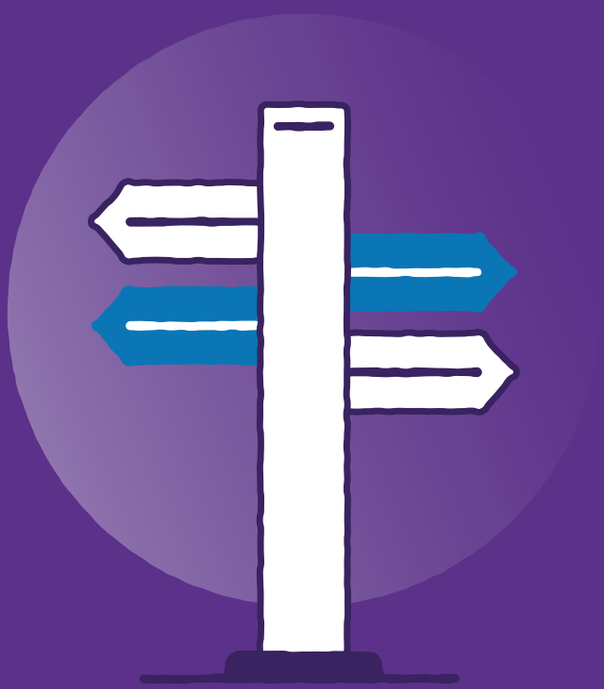
Remote Cheque Deposit

Customer technical overview.



NatWest

Tomorrow Begins Today

Table of contents

1. Introduction

Remote Cheque Deposit (RCD) is a web browser-based service that lets you scan and pay in cheque deposits without needing to go to the bank. We're introducing a new product called Unify to support this.

You can access the RCD service via Bankline. We'll soon provide you with a user guide with everything you need to get set up. Because RCD is presented via a web browser, it reduces the need for any persistent storage.

There's a few technical things you'll need to do before you can use the new RCD service.

To get started, you'll need a Windows service and a scanner driver, to be deployed on your local PC.

2. Solution overview

To access the RCD service, two configuration steps are required:

- **Step one** – Provides the user with access to the RCD functionality.
- **Step two** – Is the local installation of a Windows service and scanner drivers on your local PC to access the USB scanner.

Both configuration steps are explained in detail in the following sections.

2.1. Access to RCD functionality.

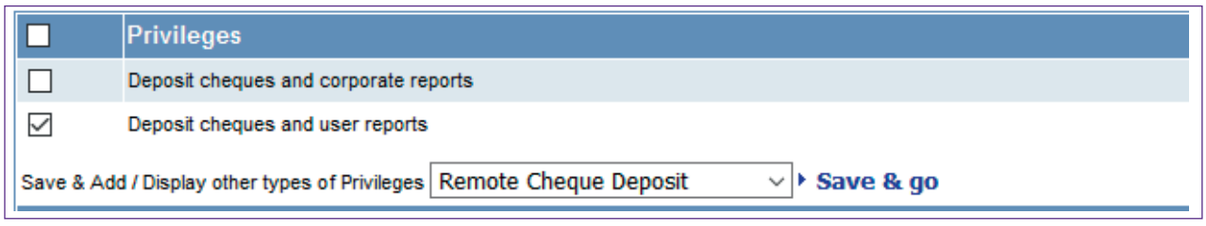
Your Bankline admin user will need to set up all RCD users with one of the two following privileges:

2.1.1. Deposit cheques and corporate reports.

With this privilege, a user can scan cheques and generate reports that include cheques processed by any of your users. This can be useful for administration or supervisor users, who need a complete overview of what has been captured on your Bankline ID.

2.1.2. Deposit cheques and user reports.

With this privilege, a user can scan cheques and generate reports that are limited to the cheques that they've processed themselves. This can be useful for larger multi-department organisations where data segregation is important.



Once access is granted, your users can access the RCD functionality via Bankline. The user will log in as usual, and look for the **Deposit cheques** link under the new **More services** tab.

2.2. Local installation and upgrade of scanner service.

To scan cheques, a cheque scanner must be attached directly to your local PC. The local PC must have a spare accessible USB port for the scanner to attach to. Supported scanner models are listed in Section 5.

Whilst the RCD user interface is presented via a web browser, the physical cheque scanner requires a Windows service called Unify Scanner Service (USS) to be installed on your local PC.

The purpose of the USS is to:

1. Manage initial deployment of the scanner drivers to your local PC
2. Update itself, as well as the scanner drivers, as necessary
3. Manage the communication between the web browser and the scanner

USS is installed on the local PC as follows:

- After the user logs in to RCD, the user interface (UI) will attempt to reach the USS. If the UI detects that the Windows service (USS) is not reachable, it'll guide the user to download and install the USS MSI (Microsoft Software Installer).
- The RCD UI sends a request to our Unify Deployment Services (UDS) to retrieve the USS MSI package from UDS.
- Once the UI downloads the MSI, a user with administrator privileges needs to run the MSI and install the scanner service.
- The USS (Windows service) runs under the NT Authority/LocalSystem account. "NT Authority/LocalSystem" account is a predefined local account and has all required privileges on the local PC to allow the scanner service to self-update and to install scanner drivers without user intervention.
- When the RCD UI identifies that a newer version of the scanner service MSI is available for download, it forces the user to install the latest updates before allowing the capture of new deposits. A request is sent to USS to download and install the new MSI. The USS performs an update by pulling down the new MSI package from UDS.
- The scanner service install will take a couple of minutes to apply updates – this can vary based on download bandwidth. After the upgrade procedure, the local PC shouldn't generally require a restart for the changes to apply.
- The RCD UI presents a list of available scanner drivers to the user. Once your user selects the appropriate scanner from the list, the UI makes a call to USS to download the driver package from UDS and install it on to the local PC. After the upgrade procedure, the local computer may require a restart for the changes to apply.
- Update of the scanner drivers will occur in a similar way to USS.

