dlx

deluxe.
trusted business technology

Remote Deposit Capture
Installation Guide
v4.1

PROPRIETARY STATEMENT

This document contains confidential and proprietary information, which are trade secrets of Deluxe Corporation, and are thereby protected by applicable state and federal law, including the Economic Espionage Act of 1996. No part of this document may be copied, disclosed or distributed, except to employees of the recipient with a job related need to review this document. By accepting this document, the recipient agrees to take all reasonable steps to ensure that this confidential and proprietary information will not be disclosed to any third parties, in whole or in part, without the prior written permission of Deluxe Corporation. See sections 1832, 1834, and 1839 of chapter 90 of the Economic Espionage Act of 1996.

Table of Contents

Items needed to access Remote Deposit Capture:

>   » **Remote Deposit Capture URL**–Links to site login page.

>   » **Username**–Identifies user as authorized user for company.

>   ▪ Identifies the Locations and Accounts user may access.

>   » **Temporary Password**–Confirms identity of user as authorized for company.

>   ▪ Identifies the Locations and Accounts user may access.

>   » **Access Code**–Directs user to company specific application.

>   ▪ Location and Account access is limited by Username access rights.

>   ▪ Access Code may be included within your customized URL.

>   » If applicable, **Computer Activation Code**–Confirms computer is authorized to access to Remote Deposit Capture site.

NOTE: The installation process will need to be completed by an individual with computer access to write to the registry. The following is one way to check the access level.

1. Right click on Computer.

2. Click Manage.

3. If you are prompted to enter credentials, you do not have the administrative access required.

Minimum Client PC Requirements

If any of the following requirements are not met for the client PC, stop the installation process. Either establish the PC with the required components or load the remote capture application on a different PC that meets the requirements listed below.

- » Operating System: Windows 8.1 (64-bit), Windows 10 (64-bit) version 1709 or higher.

- » RAM (Memory): Minimum Requirement: 4 GB RAM

- » Processor: Dual Core 2.4 GHz or better * Intel Pentium 3 or compatible (minimum required)

- » Primary Hard Drive: 5GB available hard drive space

- » Scanner Connections/Ports: One available USB 2.0 port

- » Screen Resolution: Screen Resolution of 1024 x 768 or higher with 1MB Video RAM or better

- » Software Dependencies: The following software components are necessary for the application to operate correctly and should be loaded or installed prior to the remote capture installation process.

  - ▪ Internet Explorer: Internet Explorer 11.0 (32 bit)

    - o The system will not function properly in any browser other than Internet Explorer.

  - ▪ .NET Framework: Microsoft .NET Framework 3.5.1 (Minimum required).

    - o 4.5 is optionally supported but not used by the application (3.5 still required)

  - ▪ Adobe (Acrobat) Reader: Adobe Reader 5.0 or higher, up to v11 When using Windows 8.1, download the current version of Adobe Reader. Do not use the Windows 8.1 Adobe Reader App (tile).

    NOTE: Reports are delivered as HTML and Adobe PDF. Some are provided in PDF only (QuickBooks® Reports, Research Reports and Training documents).

- » Windows Login Rights: The following Windows rights are required to access the relevant functions for remote capture.

  - ▪ Administrator Rights: Users will require local administrator access to the workstation to install the security policy, activate computer, and perform first-time capture.

- » WinZip Utility: WinZip 9.0 or higher installed. (Only required if using Image Export feature.)

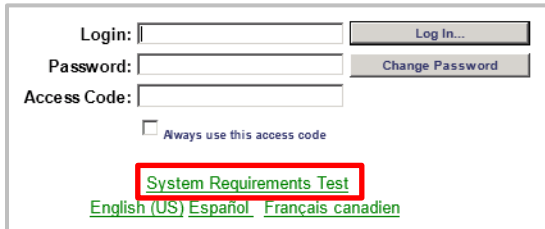- » Proxy Settings: Secure connectivity to the Deposit 24/7 server.

