RESERVE BANK OF AUSTRALIA

RITS User Interface Technical Information Paper

24 June 2023
Version 3.6

Revision History

Version	Date Completed	Comments
1.0	November 2004	Distributed to Members of RITS Technical Working Group (TWG) for review.
1.1	January 2005	Incorporating questions from TWG and more information about tokens and certificates.
1.2	June 2005	Contains details of hosts, names, addresses, URLs and some updated information
1.3	February 2006	Some updates, in particular an Appendix about ActiveX controls.
1.4	April 2006	Updated to describe use of the new RITS Launch Page.
1.5	May 2006	Update Section 6.1.1 on Trusted Zones, update Section 7.4 on Proxy Options, new Section 7.8 on MTU Parameter, and update Network Addresses in Appendix 1.
1.6	June 2006	Add notes on Fast User Switching and Software Installation requires Admin privilege.
1.7	October 2006	Internet Explorer v7 incompatibility, Proxy settings, Adobe and PDF information, other technical clarifications.
1.8	April 2007	Internet Explorer v7 Compatibility, Alternate JRE Version Support, removed Redundant Auth IP Addresses, Access options-removed reference to Old Forms Interface, Updated Contact Details.
1.9	October 2007	Update for Phase 3 Client Side Requirements, RITS Compatibility with JRE 1.5 and 1.6.
2.0	June 2008	Update for Vista Requirements.
2.1	November 2008	Removed reference to Austraclear Certificates.
2.2	January 2009	Java JRE 1.6.0_10 Plug-in Compatibility Issues, Disabling Java Auto-Updates.
2.3	September 2009	Update to include additional RBA Addresses.
2.4	August 2011	Updated for new SafeNet Token Driver Software and client Side Installer (SAC 8.0 SP2). Support for Windows 2000 stopped. Support for IE8, IE9, Windows 7 added.
2.5	December 2012	Updated for new Certificate Authority. Replace broken links.
2.6	February 2014	Support for Windows XP and IE versions 6 and 7 stopped.
2.7	April 2014	Support added for Windows 8.1 and newer versions of Internet Explorer (IE). PCs with Windows 7 can now use IE version 11 in addition to the already supported IE versions 8 and 9. PCs with Windows 8.1 can use IE version 11. Compatibility with Java version 1.7.0_51 also added.
2.8	March 2018	Support added for Windows 10 IE version 11.
2.9	May 2019	Removed superseded information on Java, updated information on tokens
3.0	August 2019	Removed support for TLS protocol versions 1.0 and 1.1. Section 6.2.1 added on how to enable TLS 1.2 in browser settings. Updated information in section 5.3.2 on Java support.

Version	Date Completed	Comments
3.1	February 2020	Removed support for Windows 7 (from 14 January 2020) and updated minimum requirements for access.
3.2	March 2020	Minor formatting change.
3.3	February 2021	Updated for new RITS certificate collection URL.
3.4	August 2021	Removal of support for Windows 8.1 (from 1 October 2021) Retirement of IE11 and introduction of requirement for Edge in IE mode
3.5	January 2023	Decommission of Applets and ActiveX controls and removal of support for Edge in IE mode in Pre-Production Environment Introduction of requirement for Google Chrome or Microsoft Edge browser extensions in Pre-Production Environment
3.6	June 2023	Extension of January Pre-Production changes to the Production Environment Add support for Windows 11 and RITS Client Software 10.5

RBA Reference Number: D22/284695

Contents

1. Introduction

1.1 Background

This paper provides detailed information about the technical requirements for Members accessing the Reserve Bank Information and Transfer System (RITS).

Members should advise the Reserve Bank immediately if they see that any of these requirements will conflict with their own environments, policies or procedures. Contact details are provided in Section 11.

1.2 Intended Audience and Purpose

This paper is for staff of RITS Members who are responsible for establishing and maintaining the technical environment for RITS users.

1.3 What is the RITS User Interface?

The RITS User Interface is the browser-based user interface for online (terminal) access to RITS.

1.4 Basis of Information

These requirements are based on information available as at 10 June 2023.

2. Access Arrangements

2.1 Access Options

The Reserve Bank and ASX Limited have agreed that online access to RITS may be provided using the Austraclear National Network Infrastructure ASX Net network, providing operational convenience for RITS Members requiring access to both RITS and the Austraclear System.

RITS can also be accessed via the Internet. Use of the Internet involves strict security controls, and is subject to certain restrictions, particularly in relation to the types of institutions that may use it as their only means of connection to RITS. Further information about these restrictions is outlined in the Requirements for Access to the RITS User Interface, which is available on the RITS Information Facility, under the 'Connectivity Requirements' tab.

2.2 Accessing RITS

A RITS Launch Page is provided for users and can be accessed via the Desktop or the Windows Start Menu. The Launch Page is an HTML page containing JavaScript. When the user attempts to connect to RITS via the Launch Page, the JavaScript automatically detects which site RITS is operating from and opens a new browser window that connects to that site. For those Members with ASX Net access, the Launch Page selects the ASX Net path by default. If ASX Net access is not available, the internet access option is chosen.

Members accessing RITS **via the internet** are using a web address that resolves to a public Internet IP using DNS.

Members accessing RITS via **ASX Net** are using a web address that corresponds to one of the following:

- a name that is resolved to the IP address of the RITS server by the Member's internal DNS (or use of the ASX Net DNS service if appropriate) or alternative name resolution mechanism or
- a name that is resolved to a private IP address by the Member's internal DNS or alternative name resolution mechanism, and subsequently converted to the target server address by network address translation (NAT).

It should be noted that RITS uses SSL to provide privacy and ensure the integrity of the connection. The direct use of IP addresses corresponding to the web addresses referred to above will work, but results in browser-generated messages such as 'The name of the security certificate is invalid or does not match the name of the site'. This approach is not recommended.

2.3 Accessible Environments

The following three RITS environments are accessible from Member sites:

- RITS Production via Reserve Bank Primary Site
- RITS Production via Reserve Bank Alternate Site
- RITS Pre-Production

Refer to Appendix 1 for details on how to set up access to each of the environments.

3. Security Arrangements

3.1 Tokens and Digital Certificates

RITS online access is based on the use of X.509 digital certificates that uniquely identify individual users. Properly authorised users are able to download a certificate following receipt of 'security codes' from the RITS Help Desk. Each RITS user is issued a personal SafeNet eToken 5110 hardware token (see image below) to safely store the digital certificate. These certificates are used for user authentication (in addition to login and password) and for digital 'signing' of user actions for 'value' transactions such as cash transfers and changes to sub- limits and queued payment statuses.

A detailed description of the SafeNet eToken 5110 is available at https://cpl.thalesgroup.com/access-management/authenticators/pki-usb-authentication/etoken-5110-usb-token.

SafeNet eToken 5110

Users are required to insert the token into a USB port of their PCs to access RITS and perform transactions.

Users will need to have write access to their USB port to be able to collect certificates.

3.2 Operational Arrangements – Tokens and Digital Certificates

This section summarises some of the operational arrangements relating to tokens and digital certificates. Information on policy and procedures is provided in the RITS Access and Security User Guide, which is available on the RITS Information Facility at:

www.rba.gov.au/rits/info/pdf/RITS_Access_and_Security_User_Guide.pdf

3.2.1 Internet Access Required

All Members are required to have public internet access to the RITS Certificate Authority (CA) for registration and collection of digital certificates. The RITS CA is only available from the public internet; details can be found in Appendix 1.