2.3. Connectivity.

RCD requires ongoing network connectivity from the RCD PC to:

- Bankline (https://www.bankline.natwest.com:443)
- NatWest Bank of APIs. (https://openapi.natwest.com:443)

Most customers will already have access to Bankline in their IT environments. NatWest Bank of APIs is required for a subset of banking products, including RCD, for which access may not have previously been configured in your IT environment. A DNS query shows that openapi.natwest.com returns a single, static public IP address, also showing the gateway is Apigee, part of Google Cloud. We don't expect the IP address to change, but there are some exceptional scenarios whereby it could change in the future.

3. Solution architecture

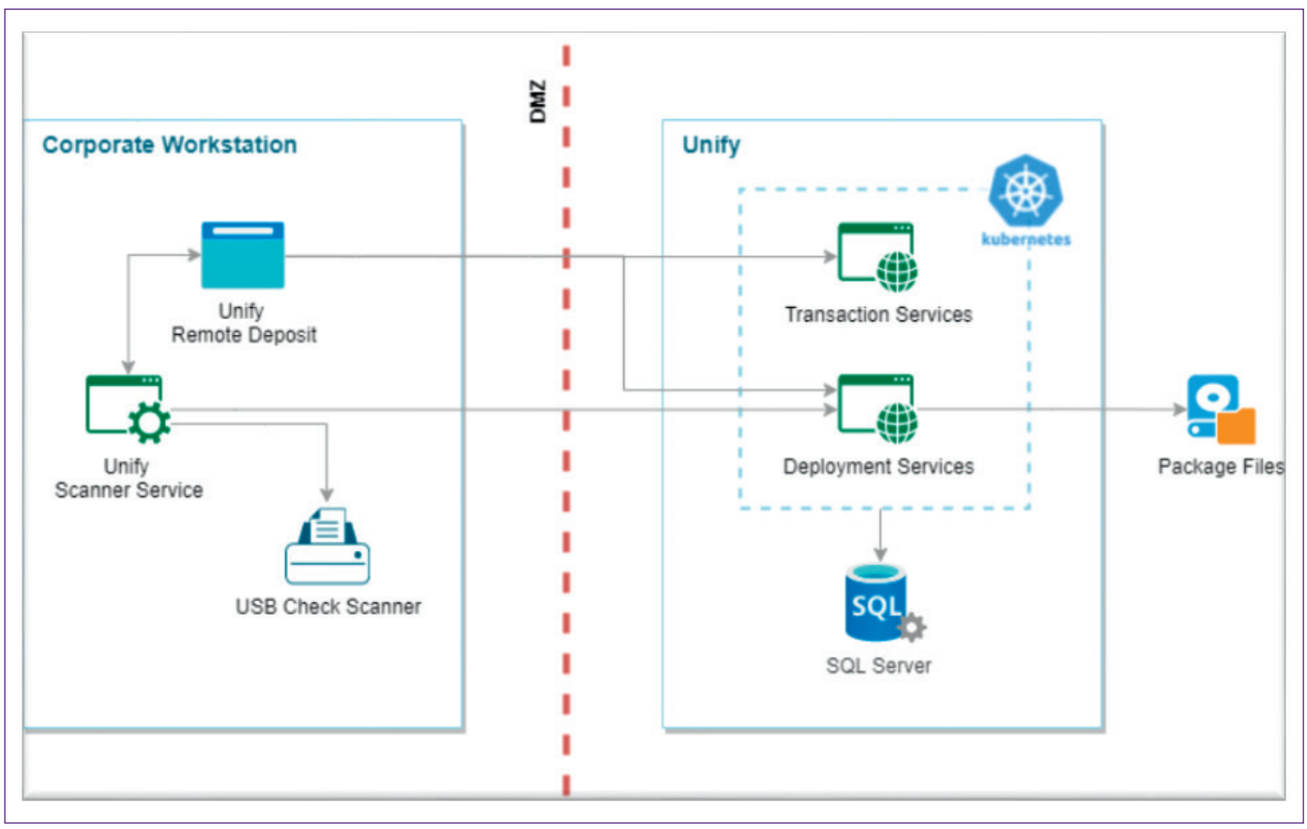
Integration between the scanner drivers, web browser and Unify solution involves three important components:

- USS installed on your local PC.
- RCD application running on a web browser.
- Unify solution hosted in the bank's environment.