If any requirements are not met for the Client PC, stop the installation process. Either establish the PC with the required components or load the remote capture application on a different PC that meets the requirements.

- » QuickBooks®: Online Edition (QBOE) only

- » Silverlight: Required for Electronic Payments (Minimum version 4.0.60531.0)

- » Simplex Scanning: Requires Twain 1.9 compatible or newer device.

Systems Requirements Test

The Systems Requirements Test can confirm your system meets the minimum requirements and direct you to any possible changes needed.

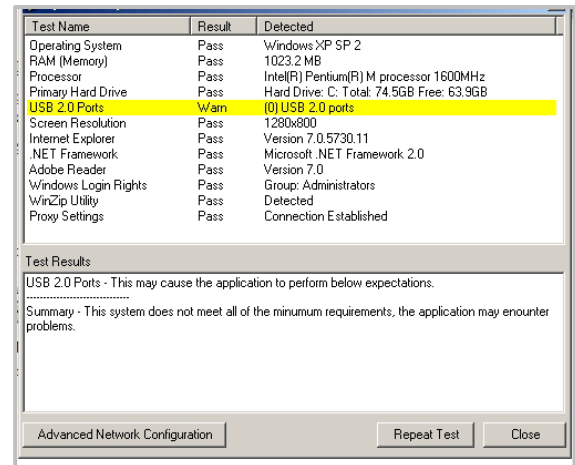1. Click System Requirements Test link.

2. Click Run.

A series of tests are run on the workstation and a detailed list of results is displayed. In addition, a log displays, and a screen shot can be sent to the central site to ensure the PC meets necessary requirements.

The results display the following information:

» Test Name: Identifies the configuration test performed

» Result: Displays status of the completed test:

  ▪ Pass–configuration meets minimum standards.

  ▪ Warn–configuration is below minimum standards and Deposit 24/7™ may not perform optimally.

  ▪ Fail–Configuration will not support Deposit 24/7™, system should be upgraded before continuing with the installation.

» Detected Hardware or Software configuration detected by the test.

» Test Results Display detailed test results.

If there are any Fail notices, update or install the needed software or hardware components per the system requirements.

3. Click Close.

Install Prerequisites

ESTABLISH A TRUST TO THE WEB SERVER

1. Open a new Internet Explorer window.

2. Select Tools.

3. Select Internet Options.

4. In the Internet Options window, select the Security tab.

deluxe.
trusted business technology

5. Highlight Trusted Sites from the web content zones at the top.

6. Click Sites.

7. Enter the URL of the Remote Capture Web Server to which the client PC will connect.

8. The application uses HTTPS (server verification). Ensure the checkbox to require server verification is checked.

9. Click Add. The URL lists at the bottom of the screen as a trusted site.

SET CUSTOM SECURITY LEVELS

1. While still in the Internet Options Security screen, with Trusted Sites still highlighted, click Custom Level for the Security Level at the bottom of the screen.

2. Confirm the following:

   » .NET Framework-reliant Components:
     - Run components not signed with Authenticode–ENABLE

   » ActiveX Controls and Plug-ins:
     - Display video and animation on a web page that does not use an external media player-ENABLE.
     - Run ActiveX controls and plug-ins–ENABLE
     - Script ActiveX controls marked safe for scripting–ENABLE

   » Enable .NET framework setup-ENABLE

   » Miscellaneous
     - Use SmartScreen filter–DISABLE

3. Click OK to save changes.

4. Select the Advanced tab.

   » Security
     - Do Not Save Encrypted Pages to Disk–DISABLE
       o If this option is enabled (checked) it can cause several problems on the system, including not running .NET controls and viewing PDFs could be affected.
     - Enable Integrated Windows Authentication–DISABLE
     - Enable SmartScreen Filter–DISABLE
     - Use SSL 2.0–DISABLE
     - Use SSL 3.0–DISABLE
     - Use TLS 1.0–ENABLE
     - Use TLS 1.1–ENABLE
     - Use TLS 1.2–ENABLE

   » When the Deposit 24/7 server environment is exclusively TLS 1.2, client workstations must have current Microsoft .NET 3.5 patches installed.

