on the ASX Austraclear homepage for downloading. The file deployment version of the software can be packaged and rolled out to the users. This method of deployment does not require the web launcher trust relationship .msi to be installed.

Browser deployment method requires Internet Explorer 6 and the web launcher trust relationship .msi to be installed. The browser deployment method checks the version of the software each time the user logs in, and allows the user to update the software if necessary.

Is the web launcher Trust Relationship (Security Policy) .msi file needed for File Deployment?

No, the web launcher Trust Relationship (Security Policy) .msi file is only needed for Browser deployment and is not required for File Deployment.

Security (including Digital Certificates)

What is a Client side digital certificate?

A Digital Certificate is the electronic version of an ID card that establishes your credentials and authenticates your connection when performing transactions.. Please refer to:

http://www.microsoft.com/windows/ie/using/howto/digitalcert/using.asp

What does a client side digital certificate mean for me?

Client side certificates have been introduced into the environment to provide two factor authentication. In simple terms, this means that it is possible to cryptographically tie a transaction to a particular username and certificate. The two factor authentication component simply means that the user must both have and know something, just like a PIN number on an ATM card.

Where is the certificate stored? (i.e. on the c: drive, on the LAN etc)

The certificates are stored in the individual browser certificate store on a per user basis. For example, if a certificate is saved in one user's profile it will not be available in another user's profile. However as the certificates are exportable, they could also be saved on the Participant's LAN.

Will the certificates be exportable or transferable?

Yes, the digital certificates can be configured in exportable mode.

Will the digital certificates for IT support staff any different from those used by the general users?

No, the same format digital certificates will be issued to all users of the ASX Austraclear system.

How are digital certificates configured for use at our BCP/DR site? i.e. can they be exported, or do new certificates need to be downloaded?

The digital certificates are configured in an exportable format, meaning that they can be copied from one PC to another, or other appropriate electronic media, e.g. USB smart card. Further end-user documentation will be provided as part of the scheduled training.

Can I use my current user id and Digital certificate to logon to Austraclear Release 3 ?

Yes you can for both Production and Test Bed environment..

Does the RSA SecurID system require any special firewall rules or does it run over the HTTPS stream?

No special firewall riles are required

Can I use my existing RSA token to login to Austraclear Release 3 environment?

Yes you can, for both Production and Test Environment.

Is there any associated software that requires installing on a user's PC to facilitate the Checkpoint client authentication?

No software is required.

How is the .Net security policy configured as part of the installation procedures?

The .Net framework requires a Security Policy to be applied before application deployments can take place. The update must be done by an administrator, preferably at the same time the framework is installed. The policy is available via the initial ASX Austraclear home page.

Is the location of the digital certificate configurable by the Participants?

The certificate storage location is completely configurable by Participants. The certificate can be exported to other appropriate forms of media, including USB drives, IKEYS etc.

Are digital certificates stored as part of the roaming user profile?

Yes, the certificates can be stored as part of the user's roaming profile. However, they can also be stored on any other media preferred by the Participants.

Are the certificates linked to a specific user?

Yes, the certificates are linked to a specific ASX Austraclear (EXIGO) username. Participants are not allowed to share usernames/password pairs across the system.

How are users uniquely identified prior to being issued with a certificate?

Users are identified by First name, Surname, E-mail address, EXIGO Username, Passcode and Participant Id prior to being issued with a digital certificate.

How is a certificate cancelled if a user leaves?

If a user leaves an organisation the ASX Austraclear helpdesk should be contacted to revoke the individual's certificate and lock the corresponding user account.

Can the certificate be transferred to the replacement user?

No, certificates cannot be transferred between users. If a user leaves the certificate will need to be revoked. A new certificate will then be issued to the replacement staff member.

Can the certificate be configured by the Participant i.e. be password protected?

Password protection and storage options are configurable by the Participant.

What options do we have for transferring certificates to our BCP / DR site (other than copying to a floppy disc)?

This is completely up to the Participant. For example, certificates can be copied across as part of a Windows Domain profile or on a USB drive or IKEY device.

Can a user's certificate be used on multiple PC's, and how would this work in practice?

A user's certificate can reside on multiple PCs (for BCP/DR requirements) by exporting it from the original PC. However, it is an ASX policy that username/password pairs are not shared amongst users.

Can different certificates be used on the same PC?

Yes, multiple certificates can be used on the same PC. When accessing the ASX Austraclear replacement system the user will be prompted by the EXIGO client to select the appropriate certificate.

I am getting an error when selecting "Enroll" on the ASX Austraclear Digital ID Centre page?

This error is most likely to be related to the Internet Explorer permissions when accessing the VeriSign web site. Please add the VeriSign web site to the "Trusted Sites" zone and repeat the operation. If you are still getting an error, logging on as a user with local Administrator rights may be necessary, and can be arranged with your local IT Help Desk.

What is the "Challenge Phrase" when enrolling for a Digital Certificate?