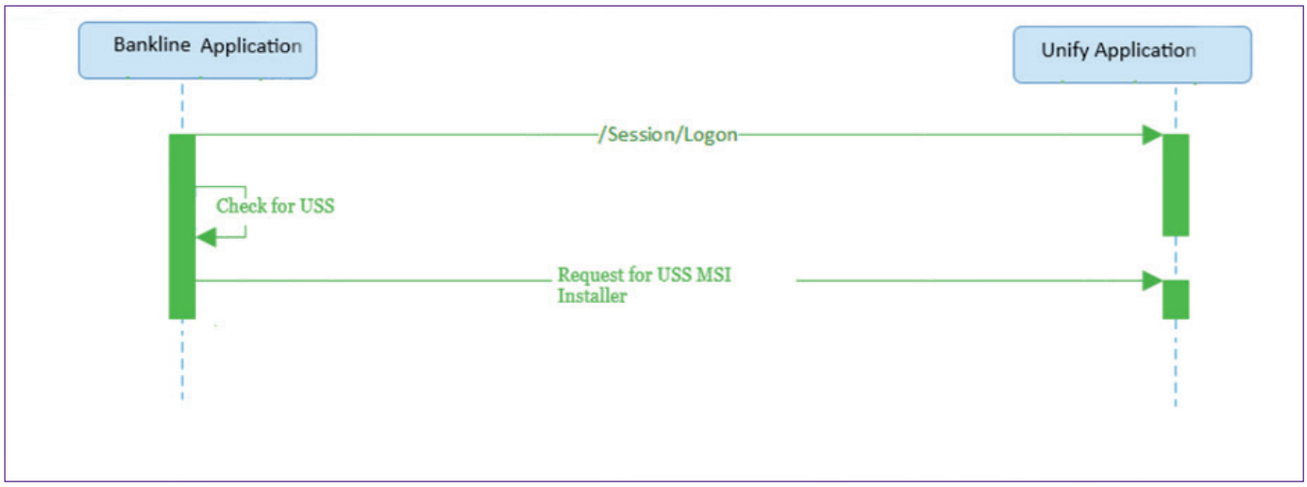
USS is a Windows service that hosts the scanner service API to provide support for USB scanners and is installed through an MSI installer. During the installation process, you have the option to configure the API/Event port, which is used for both scanner API methods and events. The installer assigns a Secure Sockets Layer (SSL) certificate to the TCP/IP port used by scanner service. The SSL certificate on the local PC is bound to a specified port so the scanner service can communicate with the RCD UI running in the web browser using HTTPS protocol. This ensures the communication between the scanner service and the RCD UI running in the web browser is secure.

The USS has two sets of APIs:

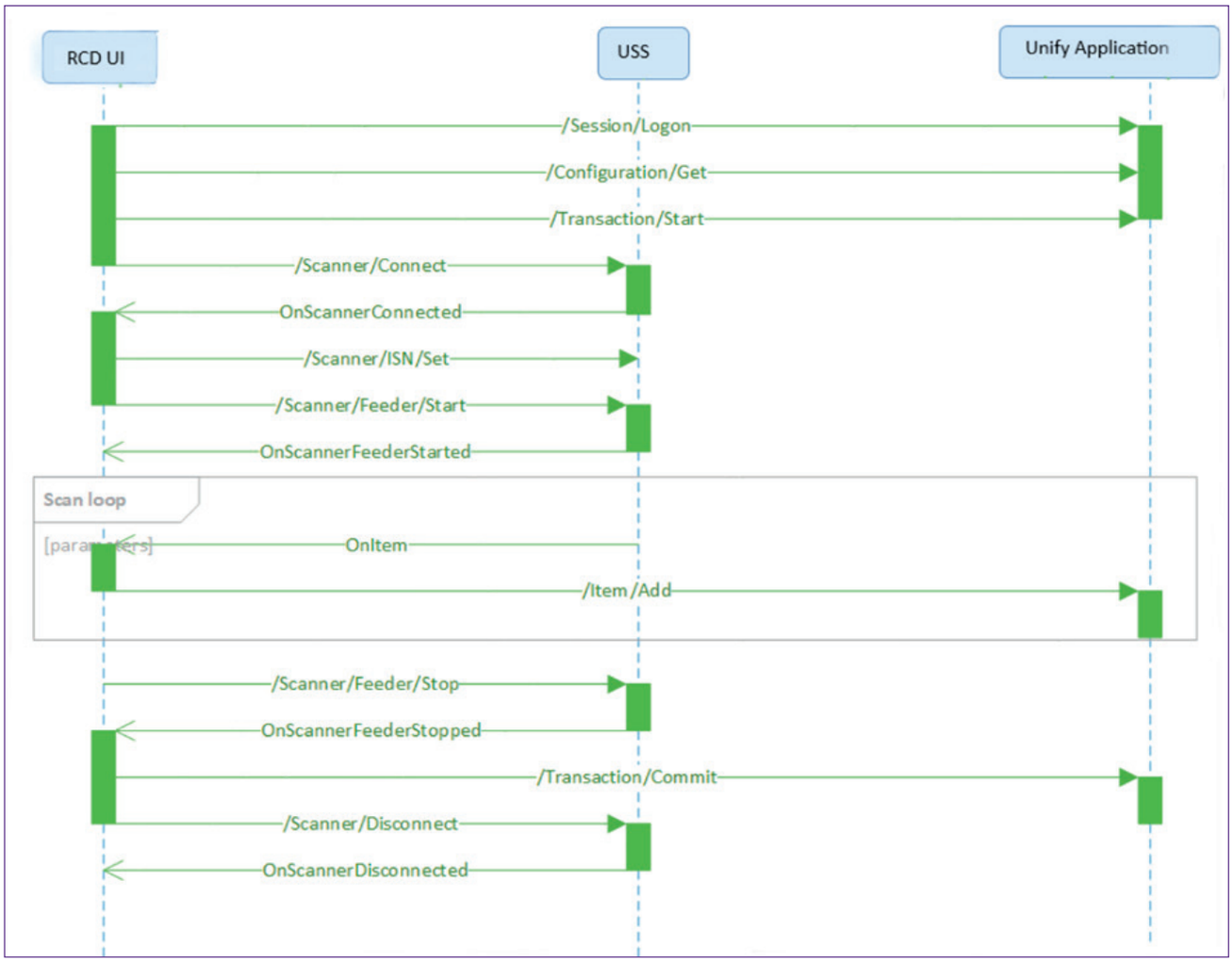
- Package Update API methods: this set of methods and events enables a client application to download and install software on the local PC.
- Scanner API methods: this set of RESTful APIs are used to scan items using a USB scanner. These APIs are used by the RCD UI running on the web browser to scan the cheques.