     NOTE: Hosted customers will require TLS 1.2 as of May 13, 2018.

5. Select the General tab.
   » Under Browsing History, click Settings:
      ▪ 'Every time I visit this webpage.'–ENABLE
6. Click OK.
7. Click OK to close the Internet Options window.

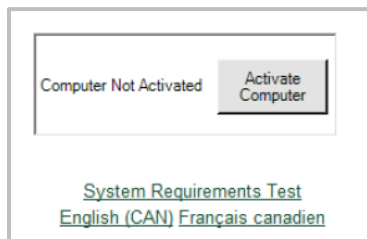# ACTIVATE MULTI-FACTOR AUTHENTICATION

These steps will be needed if you have been given a Computer Activation Code.

1. Select Help with Security Setup.

2. Click Download.

   Follow the screen prompts to complete download. After download is complete:

3. Click Close Internet Explorer.

4. Select Run as Administrator and open Internet Explorer.

5. Return to main login page.

6. Click Activate Computer.

7. Enter/paste the 20-character computer activation code (supplied by the central site).

8. Click Submit.

9. Upon successful activation, click Close.

LOG IN TO THE CLIENT APPLICATION

1. Enter Login.

2. Enter Password.

3. If applicable, enter Access Code.

4. Enter new Password.

5. Enter new Password to confirm.

6. Click Log In.

Setup within Application

INSTALL SCANNER DRIVER

These install steps are not completed if using Simplex Scanning (flat bed or 4 in 1 scanners).

Ensure that all pre-requisites have been completed before installing scanner drivers.

1. Ensure scanner is NOT connected to PC.

2. From the main menu, click Installation.

3. Select the scanner to be used for capture.

4. Click Install.

5. Follow applicable computer prompts.

    Some scanners do not display any prompts during install.

6. Once the scanner driver install is complete, close Internet Explorer to apply the scanner driver.

7. Connect scanner to PC and turn on scanner.

8. If you have any issues, verify drivers successfully installed.

    a. Right-click on My Computer | Manage.

    b. Highlight Device Manager.

    c. Expand Universal Serial Bus Controllers.

    d. Verify scanner lists as USB device.

If using Simplex Scanning, do not select a scanner from the installation menu.

    a. Run the Install from the CD provided with the flat bed or 4 in 1 scanner.

    b. Follow the onscreen instructions.

EDIT ACCESS RIGHTS

Assign user rights to specific locations and accounts.

1. From the main menu, click Configuration.

2. Select the Users tab.

3. Select a user to edit.

4. Select the Remote Capture task level.

    The location or account access may be set at any or all levels.

5. Click Edit Access Rights.

6. Select each location and account that this user may access.

7. Click OK.

8. Review the Access Rights for the user to ensure the correct properties are assigned.

    The user may now access the client application according to the assigned rights.

## DOWNLOAD CAS SECURITY POLICY (.NET SECURITY POLICY)

If this installation will not be capturing deposits, the CAS Security Policy will need to be installed.

1. From the main menu, click Installation.

2. Under Scanner Setup, select CAS Security Policy.

3. Click Install.

4. Click Run.

5. When the install shield closes, Close Internet Explorer to apply the changes.

6. Reopen Internet Explorer to RDC application URL.

    When using Win 8.1, only use the Internet Explorer icon within the desktop to open the internet. Do not use the Win 8.1 Internet Explorer App (tile) to install or access Deposit 24/7.

