

Remote Deposit Capture

RDM



Hardware Installation Manual



Contents

Introduction	l
Installation Guidelines for Scanners	2
System Requirements	2
Additional Requirements	2
Required User Privileges and Securities for Installation	3
Scanner Information	1
Items Included with the Scanner	1
Setting up a Scanner for Installation	1
Recommended Configuration for Internet Explorer	5
Compatibility Mode (IE 8 Only)14	4
Remote Deposit Capture Scanners1	5
Installing the RDM Series Scanner for Remote Deposit1	5
Verifying the Installation16	5



Introduction

The *Hardware Installation Manual* provides step-by-step instructions for the installation of all supported scanners. This manual, in conjunction with the Operator Manual included with the scanner, should provide all the instructions necessary for a successful installation.

The Hardware Installation Manual includes:

- Microsoft[®] Internet Explorer[®] configuration common to the installation of all scanners.
- Installation instructions specific to each type of scanner.
- Un-install instructions specific to each type of scanner.

NOTE: Scanner installations are documented using Microsoft[®] Windows[®] 7 Enterprise 32-bit operating system and Internet Explorer 8 unless otherwise noted. Some steps and wording may vary slightly if you have a different operating system.

For any additional questions or concerns not addressed by this document, please contact your first route of Customer Support for assistance.



Installation Guidelines for Scanners System Requirements

In addition to a high-speed Internet connection, the following components are required for working with the EPS application(s).

For Microsoft Windows[®]:

- Windows Vista (except Starter or Home Basic): IE 8 and 9 or Google Chrome
- Windows 7: IE 8, 9, 10, and 11 or Google Chrome
- Windows 8: IE 10 or Google Chrome
- Windows 8.1, update 1: IE 11 or Google Chrome
- Windows 10 Pro
- Windows 10 Enterprise
- .NET Framework 4.0 or higher

The Current version of Chrome and its two previous versions are supported.

Additional Requirements

The table below lists general requirements for a successful scanner installation.

Requirement Type	
RAM	2 Gigabytes or greater.
Updates	All current critical Windows updates.
Processor	2.4 GigaHertz (GHz) or greater.
Hard Drive space	1.5 Gigabytes or greater.
USB Port	Direct USB 2.0 port (hubs, powered or not, are not supported).
USB Cable	A USB 2.0 Hi-speed cable (included with scanner).
Power Cable	Power cable (included with scanner).
Browser	Internet Explorer is the only supported browser.
.NET	.NET 4.0 Framework for Windows 7
Internet Connection	High-speed Internet connection.
UPS	Uninterruptible Power Supply (UPS) is recommended.

NOTE: Not all scanners have been certified for Windows 7 or 64-bit compatibility; verify compatibility before attempting installation.

Required User Privileges and Securities for Installation

Prior to installation, it may be necessary to temporarily disable anti-virus, firewall, or other Internet security software. Users that will be installing scanner drivers must have Administrative rights to that PC.

NOTE: Some PC security settings may change during installation.

In Microsoft Windows Vista and Windows 7, a PC may be running User Account Control (UAC). If a PC has UAC enabled, the system may prompt for additional steps during the installation process. Additionally, if a PC currently has UAC enabled, the user may have to run Internet Explorer as an Administrator to successfully install the software.

NOTE: Users should only have one type of scanner installed at a time.



Scanner Information

Items Included with the Scanner

Selected scanners include replacement parts and extra extenders. Store these and the box in a safe place. The box and packaging should be kept for warranty purposes. Always keep the Operator's Manual for reference. For the Unisys[®] SmartSource[®] Micro Series scanner, you will need to retain the calibration sheets for installation and to re-calibrate the scanner when needed.

Setting up a Scanner for Installation

- 1. Remove the scanner and its components from the box and inspect the contents to ensure no items are missing.
- 2. Place the scanner on a flat surface within 1¹/₂ to 6 feet of a PC, preferably not in close proximity to monitors, speakers, or other electronic devices.
 - The scanner should be at least 1½ feet away from other electronic devices but close enough to an electrical outlet.
 - The scanner should not be in direct sunlight.
 - The scanner should be in a place that is convenient to place documents into it with ease.
- 3. Connect the power cable to the scanner and wall outlet.
- 4. Connect the USB cord to the back of the PC. At this time, do not connect the other end of the USB cord to the scanner, but instead place it near the back of the scanner.
- **5.** If you are installing the SmartSource Micro Series scanner, retain the calibration sheets for installation and as-needed re-calibration.
 - a. (Optional) For the RDM, Epson CaptureOne, and Digital Check CX30 scanners, open the small box of the franking ink roller and follow the installation instructions.
 - b. (Optional) For the VisionX, TellerScan series, and SmartSource Professional series scanners, open the small box of the ink cartridge and follow the installation instructions if the ink cartridge is for the endorser.