There are two important workflows that refer to USS. One is for a PC being used for the first time and the other for subsequent login to that PC. The first time a PC is used to log in to the Bankline UI through the browser and accesses the RCD UI, the user is guided to download and install USS MSI if the service is not reachable. Administrator rights are required at this time.



For any subsequent login, the RCD UI, running in a web browser, communicates with the Unify applications, hosted in bank network, for transaction functions and USS for scanner functions. All the calls to the USS are initiated from the RCD UI running in the web browser. The USS listens on the HTTPS port on localhost, configured at time of installation, RCD UI communicates to localhost to communicate with scanner service. This ensures the RCD UI application can seamlessly access APIs exposed by USS, even with restricted access privileges.



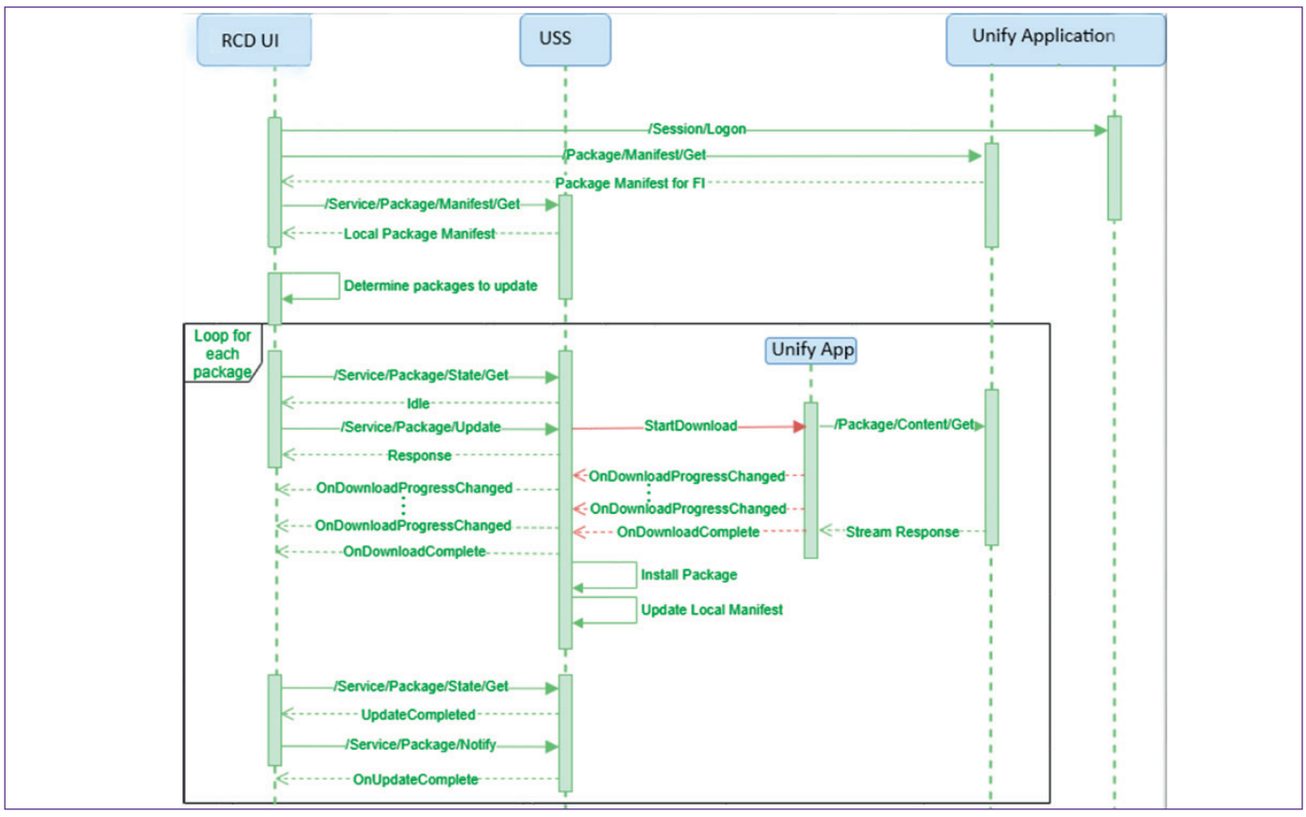
4. Security model

The core Remote Cheque Deposit (RCD) solution is hosted within the bank's infrastructure and complies with the bank's Information Security Policy. All software download locations are hosted within the bank. To access RCD, customers first log in to Bankline and then access RCD via an externally hosted API gateway (https://openapi.natwest.com, for which more information is available at https://www.bankofapis.com). The API gateway used by RCD is ISO27001 certified. RCD has been subject to all necessary functional and non-functional testing, including external Penetration Testing by a CREST and NCSC CHECK certified company.

