



RESERVE BANK OF AUSTRALIA

RITS User Access and Browser Upgrade Program – Migration Guide

**February 2023
Version 1.2**

Contents

1.	Introduction	1
2.	Migration Overview	2
	2.1 Migration stages	2
	2.2 Compatibility Matrix	3
	2.3 Migration Timeline	3
3.	Stage 1: Member Environment Configuration	4
	3.1 Centrally Managed PC Configuration	4
	3.2 Non-Centrally Managed PC Configuration	5
	3.3 Early access to the RITS Software	5
	3.4 RITS User Testing	6
4.	Stage 2: Pre-Production Testing and Readiness	7
	4.1 Centrally Managed PC Configuration	7
	4.2 Non-Centrally Managed PC Configuration	8
	4.3 RITS Software Rollout	8
	4.4 RITS Pre-Production Testing	9
5.	Stage 3: Production roll out	11
	5.1 Group policy changes	11
	5.2 Access testing	12
6.	Troubleshooting	12
7.	Appendix – Member Attestation Links	13

Revision History

Version	Status	Date Completed	Comments
1.0	Draft	4 November 2022	Initial draft (internal circulation only)
1.1	Final	1 January 2023	Final version
1.2	Final	15 January 2023	Hyperlink updated in Section 3.4

1. Introduction

This Migration Guide provides RITS Members with detailed steps necessary to migrate to the 2023 version of the RITS User Interface (UI) software, expected to go live at end- June 2023.

The changes described in the Guide are **mandatory** for all RITS users. Once the new RITS access solution is live, users will no longer be able to access RITS using previous versions of the software.

Members are expected to properly configure, test and run the new version of the RITS software to ensure their continued access to the RITS UI post go-live.

Once the steps outlined in this guide have been completed, users will access the RITS UI using either Google Chrome or Microsoft Edge. Unlike the 2022 version of the RITS software, the new version does not use Java Runtime Environment and Microsoft Edge in Internet Explorer (IE) Mode to access the RITS UI.



Warning: This Migration Guide has been developed as part of the RITS User Access and Browser Upgrade Program. It provides instructions to upgrade PCs which already have the previous version of the RITS UI software installed. Members should set up any new PCs with the 2022 version of the software before upgrading them in accordance with this Guide.

2. Migration Overview

The Migration Guide has been divided into three sections to provide clear instructions for Members accessing and testing the new software before it is released to the Production environment. Each stage requires mandatory member actions as summarised below.

2.1 Migration stages

Stage 1 – Member Environment Configuration

The first stage of the migration requires Members to configure their enterprise IT environment to enable the download and installation of the new RITS software. These steps are necessary to gain early access to the software and associated documentation. Once the new RITS software has been downloaded and installed, Members are welcome to perform their own internal security reviews on the new solution components.

By **14 April 2023**, Members **must** lodge a completed *Member Environment Configuration Attestation* to confirm their completion of stage one.

Stage 2 – Pre-Production Testing and Readiness (transitional period)

The second stage of the migration requires Members to test and configure the new solution components in the RITS Pre-Production environment. From the 17 April 2023, Members must apply configuration changes to their Group Policy settings to access RITS in the Pre-Production environment using the new RITS software. Mandatory Pre-Production testing is required to confirm the successful integration of the new software components in RITS. Members are also encouraged to perform their own testing in addition to the provided test cases to ensure all RITS functionality behaves as expected.



Warning: Once the new solution components have been released to the Pre-Production environment on 17 April, only the new (2023) version of the RITS UI software will be able to access RITS in that environment. Members should ensure that all users with a need to access the RITS Pre-Production environment for testing or BAU activities after that date are set up with the new software.

During this testing and readiness stage, the old (2022) version of the RITS UI software will continue to be used to access RITS in the Production environment. The new version will not be able to access RITS in the Production environment in this transitional stage.

By **16 June 2023**, Members **must** lodge a completed *Pre-Production Testing and Readiness Attestation* to confirm their completion of stage two.

Stage 3 – Production Roll-out

The migration will conclude with the release of the new RITS software onto the Production environment. Members will be required to apply configuration changes on the Go-Live date so that their users can access RITS in the Production environment using the new version of the RITS software and through either Edge or Chrome.



*Warning: Once the new solution components have been released to the RITS Production environment on **24 June 2023**, only the new (2023) version of the RITS UI software will be able to access RITS. Members should ensure that from this date **all** users are set up with the new software.*

2.2 Compatibility Matrix

The following table lists all software and hardware components required to access RITS.