Recommended Configuration for Internet Explorer

1. Open Internet Explorer, and from the top navigational menu, select **Tools** | Internet **Options**.

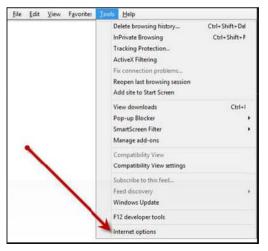


FIGURE 1 - INTERNET OPTIONS

2. The Internet Options window appears. From the tabs at the top of the window, select General.

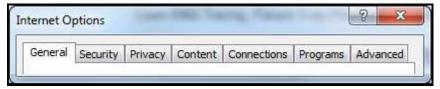


FIGURE 2 - GENERAL TAB UNDER INTERNET OPTIONS

3. Under the section **Browsing history**, select the **Settings** option.

Bar	nk	Ín	ar	1CÎ	al
					and the second se

eneral	Security	Privacy	Content	Connections	Programs	Advanced
Home p		1801100	12.858730-1	n 35 50	ant contain	
	Tode	ate home	page tabs,	type each add	dress on its o	own line.
	https	s://j atod	lay.jackher	nry.com/		~
						*
		Use cu	Irrent	Use default	Use	blank
-		C. C. C. C.				14-11-2
Browsi	ng history		1959A 112462			
1	Delata	temporar	v files, hist	tory, cookies, s	aved passw	ords,
			formation.		~	
*+	and we	eb form in		on exit	×	
* +	and we	eb form in	formation.	and a second	N Set	tings
- Coard	and we	eb form in	formation.	on exit Delete	Set	tings
Search	and we	eb form in ete brows	formation. sing history	and a second		
Search	and we	eb form in	formation. sing history	and a second		tings
S	and we	eb form in ete brows	formation. sing history	and a second		
Search	Chang	eb form in lete brows e search i	formation. sing history defaults,	Delete	Set	tings
S	Chang	eb form in lete brows e search i	formation. sing history defaults,	and a second	Set	
S	Chang	eb form in lete brows e search i	formation. sing history defaults,	Delete	Set	tings
S	Chang Chang tabs.	eb form in lete brows e search i	formation. sing history defaults,	Delete	Set	tings
Tabs -	and we Del Chang Chang Chang tabs. rance	eb form in ete brows e search (e how we	formation. sing history defaults. bpages are	Delete	Set	tings
Tabs -	Chang Chang tabs.	eb form in ete brows e search (e how we	formation. sing history defaults,	Delete	Set	tings

FIGURE 3 - SETTINGS OPTION

4. The Temporary Internet Files and History Settings window appears. Under the Check for newer versions of stored pages section, select the check box next to Every time I visit the webpage. Select OK at the bottom to continue.

Femporary Internet Files	
Internet Explorer stores copies of webpag for faster viewing later.	es, images, and media
Check for newer versions of stored pages:	
Every time I visit the webpage	
Every time I start Internet Explorer	
Automatically	
O Never	
Disk space to use (8-1024MB) (Recommended: 50-250MB)	50 🚖
· · · ·	
Current location:	
Current location: C: \Users \cjimenet \AppData \Local \Microsofi	t\Windows\Temporary
Current location: C: \Users \cjimenet \AppData \Local \Microsofi	t\Windows\Temporary
Current location: C: \Users \cjimene \AppData \Local \Microsof Internet Files \	
Current location: C: \Users\cjimene \AppData\Local\Microsofi Internet Files\ Move folder	
Current location: C: \Users \cjimene \AppData \Local \Microsof Internet Files \	View files
Current location: C: Users \cjimene. \AppData \Local \Microsofi Internet Files \ Move folder \ View objects listory Specify how many days Internet Explorer	View files