3.2.2 Email Address for Each RITS User

The Reserve Bank very strongly recommends that each RITS user has their own email address to receive security information as part of the certificate enrolment procedure. These procedures are designed to ensure that only the authorised user may enrol for the certificate issued in their name. The use of shared email addresses by a Member may weaken the very high security built into RITS certificate issuance procedures, by exposing them to a greater risk of internal misconduct, with resulting unauthorised issuance and use of certificates. It also means that a user may not receive certificate expiry reminder emails.

Where a Member's internal policies or environment does not allow each RITS user to have an individual email address, the Reserve Bank requires a written acknowledgement from that Member (signed by RITS authorised signatories), that they do not provide all users with individual email addresses, and instead rely on other internal security controls.

These might, for example, involve the following:

- that the Password Administrators have their own individual email addresses to receive notice of revocation emails, and expiry emails
- that Password Administrators should not have access to the shared email address used by RITS users

to format their own tokens and to set their Token Codeword. These details should only be known to the user themselves.

- each RITS user enrols (i.e. receives certificate) via the internet. This should not be done by any other person.

Email addresses are subject to certain restrictions that are common in business applications. In particular, apostrophes and single quotation marks are not accepted as valid characters in email addresses.

3.2.3 Multiple Logins

A user is permitted to have multiple RITS User IDs if each is with a different Member. For these users, the RITS Login Page presents a list of valid RITS certificates from which the appropriate selection can be made.

3.2.4 Lost Tokens

If a user has lost their token, they must arrange for their Password Administrator or the RITS Help Desk to revoke the certificate. The user must then enrol for a new certificate. Members maintain a small store of spare blank tokens for this purpose. If the user, a Password Administrator and RITS authorised signatories are available, this process can normally be completed within 30 minutes.

3.2.5 Contingency Arrangements

Members are advised to keep a store of blank tokens at their Disaster Recovery/Business Continuity site(s). If users have to work from their backup site and do not have their current token with them, they need to follow the procedures for a lost token (i.e. have the existing certificate revoked by a Password Administrator or the RITS Help Desk and enrol for a new certificate).

3.2.6 Certificate Expiration

In most circumstances, RITS certificates expire after two years. Users will be advised well in advance that they need to obtain a new certificate (via the standard issuance process).

3.3 Internet Access Authentication

An additional authentication step is required for those Members accessing RITS from the internet. This authentication is performed at the Reserve Bank's external firewall, and uses the same token and Reserve Bank issued RITS certificate. The user is required to select a valid RITS certificate in order to gain access to the RITS Login Page.

4. Hardware Requirements

4.1 USB Port

User PCs must have a USB port available for the security token. The token must be in place for RITS logon and when any value transaction or command action (e.g. changing an ESA sub-limit) is performed. The token is also required for administrative actions such as user updates. Enquiry-only functions will not access the token.

Users will need to have write access to their USB port to be able to collect certificates.

4.2 PC Specifications

Minimum PC specifications for RITS users include:

- Memory requirements: 1GB
- Screen resolution: 1024 × 768 pixels

5. Software Requirements

5.1 Operating System

Access to RITS is supported on Microsoft Windows 10 (64 bit) and Windows 11.

5.2 Browser

Access to RITS is supported via Microsoft Edge (v107 or later) or Google Chrome (v107 or later).

5.3 RITS Software Packages

5.3.1 Install the RITS Software Package

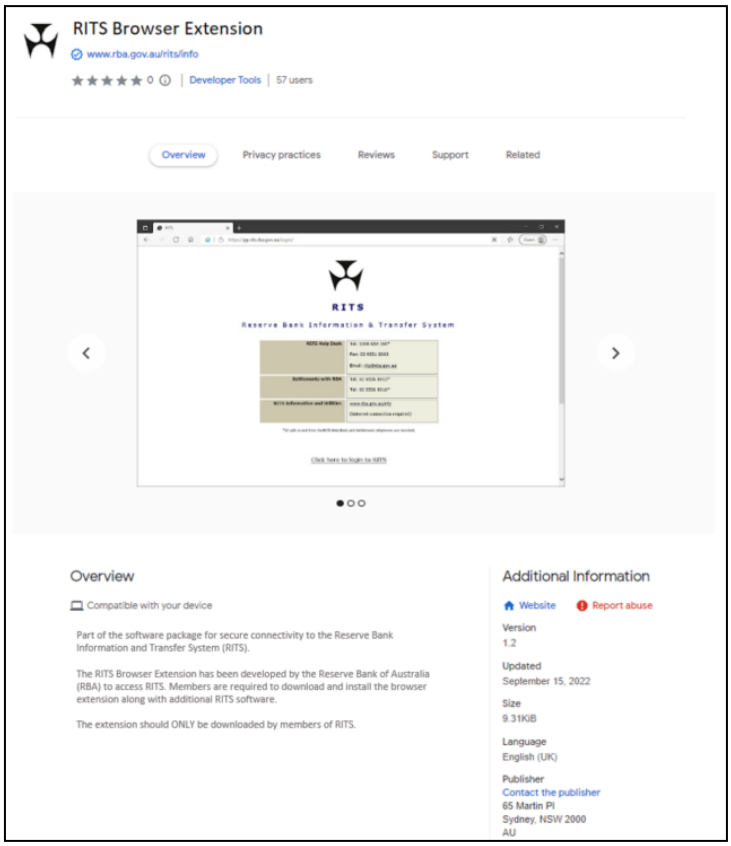
The RITS software package can be downloaded from the RITS website at www.rba.gov.au/rits/software/.

Download and install each of the following on each user's PC: RITS Browser Extension, RITS Sign Host, RITS Client Software, and RITS Launch Page. Detailed instructions on each is provided below.

5.3.2 Install RITS Browser Extension

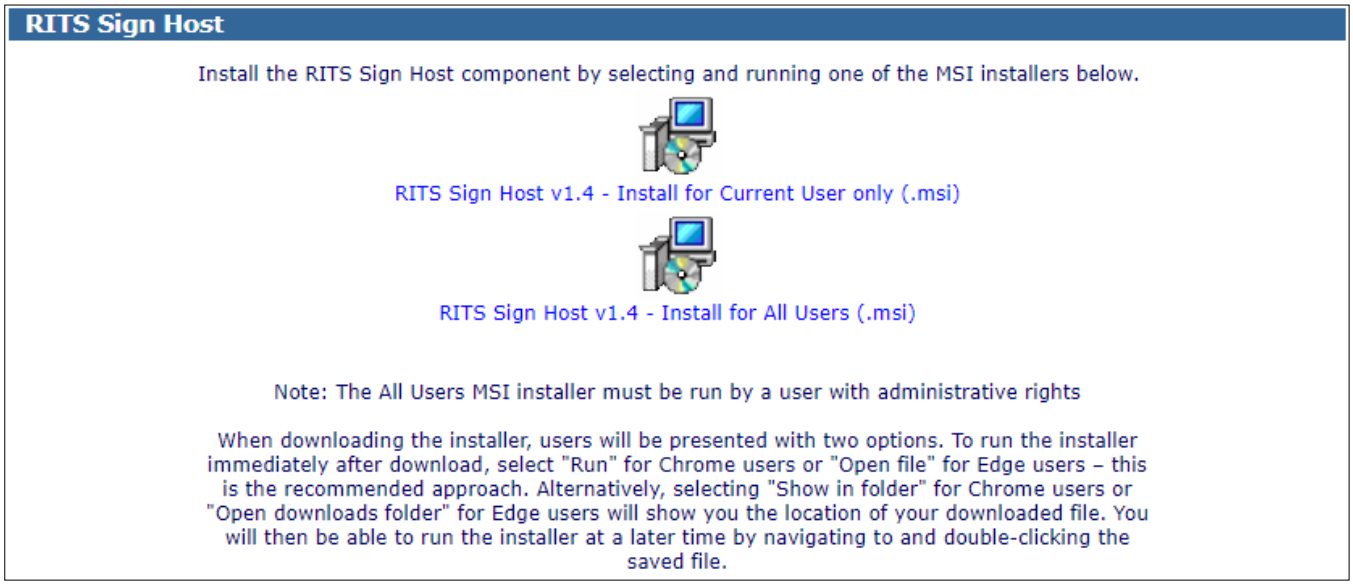
The RITS Browser Extension can be downloaded either from the Chrome Web Store or the RBA website using the links on www.rba.gov.au/rits/software/. If downloaded from the RBA website, it will need to be saved as a file on the local file system first and then installed manually.