As part of the secure user authentication, provided via Bankline, a token is provided that is then used to secure the various user journeys. No data is persisted on your workstation. Data is held on our bank network, which is secured in line with our own policies and procedures.

The following section describes the workflow and security measures taken to protect the system, while downloading and installing packages.

- USS maintains a local package manifest after the first package update and then subsequently updates the local manifest after each successful update to record the packages already installed on your local PC.
- The RCD application periodically compares the details of package present in your local PC with the manifest file present on our server. If a package is already present in the local manifest, then it may be skipped, and the remaining packages can be installed on the local PC.
- To download a new package, RCD UI invokes an API method defined in the USS passing the URL of package. USS validates the URL by whitelisting it against a list in a local file called ApprovedURLs.txt. The update will not proceed if the URLs are not whitelisted.
- A request for a new package contains JWT session token, the Package ID, Type and Signature Hash. The Package ID is used by the Unify application, hosted in the bank network, to fetch the package content and then stream it to USS. The downloaded file hash is matched by USS to the Signature Hash from the request. Updates will proceed only if they match.
- The USS and scanner drivers will both be digitally signed by the bank to ensure there's no tampering with the files being downloaded.



5. Supported configurations

A physical PC with these minimum specifications:

1. Windows 10 or 11, Professional or Enterprise Edition.
2. A USB 2.0 port to connect to the scanner.
3. Processor: Intel® Core™ i3 Processor (fourth generation or newer). Even better is Intel® Core™ i5 or Intel® Core™ i7 (2.0 GHZ or greater).
4. Browser: Edge (version 86 or higher), Chrome (version 86 or higher) or Firefox (version 81 or higher).
5. Memory: 4GB RAM or greater. If the memory is shared with your video graphics card, an extra 1GB of RAM will be needed.
6. Ethernet card: for network access, you need a minimum 100MB Ethernet card, but a Gigabit Ethernet card is recommended.
7. Display: you need a minimum workstation display resolution of 1280x800.
8. Disk space: to accommodate the operating system, application software and virtual memory, your PC needs a 60GB hard drive or greater.
9. Any additional Endpoint Protection Software (or equivalent) will need to (a) permit uninhibited access to the selected USB port on the PC to allow communication with the scanner and (b) allow the scanner service to download and run natively a self-extracting zip file in the form of a Windows executable file (.exe).
10. Please do not install the Digital Check TS240/CX30 scanner drivers before installing RCD for the first time on a PC. Only the driver delivered via RCD installation is supported (see section 2.3 of the User Guide).

A cheque scanner:

1. Digital Check TS240 or CX30.
2. Any other cheque scanner must be powered off or disconnected from the PC before using RCD.

6. Advanced troubleshooting

This section is to help your IT team troubleshoot any RCD related technical issues in your IT environment.

6.1. Your IT environment.

This section is relevant where RCD has previously been installed and used successfully to commit deposits.

1. Might any Windows patches have had a detrimental impact on the RCD scanning PC?
2. Might any other patches, security or other changes have had a detrimental impact on RCD?
3. Are there any required or pending Windows or browser updates? If so, can these be applied?
4. Do any specific exceptions/exclusions/whitelisting in your environment remain valid per section 2.3 - *Connectivity* above?
5. Do the *Supported Configurations* in section 5 remain valid?

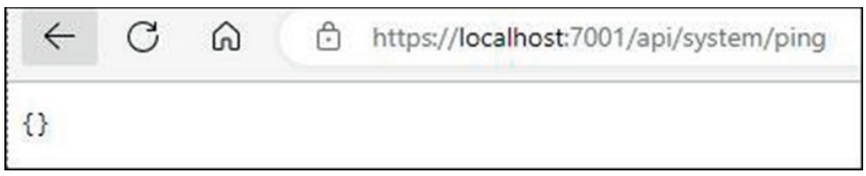
6. Might the use of any other cheque scanning applications be causing a conflict, for example if another application is connecting to the same scanner used by RCD? If so, avoid using the other application(s) to establish if there's a conflict and investigate if changes can be made to workflow, such as avoiding concurrent use of the applications and/or rebooting the PC and/or restarting the scanner between use.
7. Has the scanner USB connection been unplugged and/or inserted since the PC booted up, ie "hotplugged"? This may cause issues and can occur when laptops are used to connect to the scanner at different points during the day. Investigate if powering off the laptop and scanner, and powering on the laptop and scanner improves connectivity.