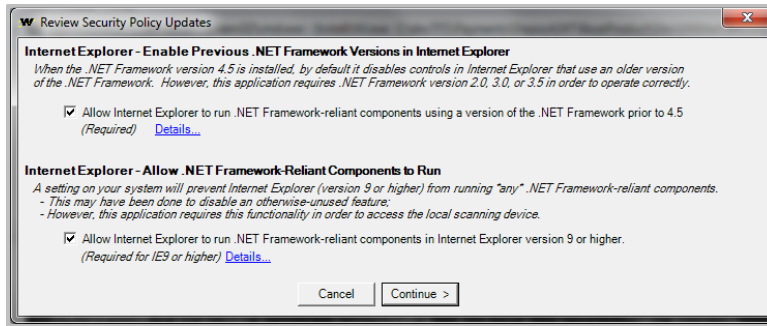## .NET 4.5 SECURITY POLICY UPDATES

1. If .NET 4.5 has been installed, click Continue to Enable Previous .NET Framework Version in Internet Explorer.
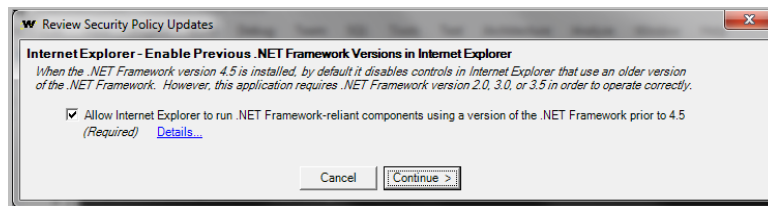

2. If ActiveX Killbits set for Null GUID, click Continue to Allow .NET Framework-Reliant Components to Run.
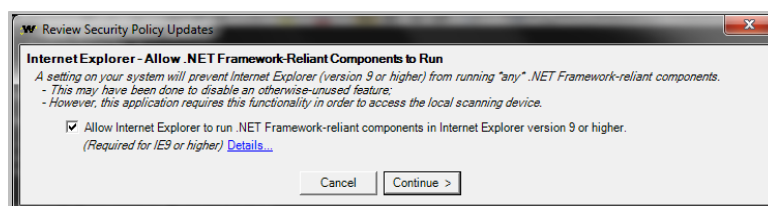
(If both issues are present on a system, the installer will prompt for permission to update both.)

3. In Interactive Mode, the installer prompts to review all settings changes. The user can select between "Trusted Sites" or "Local Intranet" when making the CAS Policy Updates. Click Continue to accept.
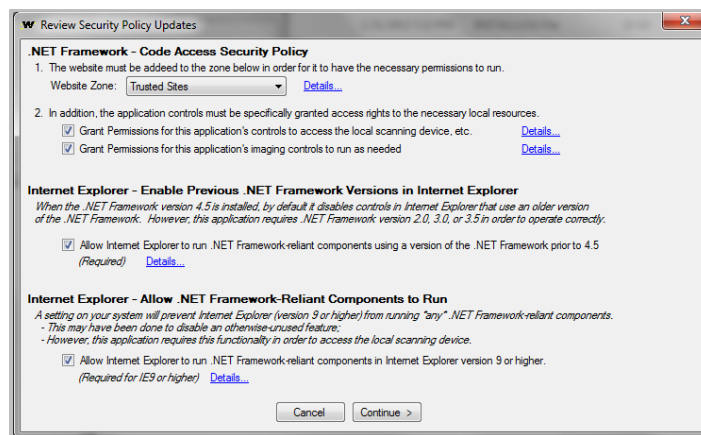
Client Application Installation Checklist

» Gather setup information

- Remote capture application URL/ access code.

- Administrator login and password.

- Password and Login rules.

- Computer activation code (for multifactor authentication).

» Access client application with supplied URL.

» Review Minimum Client PC Requirements are met.

» Complete Install Prerequisites

- Establish a Trust to the Web Server

- Set Custom Security Levels

- Download .NET Security Policy (if Scanner Driver is not installed).

» Access client application with supplied URL.

- Log in to client application with Administrative login information.

- Activate Computer (if using multifactor authentication).

    o Enter Activation Code (if requested) generated during license generation.

» Edit Access Rights.

» Install Scanner Driver.

» Close Internet Explorer to save configurations.

» Open Internet Explorer and log in to remote capture application with administrative login.

» Verify that all modules can be successfully opened.

» Capture test items and Transmit to verify functionality.

- First transaction must be captured by a Windows administrative user.