The following screenshot shows installing via the Chrome Web Store.

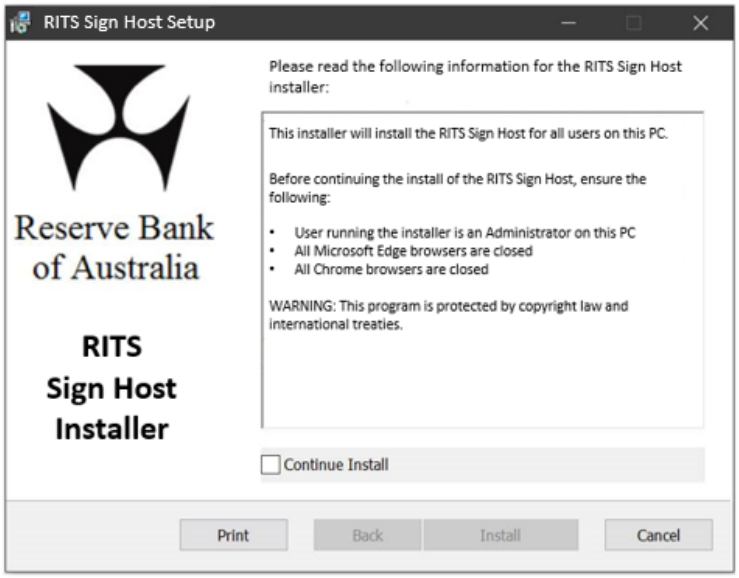


5.3.3 Install the RITS Sign Host

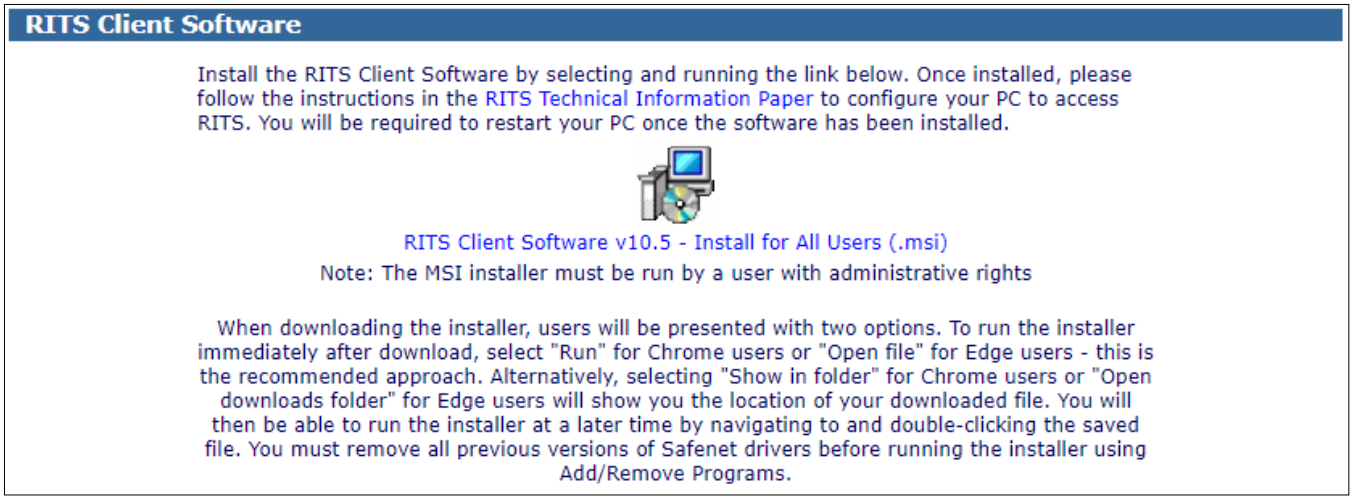
The RITS Sign Host is a native application component that can be downloaded from the RITS website at www.rba.gov.au/rits/software/ and installed on a PC either for the current user only (which does not require administrator permissions) or for all users using that PC (which requires administrator permissions to run the installer).



Choose the appropriate MSI installer and follow the prompts. The following screen is displayed for the "all users" installer. A similar screen is displayed for the "current user" installer.

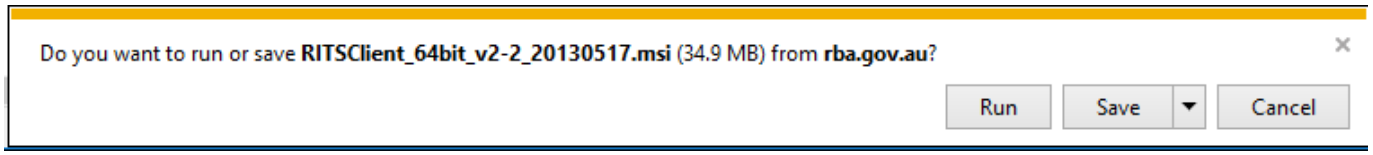


5.3.4 Install the RITS Client Software



The RITS Client Software is a Windows application that installs hardware security token drivers. It can be downloaded and installed from the RITS website at www.rba.gov.au/rits/software[1].

The following dialogue box may be displayed.

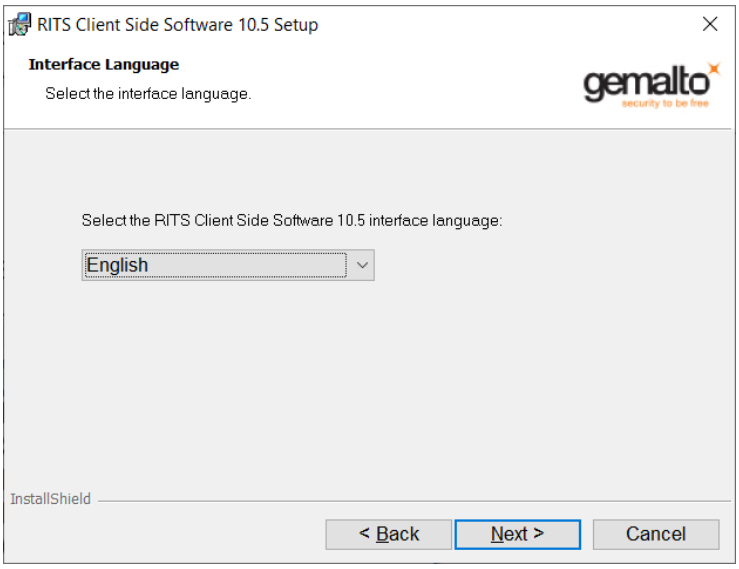


Select **Run** to continue until the following dialogue box is displayed. (If a message is displayed warning that the publisher of the file cannot be verified, again select **Run** to continue.)