FIGURE 4 - SETTINGS FOR NEWER VERSIONS OF STORED PAGES

5. From the tabs at the top of the Internet Options window, select Security.



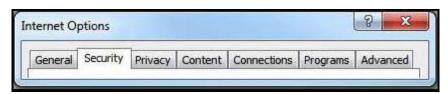


FIGURE 5 - SECURITY TAB UNDER INTERNET OPTIONS

6. Select the Trusted Sites icon to activate the Sites option. Select Sites.

ieneral	Security	Privacy C	ontent C	onnector	s Pro	grams	Advance
Select a	zone to v	view or chang	e security	settings.			
(~	1	0		
Int	ernet I	ocalintranet	Trusted	sites 8	Restrict	ed	
	Truste	d sites				Site	_
~	trust no your file	e contains we t to damage y s. e websites in	your comp	uter or		Sile	
Secur	ity level fo	or this zone					
	0	tom uston setting To change the To use the re-	e settings, commende	d setting:	s, dick D	efault le	
	Enable Pi	otected Mode		i restaron	-	et Explo	
			R	eset all zo	nes to (default l	evel
-			and by use	ur system	adminic	halar	

FIGURE 6 - SITES OPTION UNDER TRUSTED SITES CATEGORY

7. The **Trusted sites** window appears. In the **Add this website to the zone** field, enter the URL: <u>https://ssl.selectpayment.com.</u> and select the **Add** option.



You can add and remove webs this zone will use the zone's se	
Add this website to the zone:	
https://selectpayment.com	Add
Websites:	
	Remove
	+
Require server verification (https:)	for all sites in this zone

FIGURE 7 - ADDING A TRUSTED SITE

- 8. Select Close at the bottom of the Trusted sites window.
- 9. From the Internet Options window with the Trusted sites icon selected, select Custom level.



FIGURE 8 - CUSTOM LEVEL OPTION UNDER TRUSTED SITES

- 10. A list of security settings appears. Select the settings detailed below.
 - a. Under the heading ActiveX controls and plugins, the following three options should all be set to Disable:
 - i. Display video and animation on a webpage that does not use external media player.
 - ii. Download unsigned ActiveX controls.



- iii. Initialize and script ActiveX controls not marked safe for scripting.
- b. The rest of the options under this heading should be set to **Prompt** (the preferred setting) or **Enabled**.

ActiveX controls and plug-ins Allow previously unused ActiveX controls to run without prov Disable Disable Disable Prompt Automatic prompting for ActiveX controls Disable Di	etting	
Takes effect after you restart Internet Explorer		 Disable Enable Ilow Scriptets Disable Enable Prompt Automatic prompting for ActiveX controls Disable Enable Binary and script behaviors Administrator approved Disable
	1	
	Take	es effect after you restart Internet Explorer
set custom settings		
set to: Medium (default)	set	to: Medium (default)

FIGURE 9 - ACTIVEX CONTROLS AND PLUGINS SETTINGS

c. Under the **Scripting** heading, set **Active scripting** and **Scripting of Java applets** to **Enable**.

ettings		
	Prompt	
So So	ripting	
\$	Active scripting	
	O Disable	
	Enable	
	O Prompt	
2	Allow Programmatic clipboard acc	ess
	O Disable	
	Enable	
100	O Prompt	
2		pt
	 Disable Enable 	
	Allow websites to prompt for info	mation using existed wind
(===		imation using scripted what
S		
2	Disable	
<u>چ</u>	🔘 Disable	•
100 Au	 Disable Enable 	xplorer
*Takes	Disable Enable III Effect after you restart Internet E	xplorer
*Takes	Disable Enable III Effect after you restart Internet E stom settings	
*Takes	Disable Enable III Effect after you restart Internet E stom settings	xplorer
*Takes	Disable Enable III Effect after you restart Internet E stom settings	
*Takes	Disable Enable III Effect after you restart Internet E stom settings	

FIGURE 10 - SCRIPTING SETTINGS



- **11.** Select **OK** at the bottom of the window.
- 12. From the Internet Options window, select the Privacy tab.



FIGURE 11 - PRIVACY TAB

- **13.** Under the **Pop-up Blocker** section, if the **Turn on Pop-up Blocker** option is checked, continue with this step. If it is unchecked, proceed to the next step.
 - a. Select the **Settings** option.