6.2. Unify Scanner Service.

1. The *Unify Scanner Service* is packaged as an MSI file and downloaded via the RCD UI. The initial installation of this MSI package requires Windows administrator privilege. Windows administrator privilege isn't required once the Unify Scanner Service has been successfully installed: the *Unify Scanner Service* runs using the local system account. *Section 2.4 of the user guide* describes installation of the RCD software, including the Unify Scanner Service.
2. The RCD UI is served via https://openapi.natwest.com:443 and interfaces with the scanner via the Unify Scanner Service running on *https://localhost:7001*.
3. Open *Services* and verify the *Unify Scanner Service* is running
4. Open a command prompt, run netstat -an and ensure that *127.0.0.1:7001* has a state of *LISTENING*.
5. If the RCD UI can't connect to *https://localhost:7001* then the user is prompted to download and install the *Unify Scanner Service*. If the user is prompted to do so repeatedly, it's maybe that the browser or Windows Defender Firewall is blocking access to localhost 7001, and this will need remediated.
6. Immediately following installation of the Unify Scanner Service, if the RCD User Interface fails to detect the service is running, close the browser and retry. This is a known issue with specific browser versions.
7. If the RCD User Interface fails to detect the Unify Scanner Service is running, verify connectivity to the Unify Scanner Service in the browser using:

   https://localhost:7001/api/system/ping

   The expected response is {} and there should be no security warning or prompts regarding the self signed certificate.



   If there are warnings, open the Windows Certificate Manager and verify that the USS installer has created a certificate under Trusted Root Certification Authority -> Certificates issued to localhost and with a Friendly Name of UnifyScannerServices.

   Open and view Developer Tools in the browser and the Console log, recreate the issue and review the browser console log for errors. The error ERR_CERT_AUTHORITY_INVALID is indicative of this issue, which must be resolved before RCD can be used.

8. The following instructions will allow a web server to be temporarily stood up on http://localhost:8080, to verify basic connection to local ports in the web browser. This may help, for example, diagnose configuration of the Windows firewall. NB – The Unify Scanner Service uses only https (see next).

   In PowerShell:

   ```
   $Listener=[System.Net.HttpListener]::new()
   $Listener.Prefixes.Add("http://localhost:8080/")
   $Listener.Start()
   $Context=$Listener.GetContext()
   ```

   This will then wait for a client to connect to port 8080. If it doesn't wait, repeat until it does. In the browser navigate to HYPERLINK "http://localhost:8080/"http://localhost:8080. This will cause PowerShell to end its wait and return to the PowerShell prompt, and the browser will now wait for a HTTP response.

   In PowerShell:

   ```
   $Content=[System.Text.Encoding]::UTF8.GetBytes("<html><body>Hello World</body></html>")
   $Context.Response.ContentType="text/html"
   $Context.Response.ContentEncoding=[System.Text.Encoding]::UTF8
   $Context.Response.ContentLength64=$Content.Length
   $Context.Response.KeepAlive=$false
   $Context.Response.StatusCode=200
   $Context.Response.StatusDescription="OK"
   $Context.Response.OutputStream.Write($Content, 0, $Content.Length)
   $Context.Response.OutputStream.Close()
   $Context.Response.Close()
   $Listener.Stop()
   ```

   This should cause "Hello World" to be displayed in the browser.

9. The following instructions will allow a web server to be temporarily stood up on https://localhost:8443, to verify secure connection to local ports in the web browser. This may help, for example, diagnose configuration of the Windows firewall, browser settings, and certificate handling.

   a) Open add/remove programs and uninstall the Unify Scanner Service if installed.

   b) Create a new self signed certificate

   In powershell as administrator:

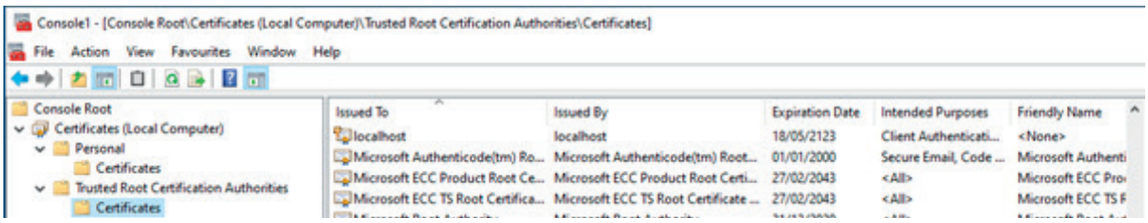
   ```
   New-SelfSignedCertificate -DnsName "localhost" -CertStoreLocation "cert:\LocalMachine\My" -NotAfter (Get-Date).AddYears(100)
   ```