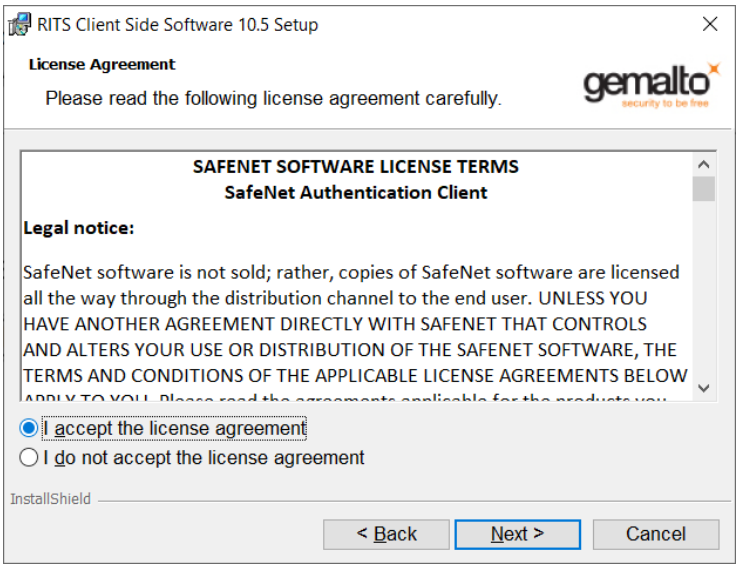
Select **Next**.

[1] These instructions relate to RITS Client Software version 10.5. If you have a business need to use RITS Client Software version 8.2, please contact the RITS Help Desk.

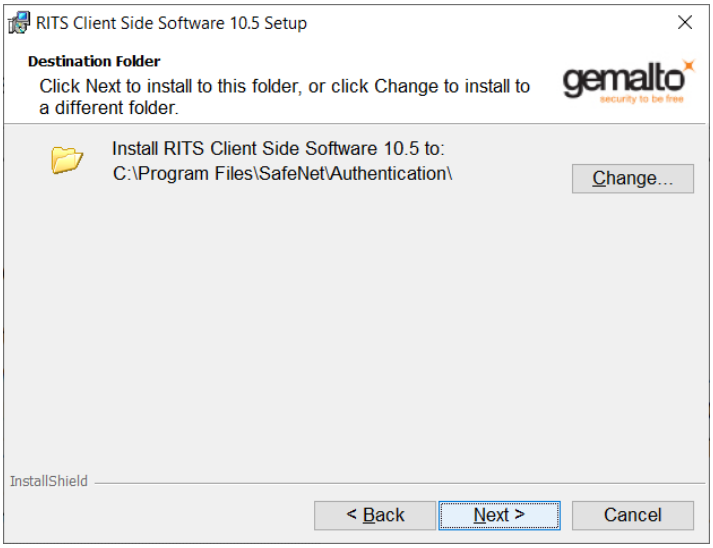
The following screen will be displayed. Select **English** then **Next**.



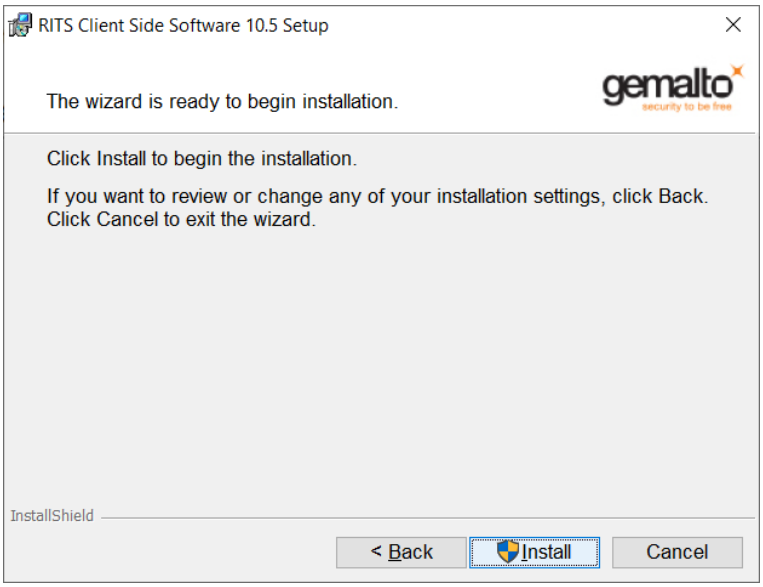
The following screen will be displayed. Select **I accept the license agreement** and click **Next**.



The following screen will be displayed. Click **Next**.



The following screen will be displayed. Click **Install**.

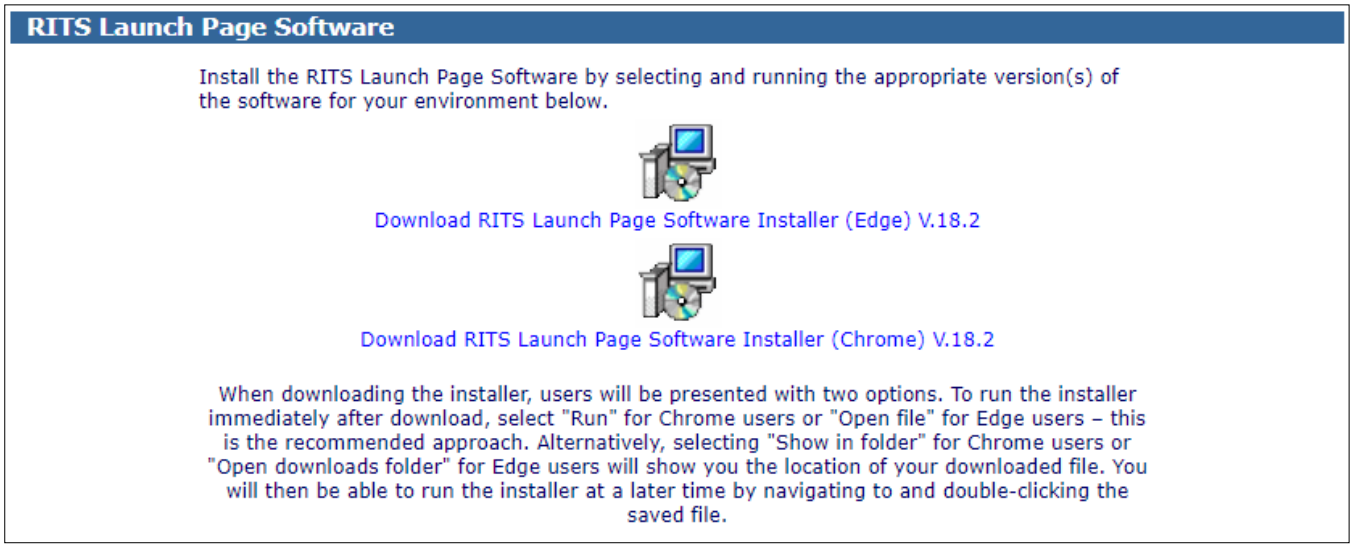


When the installation has finished, the following screen will be displayed. Click **Finish**.

5.3.5 Install the RITS Launch Page

The RITS Launch Page software installer is available from the RITS software page, www.rba.gov.au/rits/software/.

Separate versions are available for Google Chrome and for Microsoft Edge browsers. Choose and download the appropriate version(s) for your environment.



Once the RITS Launch Page software has been installed, a shortcut will be placed on the desktop:

Google Chrome *Microsoft Edge*

When selected, the shortcut opens the RITS Launch Page, which automatically detects at which sites RITS is available and connects to RITS using the default network path. It also has a manual option that permits the user to select network paths.