The Challenge Phrase is a unique phrase set by the user and not shared with anyone. This phrase can be used by a user to revoke the certificate if required. This phrase is private to the user and it cannot be changed by the user. It's format is alphanumeric, no punctuation and a maximum length of 32 characters.

Business Continuity Processing / Disaster Recovery (BCP / DR)

What is a RSA SecurID card and how do I obtain one?

A RSA SecurID token (ACE card) is required to authenticate to the ASX Austraclear firewall when accessing the system via the Internet. If an additional SecurID token is required for your BCP /DR site, the appropriate application form is available on the ASX Austraclear homepage:

https://www.asxonline.com/intradoc-cgi/groups/public/documents/participantapplicationkitsfe/asx_022928.pdfPlease print and complete this form, ensuring that it is signed by two authorised signatories, and then return the completed form to ASX Austraclear via fax on 02 9256 0116.

NETWORK Troubleshooting:

1) Routing
ANNI users should firstly check that they can telnet the address 203.4.179.224 on 443 using a DOS prompt.
Eg. telnet 203.4.179.224 443
You should get a blank screen to confirm this is working. If this works, then Go to Step 2.
If this is not possible, then try to ping this address from your last hop before the ASX controlled ANNI router. This will confirm if firewall and routes are in place for Release 3.
If this is not possible, then check that the network routes that have been setup for the ANNI network, do no conflict with other ASX products. As ASX Austraclear IP addresses are within the same class C range of addressing as other products used in the ASX distribution network (such as ASX Trade), it is NOT recommended that a subnet of /24 is used for the routing rules. More specific routing rules should be setup to allow for the addresses used in Release 3:
asx.austraclear.com.au   203.4.179.224   https
asxhelp.austraclear.com.au   203.4.179.228   https
asxta.austraclear.com.au   203.4.179.230   https
asxhelpta.austraclear.com.au   203.4.179.229   https
E2 DNS   203.4.179.50   dns

If you are still unable to ping 203.4.179.224 from your last hop on the ANNI network, then please capture a trace of the ping attempt with a timestamp and send this to ASX support.
Also, if you are unable to perform nslookup against 203.4.179.50 from your network, then please capture a trace of the nslookup attempt with a timestamp and send this to ASX support.

2) DNS
Currently for Release 2, ANNI users can use either the Internet DNS (203.18.165.215 and 59.154.35.23) or local hosts file to resolve exigo.austraclear.com.au.
For Release 3, ANNI users must NOT use the Internet DNS. They must now use the ANNI DNS 203.4.179.50. The Internet DNS will return an address for asx.austraclear.com.au of 203.15.145.75 for ANNI users, which will send them to the Internet instead of the ANNI network for the GUI. These users who are sent to the Internet will receive a technical error prompt saying their RSA passcode is incorrect (ANNI users do not require RSA passcodes). ANNI users who use the ANNI DNS will receive the correct address for asx.austraclear.com.au of 203.4.179.224.

** PLEASE NOTE that for Release 2, the ANNI DNS will return an address for exigo.austraclear.com.au of 203.18.165.249 **

Some ANNI participants have previously used the address for exigo.austraclear.com.au of 203.18.165.220 for Release 2. This would have occurred if the ANNI user was using the Internet DNS for name resolution. While this would have worked for them for Release 2, it is not the recommended address, and they should aim to use the 203.18.165.249 address for Release 2.

** Internal IT must check that the users have access to https://exigo.austraclear.com.au using 203.18.165.249 prior to cutting over their DNS forwarding from Internet DNS to the ANNI DNS. If this is not checked, then their access to Release 2 Production will be disrupted. **

If you are able to ping asx.austraclear.com.au and get a return address of 203.4.179.224, then you may now proceed to configure the PC for the Release 3 software.
If this is unsuccessful, then please review the above steps again, checking that UDP 53 is available on the network to 203.4.179.50.

Digital Certificate Troubleshooting

Things worth checking (in order) for the user if they get an unauthorised login into Exigo GUI R3:

1) Check their PC has the "VeriSign Class 3 Public Primary Certification Authority - G5" root certificate installed. This can be downloaded from http://www.verisign.com/support/roots.html
   When they install the cert, get them to install into the Root Certificate folder, and not choose Automatic.
2) Check their PC has the "SFE CA" root certificate installed. This can be downloaded from https://pki.verisign.com.au/services/SFECorporationLtdAustraclear/digitalidCenter.htm
   Again, when they install the cert, get them to install into the Root Certificate folder, and not choose Automatic.
3) When they export the Verisign Client Digital Cert from their old PC to the new one, check that they are NOT ticking "enable strong protection" during the export process. This is ticked by default, which means many companies will have them stored for safe-keeping in the *wrong* state. They must untick it before exporting.
4) When they import the Verisign Client Digital Cert into the new PC, get them to install into the Personal folder, and not choose Automatic.
5) Check that their user is not in a locked state in ASX Austraclear. If so, unlock them.
6) If they still fail, then reset their password in ASX Austraclear.
7) If they still fail, then ASX will have to reset their password in Active Directory.