RITS Access Solution Components	Current (2022 version of RITS software)	New (2023 version of RITS software)
Java Runtime Environment (JRE)	Version 1.8	Not required
RITS Integration Solution	Java applets	RITS browser extension and RITS Sign Host application
Browser	Microsoft Edge in IE mode (v78 or later)	Choice of: <ul style="list-style-type: none"> • Microsoft Edge (native) v107 or later • Google Chrome v107 or later
Operating System*	Windows 10 (64 bit)	Windows 10 (64 bit)
SafeNet Authentication Client	Version 8.2	Version 8.2 and above
Hardware Tokens	All RBA-supplied tokens	RBA-supplied eToken 5110†

* Windows 11 is not currently supported

† Some older model tokens are compatible with the new solution, but are no longer supported by the vendor. All such tokens will be replaced with eToken 5110 model tokens by the end of Q2 2023.

2.3 Migration Timeline

To review the timeline for the RITS User Access and Browser Upgrade Program migration, see RITS Advice 16/2022 and any subsequent updates.

For additional information on the program, see [RITS User Access and Browser Upgrade Program](#).

3. Stage 1: Member Environment Configuration

The purpose of this stage is to ensure that Members are ready for the rollout of new RITS Software. Members will be required to configure their group policy settings to enable the download and installation of each component. Members are encouraged to review the software components and confirm successful setup by running the Early Access RITS Test Card on PCs of the pilot group of RITS users.

3.1 Centrally Managed PC Configuration

The following section applies for PCs that are centrally managed via group policies. For non-centrally managed PCs proceed to Section 3.2.

The group policy configuration changes aim to:

- allow the RITS browser extension to be installed and run
- allow the RITS Sign Host application to communicate with the RITS browser extension
- allow early access to the new RITS Software
- allow the installation of the RITS browser extension on all user browsers (automated rollout)

Follow the instructions in Section 3.1.1 for all PCs which will access RITS using Edge, and follow the instructions in Section 3.1.2 for all PCs which will access RITS using Chrome.

3.1.1 Microsoft Edge

Perform the following changes to each RITS user's PC:

- a) Add the RITS Sign Extension ID to the [ExtensionInstallAllowlist](#) policy. The RITS Sign Extension ID can be found on the [Early Access RITS Software page](#).
- b) Add the [Chrome Web Store](#) to the [ExtensionInstallSources](#) policy.
- c) Enable the [Native Messaging User Level Hosts](#) policy.
- d) Add the RITS Sign Host ID ("au.gov.rba.rits.signhost") to the [Native Messaging Allow-list](#) policy.
- e) Add the following entry to the [Edge IE11 compatibility list](#) (edge://compat/enterprise). This is needed to allow the early access software links to run in Edge native mode during a transitional period while the rest of the RITS information and software pages still run in Edge (IE mode).

```
<site url="www.rba.gov.au/rits/browser-upgrade/">
  <compat-mode>Default</compat-mode>
  <open-in>Edge</open-in>
</site>
```

More information about Edge group policy settings can be found at <https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies>.

3.1.2 Google Chrome

Perform the following changes to each RITS user's PC:

- a) Add the RITS Sign Extension ID to the [ExtensionInstallAllowlist](#) policy. The RITS Sign Extension ID can be found on the [Early Access RITS Software page](#).
- b) Enable [Native Messaging User Level Hosts](#) policy.
- c) Add the RITS Sign Host ID ("au.gov.rba.rits.signhost") to the [NativeMessagingAllowlist](#) policy.

More information about Chrome group policy settings can be found at <https://chromeenterprise.google/policies/>.

3.2 Non-Centrally Managed PC Configuration

The following section applies for PCs that are not centrally managed via group policies. This includes any PC that is not connected to your organisation’s private network.

To apply the appropriate configuration changes for Edge users, continue to Section 3.2.1.

3.2.1 Microsoft Edge

For non-centrally managed computers, Edge’s IE11 mode needs to be disabled for the early access URLs and retained for the current RITS Production URLs.

- a) Open the Edge browser.
- b) Click the ellipsis (“...”) in the top-right corner.
- c) Select “Settings”.
- d) Select “Default Browser”.
- e) Delete the following URL from the list of the *Internet Explorer Mode pages* (if present).
<https://www.rba.gov.au/rits>
- f) Add the following URLs to the list of the *Internet Explorer Mode pages*
<https://www.rba.gov.au/rits/testcard/>
<https://www.rba.gov.au/rits/token/>
- g) Restart the Edge browser.