5.4 Reports and Data Exports

RITS provides options for generating reports in PDF format and data exports to Excel. All Reserve Bank testing of these functions has been performed with Adobe Acrobat Reader DC (Windows 10, 2021 version) and Microsoft Office Excel 2013.

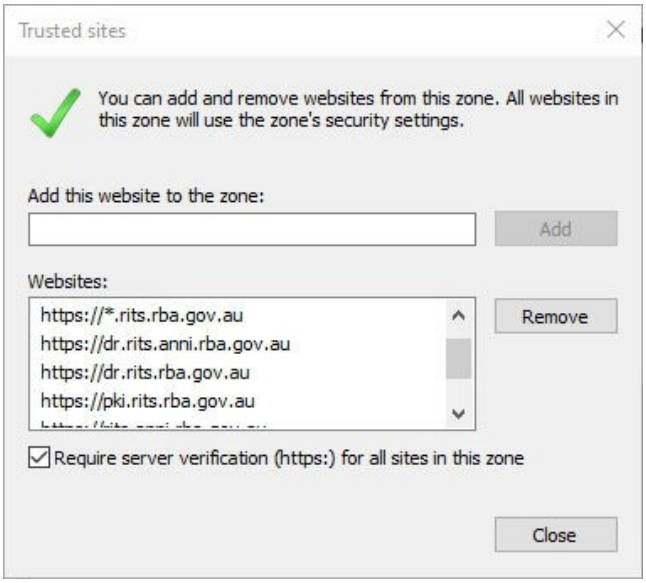
6. Browser Settings

6.1 Security Settings

6.1.1 Trusted sites zone

The following site addresses should be added to the **Trusted sites** zone list in the **Security** tab in **Internet Options**, accessible through the Windows Control Panel:

- https://*.rits.anni.rba.gov.au
- https://*.rits.rba.gov.au
- https://pki.rits.rba.gov.au
- https://rits.anni.rba.gov.au
- https://dr.rits.anni.rba.gov.au
- https://rits.rba.gov.au
- https://dr.rits.rba.gov.au

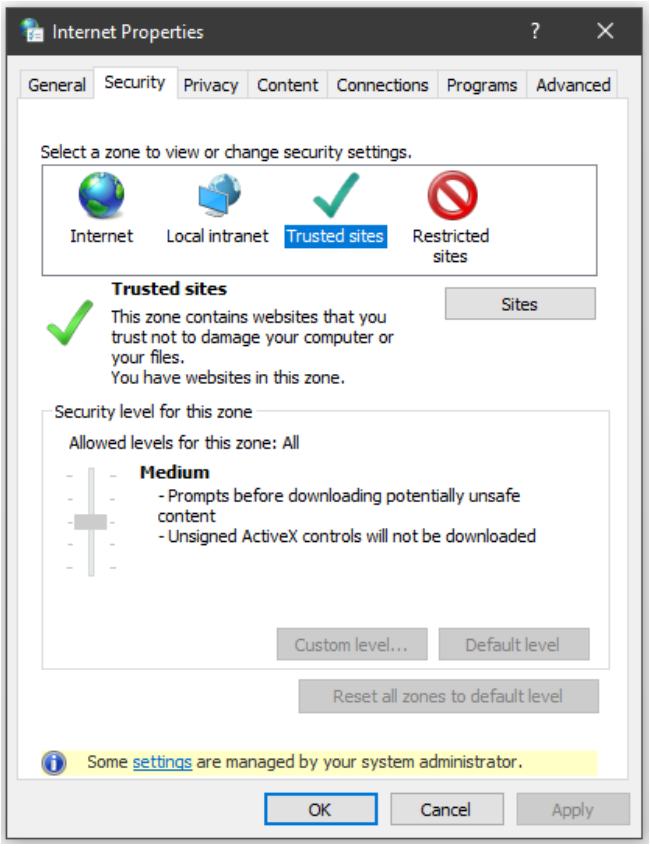


Additionally, the Trusted sites zone security settings should be modified, where required, to ensure that the following settings are set to the required levels:

Grouping	Trusted sites zone setting	Required value
Downloads	File Downloads	Enable
Miscellaneous	Web sites in less privileged web content zone can navigate into this zone	Enable

6.1.2 Protected Mode

It should be possible to login to RITS with Protected Mode switched either 'On' or 'Off'. The preferred option is to have Protected Mode switched '**On**' in the **Security** tab in Internet Options, accessible through the Windows Control Panel.



6.2 Pop-ups

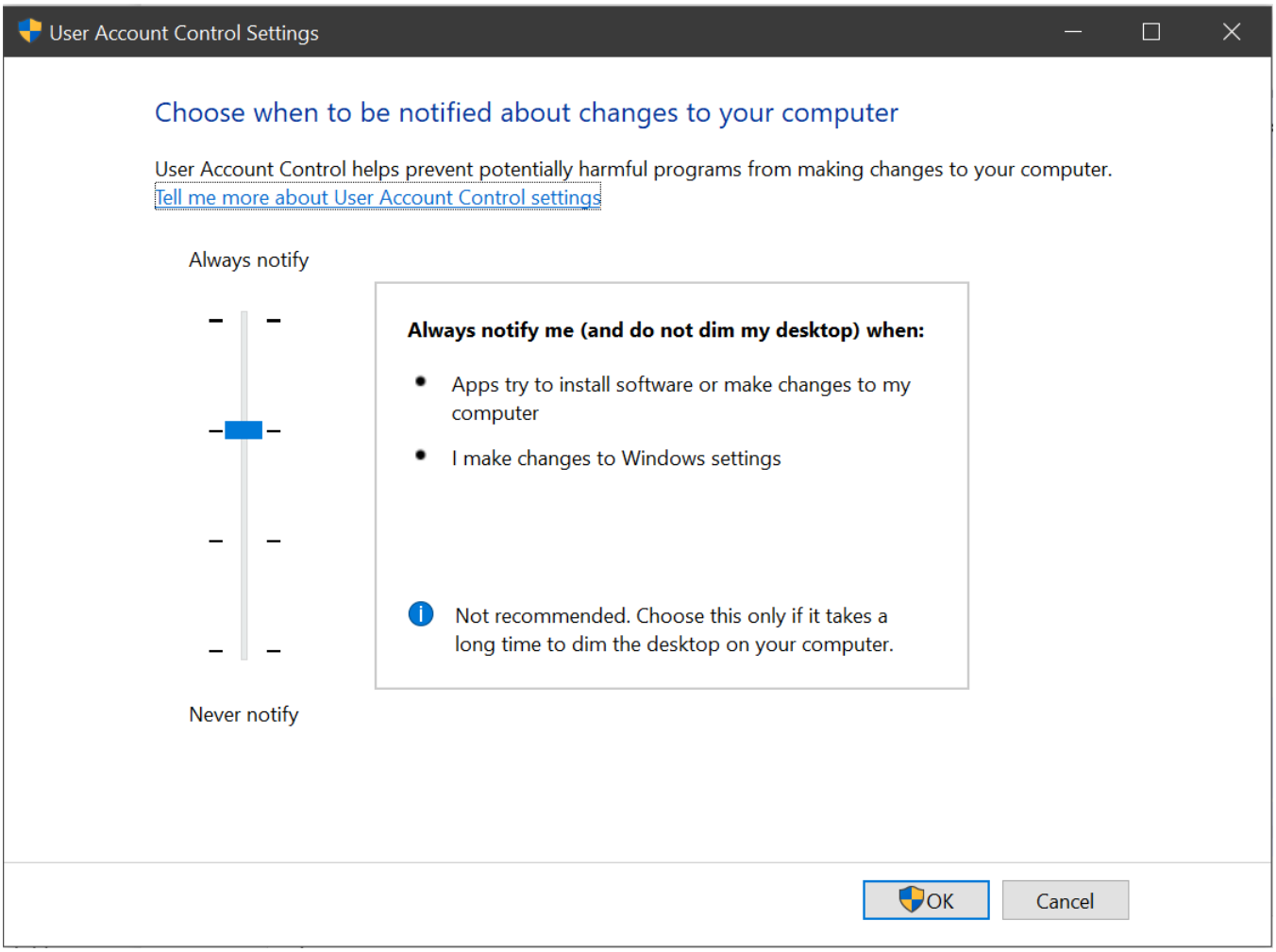
Browser pop-up blockers (in Microsoft Edge found under More -> Settings -> Cookies and Site Permissions -> Pop-ups and redirects; in Google Chrome found under More -> Settings -> Privacy and Security -> Site Settings -> Pop-ups and redirects) and third party pop-up blockers can interfere with the RITS login process, and may also interfere with other RITS screens.