General	Security	Privacy	Content	Connections	Programs	Advanced
Setting	s —					
9	Select	a setting	for the Inte	ernet zone.		
- F	Med	ium				
	priv - Blo - Re can Sites	acy policy ocks third- used to co estricts fir be used to Im Im	party cook intact you st-party co	ies that do not ies that save ii without your e okies that save you without yo Advanced	nformation t xplicit conse e informatior ur implicit co	hat can ht i that
9			up Blocker		7	
InPriva		n on Pop-	up biocker			
	¥ -	able toolb		use by InPrivat tensions when	0-200000	owsing
6) 5	ome <u>settin</u>	igs are ma	inaged by	your system ac	ministrator,	

FIGURE 12 - SETTINGS OPTION FOR POP-UP BLOCKER

b. In the **Address of website to allow** field, enter the URL: <u>https://ssl.selectpayment.com.</u> and select **Add**.

xceptions	
Pop-ups are currently blocked. You can allow websites by adding the site to the list below.	v pop-ups from specific
Address of website to allow: ssl.selectpayment.com	Add
Allowed sites: iha.csod.com	Remove
ssl.selectpayment.com	1 JOHIOVE
un en	Remove all
lotifications and blocking level: ☑ Play a sound when a pop-up is blocked.	
Show Information Bar when a pop-up is blocked.	
Blocking level:	
Medium: Block most automatic pop-ups	

FIGURE 13 - ADDING AN ALLOWED WEBSITE UNDER POP-UP BLOCKER SETTINGS

c. Select Close to return to the Internet Options window.

14. From the Internet Options window, select the Advanced tab.

General				Connections	-	
---------	--	--	--	-------------	---	--

FIGURE 14 - ADVANCED TAB UNDER INTERNET OPTIONS

15. Scroll through the settings to the **Security** section and make sure the check box next to **Do not save encrypted pages to disk** is *not checked*.

BankFinancial*

General	Security	Privacy	Content	Connections	Programs	Advance
Setting	s —	1	· · ·		harrisean an	
	Allow Allow Ched Ched Ched Ched Do no Empty Enabl Enabl Enabl Enabl	active con software to for publis for serve for signal to save end y Temporal e DOM Sto e Integrate e memory	tent to run to run or in her's certifi r certificat tures on de rypted pa ry Interne rage ed Window protection MLHTTP su	CDs to run on 1 in files on My istall even if thi ficate revocatio e revocation* ownloaded prog ges to disk t Files folder wi vs Authenticatio to help mitigat pport	Computer* e signature i on grams nen browser on*	s inv; is dc
*Tal	es effect	after you	restart Int	ernet Explorer		
		61002 (MAR)		-	advanced s	ettings
	nternet Ex	19 E. S. T.	A DESCRIPTION OF A DESC	to their default		et

Bank Financial

FIGURE 15 - SECURITY SETTING OPTION SET TO UNCHECKED

16. Also under the Security section, select the check boxes next to Use SSL 2.0 and Use SSL 3.0.

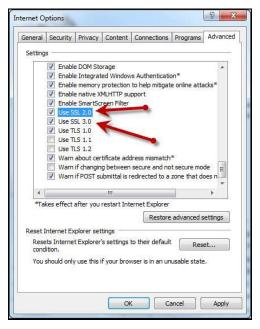


FIGURE 16 - ADDITIONAL ADVANCED SECURITY SETTINGS

17. From the bottom of the Internet Options window, select Apply.

General	Security	Privacy	Content	Connections	Programs	Advance
Setting	s					
	Enable Enable Enable Enable Use S Use S Use T Use T Use T Use T Use T Use T Warn Warn	e Integrat e memory e native X e SmartSc SL 2.0 SL 3.0 LS 1.0 LS 1.1 LS 1.2 about cer if changin	tificate add	is Authenticatic to help mitigat pport dress mismatch secure and no edirected to a	e online atta	de 冒
	Internet Ex	plorer set	tings	ernet Explorer Restore to their default	advanced Res	

FIGURE 17 - APPLYING ADVANCED SETTINGS

18. Select OK to finish.

BankFinancial"

General	Security	Privacy	Content	Connections	Programs	Advance
Setting	s					
	Enable Enable Enable Enable Enable Use S Use T Use T Use T Use T Use T Use T Warn Warn	e memory (e native XI e SmartScr SL 2.0 SL 3.0 .S 1.0 .S 1.1 .S 1.2 about cert if changing	ed Window protection MLHTTP su reen Filter tificate add	Sector Sector Sector	e online atta * •t secure mo	de 📰
*та	kes effect	after you i	restart Int	ernet Explorer	1	
			1	Restore	advanced s	settings
Rese	lition.	t Explorer'	s settings	o their default ser is in an un	Res	et

FIGURE 18 - OK OPTION TO FINISH APPLYING SETTINGS



Compatibility Mode (IE 8 Only)

There are three ways to view a website in compatibility mode with Internet Explorer 8.