   c) Add the certificate to Trusted Root Certification Authority

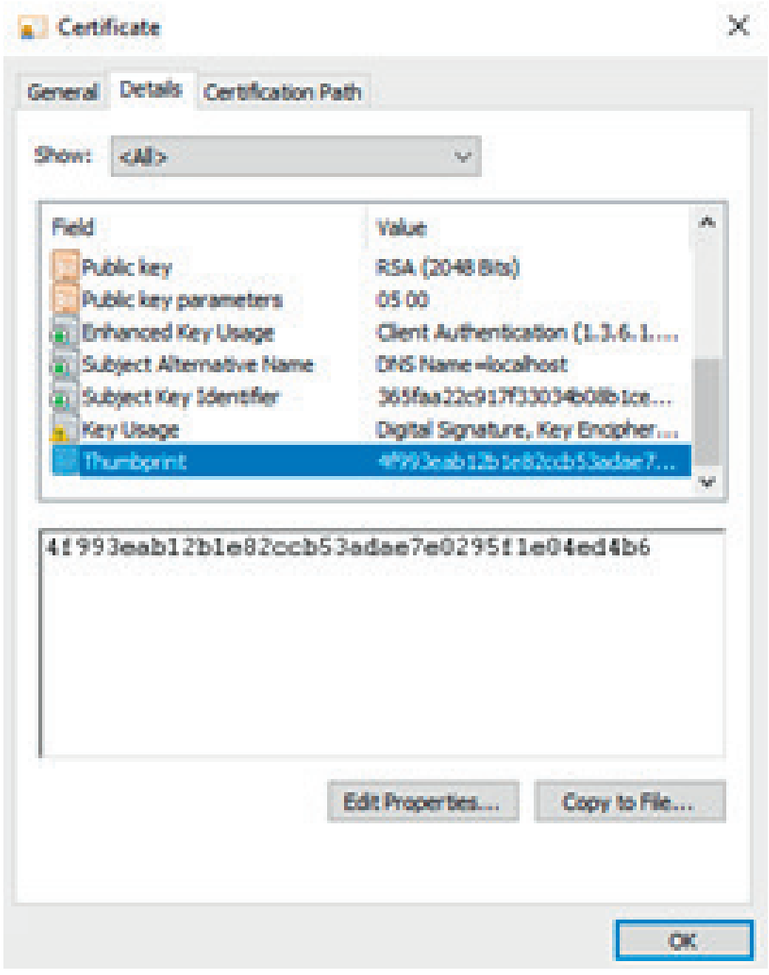
   Open Microsoft Management Console (MMC) as administrator

   File -> Add/Remove Snap-in…
   Select Certificates and Add >
   Select "This snap-in will always manage certificates for:" "Computer account"
   Click Next, Finish, OK
   Expand Certificates (Local Computer) -> Personal -> Certificates

Right click the “localhost” certificate and Copy
Expand Trusted Root Certification Authorities, right click on Certificates and click Paste.



Open the Certificate, click the Details tab and locate the Thumbprint



Highlight and copy the thumbprint

d) Create SSL Binding for port 8443

In powershell as administrator run the following, substituting the certhash with the above thumbprint. Using the above example:

netsh http add sslcert ipport=0.0.0.0:8443 certhash=4f993eab12b1e82ccb53adae7e0295f1e04ed4b6 “appid={00112233-4455-6677-8899-AABBCCDDEEFF}”

e) Create listener

In powershell as administrator:

$Listener=[System.Net.HttpListener]::new()
$Listener.Prefixes.Add(https://localhost:8443/)
$Listener.Start()

f) Wait for a connection

In powershell as administrator:

$Context=$Listener.GetContext()

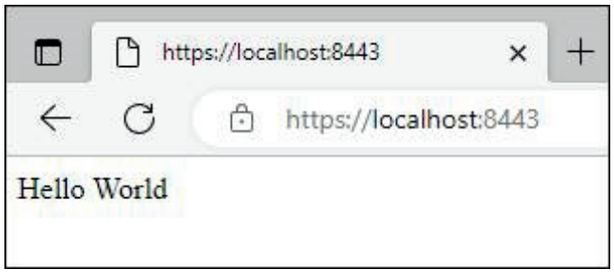
This will then wait for a client to connect to port 8443. If it doesn't wait, repeat until it does. In the browser navigate to HYPERLINK "https://localhost:8443/"https://localhost:8443. This will cause PowerShell to end its wait and return to the PowerShell prompt, and the browser will now wait for a HTTP response.

g) Provide the response

In powershell as administrator:

```
$Content=[System.Text.Encoding]::UTF8.GetBytes("<html><body>Hello World</body></html>")
$Context.Response.ContentType="text/html"
$Context.Response.ContentEncoding=[System.Text.Encoding]::UTF8
$Context.Response.ContentLength64=$Content.Length
$Context.Response.KeepAlive=$false
$Context.Response.StatusCode=200
$Context.Response.StatusDescription="OK"
$Context.Response.OutputStream.Write($Content, 0, $Content.Length)
$Context.Response.OutputStream.Close()
$Context.Response.Close()
```

h) Review the browser



Note the padlock symbol and there are no warnings about the certificate.

i) Clean up

In powershell as administrator:

```
$Listener.Stop()
netsh http delete sslcert ipport=0.0.0.0:8443
```

In MMC, Certificates (Local Computer):

Right click the "localhost" certificate under "Trusted Root Certification Authorities" and Delete
Right click the "localhost" certificate under "Personal" and Delete

6.3. Scanner drivers.

1. The Digital Check CX30/TS240 drivers are delivered via RCD and should not be installed separately. *Section 2.4 of the user guide* describes installation of the RCD software, including scanner drivers.
2. The scanner driver download is handled by the *Unify Scanner Service*, which runs as a Windows service using the context of the current logged-in user to download the driver packages. Both the web browser and the *Unify Scanner Service* require access to *https://openapi.natwest.com:443*. The RCD UI, served via *https://openapi.natwest.com:443*, interfaces with the scanner via the Unify Scanner Service running on *https://localhost:7001*.
3. In IT environments where a proxy service is required, this must be configured in *Windows via Settings -> Network & Internet -> Proxy,* not the browser alone. Alternatively, a change to the

IT environment can enacted to allow direct access from the PC to openapi.natwest.com:443, bypassing any proxy or firewall.