Most packages allow pop-up blocking to be disabled for specific sites. However, due to the wide variety of blocking software available, the Reserve Bank cannot provide specific instructions for doing this for every package available. If you encounter errors such as the ones in Appendix 3, and you have ensured your settings comply with those in this guide, please ensure that pop-up blocking is not active for the RITS website. If that does not work, try disabling all pop-up blocking software. See your System Administrator if you require further assistance with this. If no pop-up blocking software is active and your software is configured as indicated in this guide, then contact the RITS Help Desk.

6.2.1 User Account Control (UAC)

Collection of RITS certificates may be affected by this setting. Before collecting a certificate, please disable UAC for the user account that will collect the certificate. Note: you must be an Administrator to modify the UAC Settings.

This is done by selecting Control Panel->User Accounts->Select the user collecting the certificate->Select 'Turn User Account Control On (Always Notify) or Off (Never Notify)' by using the slider up/down accordingly.



Once the certificate has been collected, you may turn UAC back on (Always Notify) and use RITS. Only the collection of certificates is affected by this setting.

7. Environment Requirements

7.1 Unique Email Addresses

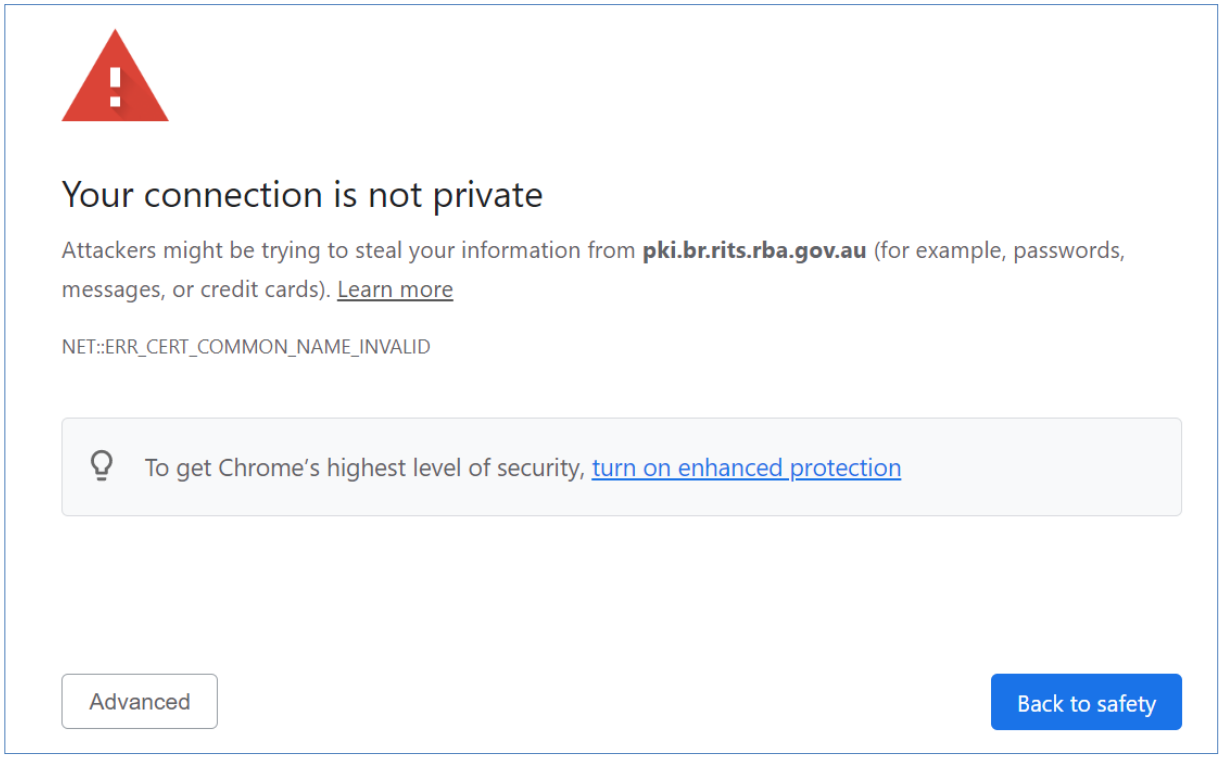
RITS records an email address for each user ID. This is used to send security information during the certificate enrolment procedure. By default, RITS security arrangements do not allow multiple users to have identical email addresses for receipt of this information. This does not preclude users from being in email groups for other purposes. Refer to Section 3.2.2 for more information.

Email addresses are subject to certain restrictions that are common in business applications. In particular, apostrophes and single quotation marks are not accepted as valid characters in email addresses.

7.2 SSL Encryption

Member access to RITS systems is protected via SSL. This requires that the Member must type **https://** before the appropriate URL.

For the Member to be confident in their secure connection, the 'common name' referred to in the SSL certificate should match the corresponding name in the URL used for accessing the server. If the name does not match, a warning message is displayed that indicates a mismatch. The following image shows a sample browser-generated warning message that a Member may see if a mismatch occurs.



Under normal circumstances, Members should not see a warning message. Members that access RITS via the internet, and Members that have set up their internal DNS or alternative name resolution mechanism in accordance with Reserve Bank recommendations, should not see these warning messages.

Note that HTTP/HTTPS requests may be compressed between RITS and users' PCs to achieve optimum response times.

7.3 Network Address Translation (NAT)

Members who currently perform their own NATing to access RITS need to modify the IP addresses provided by the Reserve Bank. Details of IP addresses are provided in Appendix 1.

7.4 DNS and Name Resolution

For **internet-based access** to RITS, the look-up is performed by checking the Reserve Bank's (public) domain name server (DNS), which is registered as being authoritative for the domain rba.gov.au.

For **ASX Net access**, where there is no DNS, a Member organisation must use its own mechanism to resolve to the correct IP address.

The most common approach is to use an internal (private) DNS server that is checked first before the external name server.

Another option that may be used is to configure the 'hosts' file with the required look-up information. The relevant hosts file could be on the workstation or on a proxy server, depending on the following:

- if the browser **is** configured to use a proxy server[2] and there is ASX Net connectivity from that proxy server, then the hosts file on the proxy server should be modified;
- alternatively, if the browser **is** configured to use a proxy server and the RITS addresses (*rits.anni.rba.gov.au) are included in the proxy exception list[3], then the workstation hosts file should be modified. Some Members may use a Proxy Automatic Configuration (PAC) file as a variation on this solution; or
- if the browser **is not** configured to use a proxy server, then the hosts files on the workstation should be modified accordingly.

Details of URLs, DNS and host file details and IP addresses are provided in Appendix 1.