3.2.2 Google Chrome

No migration action is required in this step¹.

3.3 Early access to the RITS Software

To be able to download and install the Early Access RITS Software, the policy configurations (Sections 3.1-3.2) must be applied. Once the applicable Early Access RITS Software has been installed on each PC, run the automated tests in Section 3.4 to validate the configuration.



*Warning: The RITS Launch Page Software should **NOT** be used to access RITS until the Pre-Production cutover (Stage 2). Once the new RITS solution has been rolled out to the Pre-Production environment (Stage 3), the new solution will only work in Pre-Production until the Production Go-Live date. The RITS Launch Page Software has been included in the Early Access period for Members’ own internal testing and review.*

3.3.1 Install RITS Browser Extension

The *RITS Browser Extension* should be installed for the Chrome and/or Edge browser via the [RITS Browser Extension \(from Chrome Webstore\)](#) link available on the [Early Access RITS Software page](#). The recommended approach is via the Chrome Web Store, however the extension can be downloaded directly from the [Early Access RITS Software page](#) and installed manually in the Chrome or Edge browser.

¹ As Chrome is not supported by the 2022 version of RITS, no RITS configuration should have been made in this browser prior to migration.

3.3.2 RITS Sign Host

The *RITS Sign Host* application should be downloaded from the [Early Access RITS Software page](#). There are two MSI installer versions – one which only installs the software for the current user, and one which installs the application for all users. The ‘all users’ version requires the Windows user performing the installation to have administrative rights. The MSI installers and the signhost.exe executable are both [signed applications](#), however in some very restricted environments they may be need to be whitelisted manually.

3.3.3 Install the RITS Client Software

Existing PCs should have the RITS Client Software installed already. If setting up a new PC for migration testing purposes only, the token drivers can be installed via downloading and running the RITS Client Software installer (MSI) on the Production [RITS Software page](#) or the [Early Access RITS Software page](#). Installing this component requires the user performing the installation to have administrative rights. If setting up a new PC to access RITS during the transition period, set up the PC with the 2022 (current production) version of the software in accordance with <https://www.rba.gov.au/rits/info/technical/requirements.htm> then, if also needed for testing, upgrade it in accordance with this Migration Guide.

3.4 RITS User Testing

After the successful installation of the above three components (RITS browser extension, RITS Sign Host, and the RITS Client Software), users can test their set up by running the [Early Access RITS Test Card](#). To complete all the available tests, ensure a RITS SafeNet token is connected to the PC.

4. Stage 2: Pre-Production Testing and Readiness

The purpose of this stage is to roll out the RITS Software to users on the Pre-Production environment. Members will be required to implement configuration changes to enable RITS access via Edge and Chrome browsers. Members must also perform mandatory testing to confirm RITS functionality on the new browser environments. An attestation containing the mandatory tests and configuration changes must be submitted upon completion, it is recommended that Members roll out these changes to a sufficient number of RITS users to uphold current and future minimum staffing requirements at all times.

All RITS users who will continue to use Edge for accessing RITS in the Pre-Production environment will be required to disable Edge's IE11 mode **only** for the RITS Pre-Production URLs listed below.

- pp.rits.anni.rba.gov.au
- pp.rits.rba.gov.au

This can be achieved via group policy changes (for centrally-managed computers) or via manual configuration.

4.1 Centrally Managed PC Configuration

4.1.1 Microsoft Edge

The aim of the group policy configuration changes at this stage is to switch the RITS Pre-Production URLs from IE11 compatibility mode to Edge native mode. This change is necessary only for centrally controlled PCs that will be using Edge for accessing RITS in the Pre-Production environment.

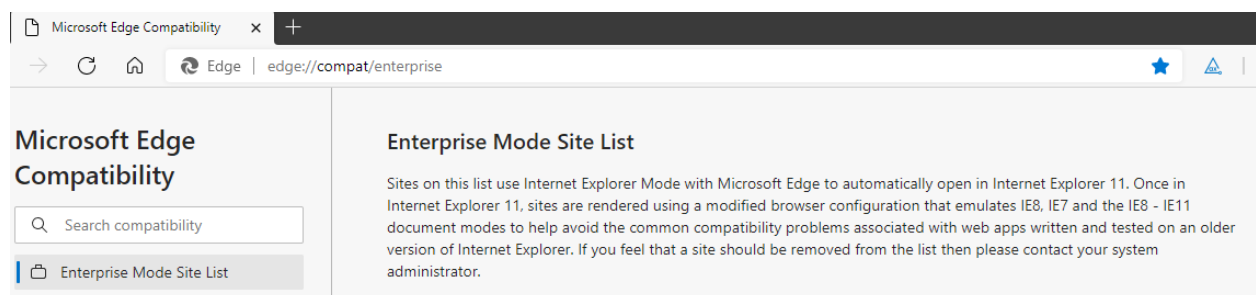
To switch from IE11 to Edge native mode, the <open-in/> element value should change from IE11 to Edge for the URLs listed in section 4.1.