• **Option 1**: Open Internet Explorer, and go to <u>https://ssl.selectpayment.com</u>. From the browser menu, select **Tools** | **Compatibility View**.

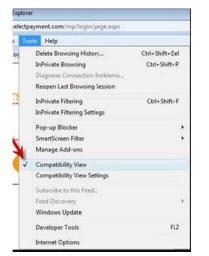


FIGURE 19 - TOOLS OPTION FOR COMPATIBILITY VIEW

• **Option 2**: Select the ripped paper icon to the right of the address bar.



FIGURE 20 - COMPATIBILITY MODE ICON

• Option 3: Navigate to <u>https://ssl.selectpayment.com</u>, and select **Tools** | **Compatibility** View Settings. In the Add this website field, enter <u>https://ssl.selectpayment.com</u>, and select Add.



FIGURE 21 - ADDING A WEBSITE TO THE COMPATIBILITY SETTINGS



Remote Deposit Capture Scanners

Installing the RDM Series Scanner for Remote Deposit

Use the following instructions to install the drivers for the RDM EC Series scanner when using it with Remote Deposit Capture.

NOTE: If ActiveX permissions are set to **Enable**, prompts may not be received that are described in this document. Certain sections will install automatically instead of providing a prompt to do so.

Do **not** plug the USB cable into the scanner until the installation is complete. Please verify that Internet Explorer has been updated to the recommended settings. See the "Recommended Configuration for Internet Explorer" section of this document for more information.

1. Log in to Remote Deposit Capture as the PC administrator or with administrative privileges.

NOTE: This process may require the IT department to disable anti-virus and/or firewall.

- 2. Log in to Remote Deposit Capture, and select the **Transactions** tab from the top of the page.
- 3. Click Remote Deposit with RDM located in the navigation links on the left.
- 4. Select Start the Installation.
- 5. The ActiveX install will begin. This may appear as an information bar at the top of the page, which states: *This Website wants to install the following add-on: (RDC_x86x64_RDM' from 'JACK HENRY & ASSOCIATES, INC.'. If you trust the website and the add-on and want to install it, click here...*
- 6. Select the information bar and click Install This Add-on for All Users on This Computer. Wait for the page to load.
- 7. An additional option will appear as a security warning pop-up, the text of which states: Do you want to install this software? Name: RDC x86x64 RDM. Select Install.
- 8. An InstallShield Wizard appears. Select Next to continue.
- 9. Ensure that all users who will be working with this computer are selected on the **Customer Information** screen. Select **Next**.
- **10.** The software installation begins. Select **OK** to a pop-up prompting for the installation of RDM drivers.
- **11.** A pop-up will appear stating: *It is now safe to apply power to the scanner and connect the scanner's communication cable to the PC.* Select **OK** to continue.
- 12. Plug in the scanner power cord and USB cord, click OK.
- 13. Select Finish.



- **14.** A pop-up appears stating that the browser session will need to be restarted. Select **OK** to continue. If Internet Explorer does not automatically restart at this time, log out of the website, and close the Internet Explorer browser.
- **15.** Open Internet Explorer, and log in to Remote Deposit Capture.
- **16.** From the top of the page, select the **Transactions** tab.
- **17.** From the left navigational bar, select **Remote Deposit with RDM**.
- **18.** The scanner will initialize and navigate to the **Open Deposits** page. The installation is complete.

NOTE: For continued accuracy and dependability, adhere closely to all maintenance and service requirements described in the materials received with the scanner.

Verifying the Installation

Use the following instructions to verify the RDM scanner installation was successful.

- 1. The RDM scanner will display in the **Device Manager** under **Universal Serial Bus Controllers** as **RDM USB Class Device**.
- 2. The Installation will display in Programs and Features in the Control Panel as Profit Stars RDC RDM ec6000i, ec7000i, ec7500i.