7.5 Caching for Improved Response Times

Some screen information may be cached on PCs to reduce network traffic and hence improve response times. Accordingly, Members' proxy and firewall configurations should respect HTTP cache-control directives.

Tests performed at the Reserve Bank using a Microsoft ISA Proxy server showed a significant system performance benefit when the settings ***Use HTTP 1.1*** and ***Use HTTP 1.1 through proxy connections*** were enabled in the browser. Members should assess whether this is helpful in their own environment.

7.6 Adobe Reader Settings

Adobe Reader may be used to read RITS reports generated in PDF format. If the ***Use HTTP 1.1 through proxy connections*** setting is enabled in the browser (see above), then in some versions of Adobe Reader, the ***Display PDF in browser*** option must be unchecked in Adobe Reader preferences. A reboot may be required for the change to take effect.

7.7 Timeout Period

Members' proxies and firewalls should not timeout pending HTTP/HTTPS requests in less than 60 seconds and, desirably, should be configured for a longer timeout period to assist their users.

[1] See Windows Control Panel/Internet Options/Connections/LAN Settings
[2] See Windows Control Panel/Internet Options/Connections/LAN Settings/Advanced

7.8 Maximum Transmission Unit (MTU) Size

Members may experience a 'no page displayed' error caused by registry settings for MTU size. In this case, the machines may require an additional entry in the registry, the MTU parameter. (**Please note that changes to the Registry require great care and should only be undertaken by experienced personnel.)** To add this registry entry:

1. Start Regedit.
2. Select HKEY_LOCAL_MACHINE.
3. Select System/Current Control Set/Services/TCPIP/Parameters/Interfaces. There will be several keys under Interfaces. Select the key that contains the Current IP address by inspecting each of the keys values for DhcpIPAddress. The current IP address can be found using IPCONFIG in a DOS window.
4. Once the correct key is determined, a new value needs to be added (i.e. if the MTU value does not already exist. If the MTU value does exist, make a note of the current setting):
    - Select Edit-New-DWORD value;
    - Name the value MTU;
    - Double click on MTU;
    - Set the MTU to have a decimal value of 1300;

    NOTE: If the MTU value already exists, ensure that it is set to 1300 or less.
5. Exit from Regedit and RESTART the machine. Test access to RITS. If this registry change does not fix the problem, then set the MTU parameter back to the previously noted value and advise the RITS Help Desk.

7.9 Fast User Switching

The Fast User Switching feature must be disabled. To do this:

1. Login as a user with administrative rights.
2. Click Start, type `gpedit.msc` in the Start Search or Run dialog box and click Enter.
3. Navigate to the following location: Local Computer Policy > Computer Configuration > Administrative Templates > System > Logon.

Set *Hide entry points for Fast User Switching* to *Enabled*.

7.10 Secondary Site Arrangements

The RITS Launch Page will detect if the secondary site links are to be used for RITS access. Users who are logged in before a failover to the secondary site will need to login again.

Details of URLs for the secondary site system are provided in Appendix 1.

8. Thin Client Installations (e.g. Citrix or Windows Terminal Services)

The Reserve Bank does not provide Member support for thin client installations, whether via Citrix, Windows Terminal Server or other products. Where a Member decides to use thin client technology, they should ensure that the client/server connection is encrypted to preserve the integrity of the signing and the privacy of the token PIN.

The Reserve Bank does use Citrix in some of its operational environments. Consequently, RITS has undergone some testing with Citrix, particularly in relation to the use of the SafeNet eToken security tokens. Testing revealed the standard SafeNet Token drivers supplied as part of the RITS Client Installer should be installed on the both the Citrix Server and Citrix client. Each organisation has its own technical environments and this Technical Information Paper provides basic guidelines and steps towards the thin client installation due to differences in the member technical environments.

The Reserve Bank has not investigated whether its experience with Citrix is relevant to the Windows Terminal Services environment.

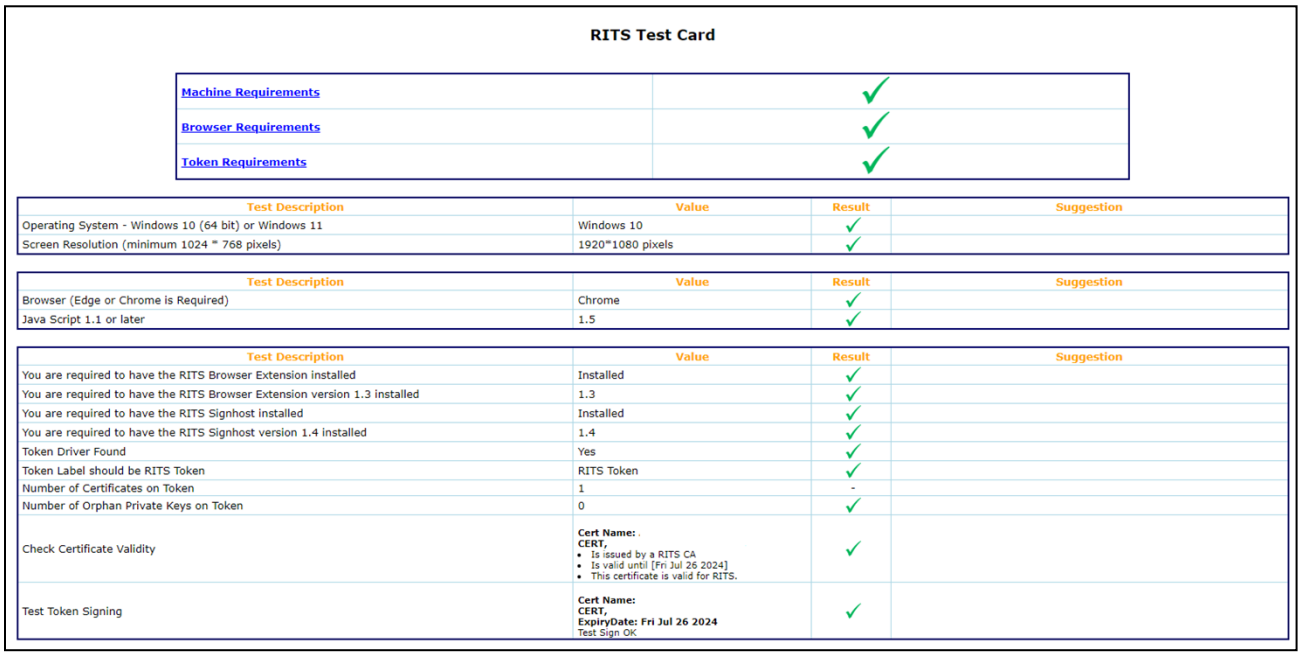
9. System Validation – Test Card

The Reserve Bank has developed a 'Test Card' web page where Members are able to confirm that all the required software has been installed correctly on a particular PC and that it has connected through relevant firewalls and networks to RITS. The Test Card also identifies if a token with a valid RITS certificate installed is present. However, it will not be necessary to have a token/certificate for the initial system validation.

The Test Card can be accessed from a link on the RITS Login page, or directly at www.rba.gov.au/rits/testcard.

Please note that the first time you run the Test Card, you may be prompted to enter the token codeword.