Following is an example:

```
<site url="pp.rits.rba.gov.au/">
  <compat-mode>Default</compat-mode>
  <open-in>Edge</open-in>
</site>

<site url="pp.rits.anni.rba.gov.au/">
  <compat-mode>Default</compat-mode>
  <open-in>Edge</open-in>
</site>
```

To test that the group policy has been correctly set up, start an Edge session and enter "edge://compat/enterprise" in the URL bar.



The following RITS Pre-Production site entries should appear:

Domain		Engine		Allow redirect
*://pp.rits.anni.rba.gov.au/		EDGE		False
*://pp.rits.rba.gov.au/		EDGE		False

More information about MS Edge compatibility list configuration can be found on <https://learn.microsoft.com/en-us/deployedge/edge-ie-mode-policies>.

4.1.2 Google Chrome configuration

No migration action is required in this step².

4.2 Non-Centrally Managed PC Configuration

4.2.1 Microsoft Edge

This section describes how to disable IE11 mode on stand-alone (i.e. not centrally managed) computers.

- a) Open the Edge browser
- b) Click the ellipsis (“...”) in the top-right corner
- c) Select “Settings”
- d) Select “Default Browser”
- e) Delete the following URLs from the list of the *Internet Explorer Mode pages*
 - <https://pp.rits.anni.rba.gov.au/login/index.jsp>
 - <https://pp.rits.rba.gov.au/login/index.jsp>
- f) Restart the Edge browser

4.2.2 Google Chrome

No migration action is required in this step².

4.3 RITS Software Rollout

RITS users must install the RITS Browser Extension, RITS Sign Host and RITS Client Software as described in [Section 3.3](#) (if not already installed as part of Stage 1).

4.3.1 RITS Launch Page for Edge or Chrome

Download the new RITS Launch Page Software Installer from the [Early Access RITS Software page](#).

There are separate versions for Edge and Chrome browsers, and they can co-exist on the same PC. If the RITS user is installing the new RITS Launch Page for Edge, the current version (RITS Launch Page for Internet Explorer Mode) must first be uninstalled. Alternatively, if the RITS user is installing the Chrome version; do not uninstall the current Launch Page, doing so will result in the inability to access RITS in Production.

Once downloaded, run the MSI file to install the chosen version(s) of the RITS Launch Page software and follow the prompts. At completion of the installation, launch page shortcut(s) should be located on the

² As Chrome is not supported by the 2022 version of RITS, no RITS configuration should have been made in this browser prior to migration.

Windows desktop. When selected, each launch page shortcut should open the same browser as indicated by the MSI file.

Note that RITS Launch Page Software Installer requires the Windows user performing the installation to have local administrative permissions.

4.4 RITS Pre-Production Testing

The following section describes a minimum suite of tests that members must perform in this stage and before progressing to the next. Members are encouraged to exercise their normal business activities and testing using the browsers that they intend to use in Production at the next stage. The Reserve Bank recommends that Members perform their own testing in addition to the provided test cases to ensure all RITS functionality behaves as expected. In addition, if the RITS software has not been rolled out to all users; Members must test the RITS Software on an appropriate sized user group to ensure they can continue to meet the minimum [RITS staffing requirements](#) during and after the migration stage.

No	Test Item	Test Objective	Test Steps/Details	Remarks
T_01	Run Test Card	To ensure that all Test Card requirements are displayed as Passed with a Green Tick box in the Result column.	<ol style="list-style-type: none"> 1. Open the RITS Login page 2. Click on 'RITS Test Card' 3. Select Token and enter Token password 4. Check the requirements status 	
T_02	Login into RITS	To ensure that the user can access the RITS Home page successfully.	<ol style="list-style-type: none"> 1. Open the RITS Login page 2. Enter RITS credentials 3. Select Token and enter Token password 4. Check that the user arrives on the RITS Home page and the RITS UI is as per BAU 	
T_03	Execute any signed action	To ensure that RITS Signed actions are working correctly and users are able to write data into the RITS Database.	<p>Examples of Signed action in RITS that user may wish to execute:</p> <ol style="list-style-type: none"> 1. Update ESA Sub-Limit or Update Cash Account Limit 2. Enter a Cash Transfer transaction with Cash Account Status as "D" <p>Examples of Signed action in FSS:</p> <ol style="list-style-type: none"> 1. Update AT Trigger 2. Return to Reset Point AT 	Users may also wish to execute commonly used signed actions as per their BAU needs.