4. The error message *Update Failed / Update has failed for a package* also refers to the initial driver install. Per the Further troubleshooting section below, the browser console log accompanying such an error should contain an error code such as:

   OnDownloadComplete {“packageName”:”Digital Check (TS240/CeXpressCX30)”,”type”:2,”cancelled”:false,”errorCode”:11044}

5. Error code 11044 is symptomatic of the Unify Scanner Service being unable to contact openapi.natwest.com due to a customer proxy/firewall issue; Error code 11023 that the proxy is prompting for authentication.

6. Basic connectivity can be checked in a command prompt using curl -v https://openapi.natwest.com, the output of which should include a HTTP 302 Redirect to https://www.bankofapis.com. The latter is an information page which is not used by RCD. RCD only uses a subdirectory under https://openapi.natwest.com.

7. The scanner drivers are delivered as a self-extracting zip file in the form of a Windows executable file (.exe). Basic connectivity can be checked by identifying a .exe file from a trusted and unauthenticated source, in a command prompt using curl -o test.exe *<url of a .exe file>*

8. The Windows *iexpress* tool can be used to create a test self-installing package. A batch file helloworld.bat can be included:

   ```
   @echo off
   echo Hello World
   pause
   ```

   specifying the install program as cmd /c helloworld.bat, to run maximised. The resultant .exe file can be used to test a self-installing package.

9. If the RCD scanner driver package has be downloaded and run, the installation log can be found in the *%TEMP%\ AlogentScannerController* directory

6.4. Verifying scanner connectivity outside of RCD.

1. Open *Device Manager* and expand *Universal Serial Bus controllers,* ensuring that *TellerScan* is listed and shown without any warning or error icons. Plugging and unplugging the scanner USB cable from the PC should cause *TellerScan* to disappear and reappear from the list.

2. Digital Check, the manufacturer of the CX30/TS240 scanner used by RCD, provide a tool called ScanLite, a stand-alone utility that allows the scanner to be tested without being connected to Remote Cheque Deposit. ScanLite can also used to activate the cleaning function on some models of Digital Check scanners. ScanLite can be downloaded directly from Digital Check using the following link: https://www.digitalcheck.com/drivers_demo/ScanLite2_v16.11_with-sensor-guide.zip

   - Reboot the PC and log in without starting any scanning related applications/activity
   - The contents of the zip file should be extracted and scanlite2.exe run stand-alone, no installer is required.
   - If prompted to “Try Initializing scanner with local firmware”, select “No”
   - The error “BUICInit => -125. Is the scanner on and connected?” will be shown if the PC cannot connect to the scanner. Click OK.
   - A menu page will appear if the scanner connects. Click Exit.

- Please note: other versions of the Digital Check USB scanner drivers are available on their website. Please only use the drivers that are delivered via Remote Cheque Deposit.

6.5. Scanner connection issues in RCD.

1. A *Connecting…* timeout or the following error message indicates that RCD is unable to connect to the scanner: *Could not connect to the scanner. This could be because of hardware failure or if the scanner cable was disconnected from the USB port or if the scanner was powered off.*
2. Follow the troubleshooting steps in the user guide and the Advanced Troubleshooting steps above.
3. Open *Add or Remove Programs* and ensure the *Unify Scanner Service* and *TellerScan Combined Driver* are listed as installed.
4. Ensure the additional TellerScan Deployment Files are located within the installation directory of the Unify Scanner Service by checking for the existence of *dccimage.dll* within the installation directory, the default being *C:\Program Files (x86)\Unify\ Scanner Services*
5. Open *Services* and ensure the *Unify Scanner Service* is listed with a status of *Running.*
6. Open *Event Viewer* and review any warning or error messages under *Windows Logs,* which may assist further troubleshooting.
7. Follow the reinstallation steps described below.

6.6. Reinstallation.

1. Disconnect the USB cable for the CX30/TS240 scanner from the PC, and power the scanner off.
2. Clear the browser cache.
3. Open *Add or Remove Programs* and uninstall the *Unify Scanner Service* and *TellerScan Combined Driver.*
4. Remove the *C:\Program Files (x86)\Unify\Scanner Services* directory.
5. Reboot the PC, ensuring that the boot-up and login processes have fully completed before launching Bankline.
6. Open RCD and follow *section 2.4 of the user guide* closely. Ensure the port number (7001) and certificate options are as specified.

6.7. Further troubleshooting.

1. Open the browser console (More Tools -> Developer Console), selecting the “Console Tab” and ensuring the Console Preferences enable *Show timestamps*.
2. Recreate the issue. Note the date/time of the error; the bankline username; the Windows Computer Name (*System Information -> System Summary -> System Name*); take a screenshot showing the error, and save the console log (right click then choose *Save As*).
3. The information gathered can be shared with us securely using Egress (*https://reader.natwest.com*).
4. Please think about how screen share can be affected, so our engineers can provide remote assistance. Please also consider the download and use of Microsoft SysInternals DebugView (*https://learn.microsoft.com/en-us/sysinternals/downloads/debugview*) to allow further logs to be captured.

P615404 July 2023