

Digital Channels RDS & Citrix Integration Guidelines

Contents

1. Introduction	2
2. Installation	2
2.1. Client – hardware and software installation	2
2.2. RDS or Citrix server or desktop - software installation	2
3. Configuration	2
3.1. Client	2
3.2. RDS server or Citrix server or desktop	2
3.3. Group Policy Objects (GPOs)	2
3.4. Proxy servers	2

4. Appendix 1 – infrastructure notes	3
4.1. Network	3
4.2. Best practice	3

1. Introduction

This guide details how to integrate the Barclays security software into a Microsoft Remote Desktop Services (RDS) or Citrix environment. For digital channels to function correctly the end-user device used to connect to your RDS and Citrix infrastructure must correctly redirect the smart card reader within the user session. Compatibility and redirection Issues are rarely seen with Windows clients, but are more frequently seen with non-Windows clients. For support with compatibility and redirection issues please refer to the manufacturer of the end-user device.

Please note: Only the finger vein scanner is supported with Apple Mac end-user devices; and only when using Citrix Receiver. Please contact your client servicing team for installation guidelines.

2. Installation

2.1. Client – hardware and software installation

Only the smart card reader or finger vein scanner driver should be installed on the client. The drivers for the smart card reader can be downloaded from <https://supportportal.gemalto.com>. The finger vein scanner uses the in built-in Windows smart card driver.

Please note: Do not install the security software on the client. This configuration is unsupported and is known to cause issues.

2.2. RDS or Citrix server or desktop – software installation

Install the security software as outlined in the respective installation guides found in the Technical Support section.

Please note: Bluetooth functionality is not supported when using RDS or Citrix.

3. Configuration

3.1. Client

On the end-user device, ensure the Remote Desktop Client (RDC) or Citrix client is configured to allow smart card redirection and, where applicable, the smart card service is running.

3.2. RDS server or Citrix server or desktop

On the server or virtual desktop, perform the following tasks:

1. Ensure the RDS or Citrix server or desktop is configured to allow smart card redirection to the end-user device.
2. Ensure the smart card service is running.

3.3. Group Policy Objects (GPOs)

If you are operating in a Domain environment and use GPOs to configure user settings, you need to take the following into consideration:

The <https://cashmanagement.barclays.net> and *.barclays.com (for digital channels other than Barclays.Net) URLs will need to be added to any GPOs you use to configure trusted sites.

Ensure that Enable Protected Mode is unchecked for the Trusted Sites zone.

The Trusted Sites Zone will need to have its security level set to Medium or lower.

3.4. Proxy servers

If you use a content screening proxy server in your environment, you will need to take the following into consideration:

The URLs previously added to the trusted sites list will need to be added to any whitelist or other access control list in use in your environment.

When deploying the solution, please ensure that any proxy server you use are not inspecting or intercepting the SSL traffic to Barclays' digital channels. As an example, SSL inspection must be switched off for *.barclays.net and *.barclays.com

4. Appendix 1 – infrastructure notes

The following sections outline considerations you may find helpful regarding the infrastructure components impacted by the Gemalto eSigner and Classic Client software.

4.1. Network

Latency – network latency of more than 20ms RTT between the client and the virtual infrastructure will affect smart card reader users. In cases like this, we recommend using the finger vein scanner.

Jitter – this should be <5ms

Datagram loss – this should be <1%

Please note: Implementation of up to 20 Barclays' digital channel users using RDS or Citrix should not noticeably impact the performance of your network. In implementations of over 20 users, you should satisfy yourself that network performance will not be impacted by performing proper testing.

4.2. Best practice

In an RDS or Citrix environment, do not disconnect the session. You should always log off and ensure your session has logged off correctly from the remote server/session. If disconnected, a session may need to be re-opened on the same end user device to recover your smart card environment.

In order to benefit from any PC smart card enhancements, ensure that you have the latest hotfix or service pack installed on your system.

Plug and play of devices does not always work correctly over an active RDS/Citrix session, so please avoid hot-plugging of the smart card reader or smart card in an RDS or Citrix implementation.

The information contained within this document applies to Barclays' digital channels.

If you need further support, please contact your **Client Services Team** via the details available at:

- [Digital Channels Help Centre contact us](#)

General information about our digital channels can be found at:

- [Digital Channels Help Centre](#)

You can get this in Braille, large print or audio by calling 0800 027 1316, Option 1* (via Text Relay or Next Generation Text Relay if appropriate). For more information, please visit barclayscorporate.com/alternativeformats. Clients outside of the UK please contact your local Barclays representative or call +44 207 757 7323, Option 1**.

*Calls to 0800 numbers are free from UK land lines and personal mobiles, otherwise call charges may apply. Please check with your service provider. To maintain a quality service we may monitor or record phone calls. Lines are open Monday to Friday, 8am to 7pm.

**International call charges may apply.

This document is used by Barclays Bank PLC, Barclays Bank UK PLC, Barclaycard International Payments Limited, trading as Barclaycard and Barclays Bank Ireland PLC. Details of your service provider are set out in your customer agreement.

Item Ref: 9912792_DB. March 2021.