No	Test Item	Test Objective	Test Steps/Details	Remarks
T_04	Perform a data search	To verify that data search is working correctly.	<p>This will ensure that data is successfully retrieved from the database. The users can search for data in any of their preferred RITS enquiry screens for both Current Date and/or Archived Dates.</p> <p>For example:</p> <ol style="list-style-type: none"> 1. RITS Settled Payments under ESA Management 2. Settled Payments under FSS Menu (only for FSS participants) 	
T_05	Export data	To verify that the export functionality is working.	This will ensure that the user can export searched data in any of their preferred RITS Enquiry functions and validate that the data is exported correctly.	
T_06	Access the RITS Information Facility	To verify that users can access the Reserve Bank Information & Transfer System Information Facility.	<ol style="list-style-type: none"> 1. Click on the RITS Information Facility icon 2. Verify that the Reserve Bank Information & Transfer System Information Facility page opens successfully 	
T_07	Access the RITS Token Administration	To verify that the Token Administration functionality is working.	<ol style="list-style-type: none"> 1. Open the RITS Login page 2. Click on the 'RITS Token Administration' 3. Click on 'Check Orphan Key' 4. Enter Token password 5. Check that the appropriate message is shown 	

5. Stage 3: Production roll out

The purpose of this stage is to complete the migration process and to cut over the new RITS software to Production. Members will be required to implement group policy changes to allow for Chrome and Edge browser compatibility with RITS in the Production environment. Once this stage has been completed, RITS Production will only be accessible using the new RITS software. Members will no longer be able to access RITS Production using Edge in IE11 mode.

5.1 Group policy changes

The group policy configuration changes at this stage will be similar to those in stage 2, with the aim of removing the IE11 compatibility mode from all remaining RITS URLs.

5.1.1 Group policy changes

This section applies for centrally controlled PCs that will be using Microsoft Edge for accessing RITS.

Remove all RITS URLs from the Enterprise Mode Site List:

- rits.anni.rba.gov.au
- rits.rba.gov.au
- dr.rits.anni.rba.gov.au
- dr.rits.rba.gov.au
- pki.rits.rba.gov.au
- pp.rits.anni.rba.gov.au
- pp.rits.rba.gov.au
- www.rba.gov.au/rits/
- www.rba.gov.au/rits/browser-upgrade/

To test that the group policy has been correctly set up, start an Edge session and enter “edge://compat/enterprise” in the URL bar. None of the above URLs should appear in the list.

More information about MS Edge compatibility list configuration can be found on

<https://learn.microsoft.com/en-us/deployedge/edge-ie-mode-policies>

5.1.2 Manual browser configuration

This section describes how to disable IE11 mode on stand-alone (i.e. not centrally managed) computers.

- a) Start MS Edge browser
- b) Click the ellipsis (“...”) in the top-right corner
- c) Select “Settings”
- d) Select “Default Browser”
- e) Delete the following URLs from the list of the *Internet Explorer Mode pages*
 - <https://dr.rits.anni.rba.gov.au/login/index.jsp>
 - <https://dr.rits.rba.gov.au/login/index.jsp>
 - <https://rits.anni.rba.gov.au/login/index.jsp>
 - <https://rits.rba.gov.au/login/index.jsp>
 - <https://www.rba.gov.au/rits/testcard/>
 - <https://www.rba.gov.au/rits/token/>
 - <https://pki.rits.rba.gov.au/>
- f) Restart the Edge browser

5.2 Access testing

As part of Stage 2, all RITS software has been installed and tested in the Pre-Production environment. To confirm RITS access in Production via Edge or Chrome, users can simply login to RITS to test accessibility.

6. Troubleshooting

For troubleshooting guidance, see the [RITS Troubleshooting Guide](#).

7. Appendix – Member Attestation Links

7.1.1 Stage One – Member Environment Configuration

Attestation: https://www.rba.gov.au/rits/info/pdf/rits_upgrade_attestation_one.pdf

7.1.2 Stage Two – Pre-Production Testing and Readiness

Attestation: https://www.rba.gov.au/rits/info/pdf/rits_upgrade_attestation_two.pdf