An example Test Card screen is shown below:



RITS Test Card

Machine Requirements	✓
Browser Requirements	✓
Token Requirements	✓

Test Description	Value	Result	Suggestion
Operating System - Windows 10 (64 bit) or Windows 11	Windows 10	✓	
Screen Resolution (minimum 1024 * 768 pixels)	1920*1080 pixels	✓	

Test Description	Value	Result	Suggestion
Browser (Edge or Chrome is Required)	Chrome	✓	
Java Script 1.1 or later	1.5	✓	

Test Description	Value	Result	Suggestion
You are required to have the RITS Browser Extension installed	Installed	✓	
You are required to have the RITS Browser Extension version 1.3 installed	1.3	✓	
You are required to have the RITS Signhost installed	Installed	✓	
You are required to have the RITS Signhost version 1.4 installed	1.4	✓	
Token Driver Found	Yes	✓	
Token Label should be RITS Token	RITS Token	✓	
Number of Certificates on Token	1	-	
Number of Orphan Private Keys on Token	0	✓	
Check Certificate Validity	**Cert Name: . CERT,** • Is issued by a RITS CA • Is valid until [Fri Jul 26 2024] • This certificate is valid for RITS.	✓	
Test Token Signing	**Cert Name: CERT, ExpiryDate: Fri Jul 26 2024** Test Sign OK	✓	

10. PC Information Captured at Logon

Information about a user's PC configuration is captured at every logon to RITS. This information is limited to:

- Browser Version
- Windows Version
- Token Driver Version
- Token Serial Number
- Token Model Type

An example of this information is shown below:

```
IE=Edge,OS=Windows10,TDV=eTPKCS11.dll,TSN=90188678,TM=eToken
```

This information can be used to troubleshoot Member technical issues and to guide future support arrangements for the RITS user interface.

11. Further Information

Further information is available from the RITS Help Desk:

Freecall: 1800 659 360*
International: +61 2 9551 8930*
Email: rits@rba.gov.au
* Calls to and from this number are recorded.

Appendix 1 – Summary of Hosts, Names, Addresses and URLs

(1) Web addresses for RITS environments via Internet:

Resolved over the public DNS – no IP addresses required:

- https://rits.rba.gov.au – access to RITS Primary Site Production via Internet/Intranet
- https://dr.rits.rba.gov.au – access to RITS Alternate Site Production via Internet/Intranet
- https://pp.rits.rba.gov.au – access to RITS Pre-Production via Internet/Intranet

The Reserve Bank may vary at its option the environment used for connection to RITS.

(2) Web addresses for RITS environments accessed via ASX Net:

Resolved using Member organisation DNS, or local hosts files:

- rits.anni.rba.gov.au – access to RITS Primary Site Production via ASX Net 172.21.1.10
- dr.rits.anni.rba.gov.au – access to RITS Alternate Site Production via ASX Net 172.23.1.10
- pp.rits.anni.rba.gov.au – access to RITS Pre-Production via ASX Net 172.23.1.30

(3) Certificate Authority: Web addresses used by Members during certificate enrolment:

Resolved over the public DNS – no IP addresses required:

- https://pki.rits.rba.gov.au – Member enrolment

NETWORKS USED BY RITS

For Members' information, the following networks are reserved for internal use by the Reserve Bank and the ASX for RITS communications. Members DO NOT need to have routes to these full Class B networks; however, they have been established for external access to Reserve Bank applications.

- 172.21.0.0/16
- 172.22.0.0/16
- 172.23.0.0/16

NETWORK ROUTES REQUIRED

Routes **ARE REQUIRED** in the Members' network to the following sub-networks to access RITS:

- 172.21.1.0/24 RITS UI Primary Site applications
- 172.22.1.0/24 (reserved for future use)
- 172.23.1.0/24 RITS UI Secondary Site applications and Pre-Production

The Gateway to these networks is the local ASX Net router.

NETWORK PORTS REQUIRED TO BE OPEN

80	(http)
443	(https)

Note also that certificate enrolment requires https access over the internet.

SAMPLE HOSTS FILE FOR ASX NET ACCESS

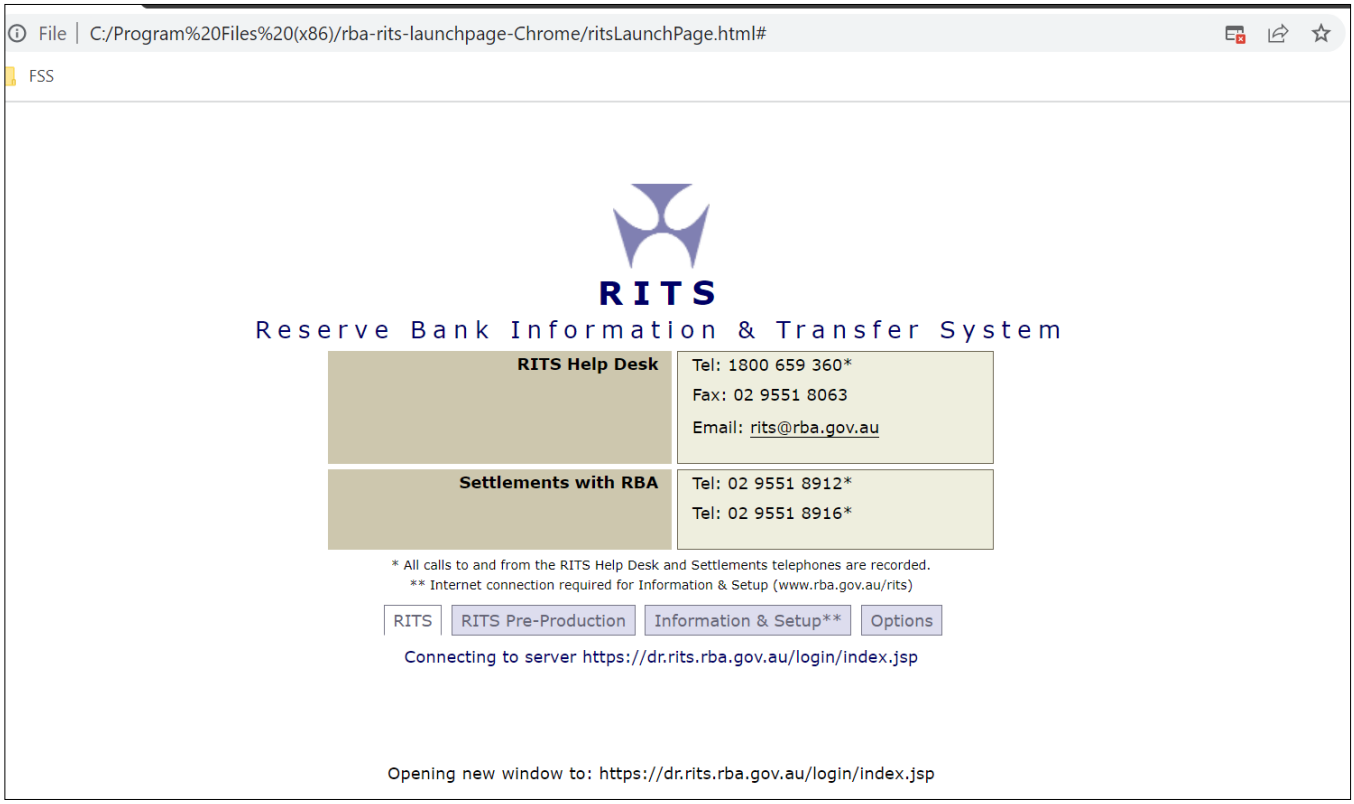
```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a # symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#      38.25.63.10      x.acme.com              # x client host

127.0.0.1       localhost
172.21.1.10     rits.anni.rba.gov.au
172.23.1.10     dr.rits.anni.rba.gov.au
172.23.1.30     pp.rits.anni.rba.gov.au
```

Appendix 2 – Examples of problems caused by pop-up blocking

Warnings such as the samples below may be seen when accessing RITS when pop-up blocking is enabled.

Chrome browser:



Microsoft Edge browser: