USER GUIDE

NCR Retail Platform Software for Windows

Releases 4.x and 5.x

B005-0000-1634
Issue H

The product described in this document is a licensed product of NCR Corporation.

NCR is a registered trademark of NCR Corporation. NCR SelfServ is a trademark of NCR Corporation in the United States and/or other countries. Other product names mentioned in this publication may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Where creation of derivative works, modifications or copies of this NCR copyrighted documentation is permitted under the terms and conditions of an agreement you have with NCR, NCR's copyright notice must be included.

It is the policy of NCR Corporation (NCR) to improve products as new technology, components, software, and firmware become available. NCR, therefore, reserves the right to change specifications without prior notice.

All features, functions, and operations described herein may not be marketed by NCR in all parts of the world. In some instances, photographs are of equipment prototypes. Therefore, before using this document, consult with your NCR representative or NCR office for information that is applicable and current.

To maintain the quality of our publications, we need your comments on the accuracy, clarity, organization, and value of this book. Please use the link below to send your comments.

EMail: FD230036@ncr.com

Preface

Audience

This book is written for software and hardware installer or service personnel, system integrators, and field engineers.

References

- *NCR Retail Systems Manager Software User's Guide* (B005–0000–1518)
- *NCR Retail Controls 3.x UPOS User's Guide for Windows* (B005–0000–1619)
- *NCR Partition Image User's Guide* (B005–0000–1641)
- *NCR PXE Image Loader User's Guide* (B005-0000-2326)
- *NCR Command Center Management Tool – Retail Site Setup Guide* (B005-0000-2331)

Table of Contents

Chapter 4: Using the RSM LE

Revision Record

Issue	Date	Remarks
A	Feb 2005	First Issue
B	Apr 2005	Various updates.
C	Dec 2006	Updates for RSM Release 2.1.2.
D	Jun 2007	Added SNMP Configuration. Various updates for RSM Release 2.2.
E	Jan 2009	Updated for release 3.0.
F	Sept 2009	Separated into chapters.
G	Nov 2012	Used the new IP book template. Various updates for RPSW Release 4.0.1 and 4.0.2. Added brightness settings information. Added Appendix A about troubleshooting SNMP. Updated the list of operating systems that RPSW supports. Updated the list of service object devices.
H	Apr 2016	Various updates for RPSW 4.x and 5.x releases. Added information on the new Image Scanner service object. Added Windows 10 in the list of supported operating systems.

Chapter 1: Retail Platform Software for Windows

Overview

Retail Platform Software for Windows (RPSW) provides a single Windows installation program to install the various NCR retail terminal software components. The RPSW installer is released on a single LPIN, eliminating the need of separate media for NCR retail terminal software components.

The following table displays the LPIN for the latest RPSW releases.

RPSW Release Version	LPIN
Release 4.x	D370–0924–0100
Release 5.x	D370–0986–0100

For information on the LPIN of the previous RPSW release versions, refer to *Previous LPIN* on page 3.

Benefits of the RPSW

The Retail Platform Software for Windows (RPSW) installer provides the following benefits:

- Single installer distribution for all Retail Platform software.
- Auto–detection of terminal type (if it is running on an NCR Gold Drive or OS Recovery Image).
- Ability to select complete or custom installation of platform software.
- Complete installation installs NCR Base Platform, NCR OPOS, NCR JavaPOS, and RSM Local Edition (LE) software. The installation requires minimal customer input, and only one reboot to install all components.
- RSM LE is installed to provide access to the OPOS Configuration and diagnostics locally.
- There is no need to know the order of installing platform software. The RPSW installation ensures that all required components are installed and configured properly.
- Custom installation provides the ability to pick and select components based on a customer configuration. The RPSW installation ensures that all the software required in support of a selected component is installed and configured properly.
- Custom installation selections include:
  - NCR Base Platform Support
  - NCR OPOS
  - NCR JavaPOS
  - NCR Retail Systems Manager LE
  - NCR Predictive Services
  - NCR FitClient (Available only for RPSW versions below 4.0)
- Ability to upgrade existing installations.
- Distribution of both `.exe` and `.msi` files to permit partners or branded applications to bundle platform software installation into their own Windows Installer applications.
- The `Retail Platform Software for Windows.msi` distribution can also be uploaded to the RSM SE servers for installation on remote terminals.

  For more information on installing RPSW, refer to *RPSW Installation* on page 7.

Configurations and Dependencies of the RPSW

This section describes the dependencies of installing the Retail Platform Software for Windows (RPSW) and the configurations you might need to perform.

Supported Operating Systems

The RPSW installer installs NCR OPOS, NCR JavaPOS, and NCR RSM Local Edition (LE) on NCR terminals that run on the following Windows operating systems:

Operating System	RPSW 4.x	RPSW 5.x
Windows 10	✓ (32–bit)	✓ (64–bit)
Windows 7	✓ (32–bit)	✓ (64–bit)
Windows POSReady 7	✓ (32–bit)	✓ (64–bit)
Windows POSReady 2009	✓	✗

Previous LPIN

The LPIN of the previous RPSW release versions are listed as follows:

RPSW Release Version	LPIN
RPSW 2.3 to 2.4	D370–0548–0100
RPSW 2.5 to 3.1	D370–0782–0100

For information on the LPIN of the latest RPSW releases, refer to *Retail Platform Software for Windows* on page 1.

Internet Explorer Security Settings

Some settings are necessary for any supported Windows operating system. Some settings are specific to Windows XP Pro SP2 or greater and Windows XPe SP2 or greater.

The RPSW installation package configures these browser settings to permit the RSM user interface to work, unless you choose not to modify the browser settings.

If you do not permit the RPSW installation to change the Internet Explorer settings, you must change them manually. To change these settings manually, select the following settings from your Internet Explorer browser:

Blocked Content

In the Internet Explorer advanced settings, permit blocked content to display through the following steps:

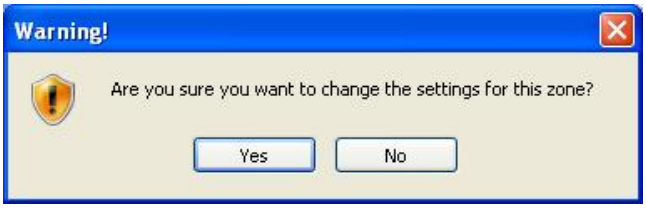
1. Open the Internet Explorer browser, and then select **Tools→Internet Options→Advanced→Security**.
2. Enable the **Allow active content to run in files on My Computer** option.
3. Select **Apply→OK**.

Note: If this option is not set, the user must allow the blocked content manually each time the RSM user interface is initiated.

ActiveX Controls

In the Internet Explorer security settings, enable the ActiveX controls through the following steps:

1. Open the Internet Explorer browser, and then select **Tools→Internet Options→ Security→Internet→Custom Level→ActiveX controls and plug–ins**.
2. Enable the **Automatic prompting for ActiveX controls** option.
3. Select **OK**. The system displays this window.



4. Select **Yes**.

Firewall Settings

If a firewall is installed in the system, you must modify the firewall settings to open certain RSM ports and provide RSM the functionality to communicate properly with the RSM Site Server (SE).

For systems using the Windows Firewall, the RPSW installation package opens the following required ports for the system, unless you choose not to modify the firewall settings:

- TCP 8502—RSM File Agent (required only for file distribution or retrieval features with RSM servers)
- UDP 68—DHCP/PXE client
- TCP 8504—RSMDesktopAgent.exe
- TCP 5800—VNC Server for Win32 (if you selected to install VNC)
- TCP 5900—VNC Server for Win32 (if you selected to install VNC)
- TCP 16992—RSM AMT Agent (Terminals 7459, 7350, 7403, and 7409 only)
- TCP 16993—RSM AMT Agent (Terminals 7459, 7350, 7403, and 7409 only)

If you do not permit the RPSW installation to open the ports, you must manually configure the settings.

For systems using the Windows Firewall, select **Start→Settings→Control Panel→Windows Firewall→Exceptions** to open the required RSM ports, depending on the location and intended use.

If a different firewall is used, open the RSM ports using the appropriate procedure for the firewall being used.

For more information about the ports used for RSM communication, refer to the *NCR Retail Systems Manager Software User's Guide* (B005–0000–1518).

Chapter 2: RPSW Installation

Overview

This chapter describes the prerequisites, installation steps, and post–installation activities of the Retail Platform Software for Windows (RPSW). This chapter also discusses the steps on how to create a client image.

Pre–installation Information

Install the Retail Platform Software for Windows (RPSW) (D370–0924–0100) through any of the following ways:

- Through the installation CD
- Through installers that you can download from the NCR website *http://www.ncr.com/support*.

After obtaining the installers, either use the installation packages on the terminals or upload the installers to the RSM SE Server or FitClient Server so that it can be downloaded and installed on the terminals. For additional information on how to upload applications, refer to the "RSM File Distribution" section in the *NCR Retail Systems Manager Software User's Guide* (B005–0000–1518).

Installation Versions

The RPSW comes in two versions:

- `Retail Platform Software for Windows.msi`
- `Retail Platform Software for Windows.exe`

Remote Installation

Remote installs can be performed on `.msi` files, which mean that the application can be pushed from the server to the client without any action at the client terminal. The Install Parameters (for non–GUI installation) for the RPSW are listed in the `Command line parameters for Retail Platform Software for Windows.doc` file on the CD.

You cannot perform push installs using RSM until the RPSW LPIN (with RSM client software) is installed on the system terminal. Upgrades of RPSW can be installed remotely using RSM. For additional information on using RSM to remotely upgrade the RPSW, refer to the section on using Packages in the *NCR Retail Systems Manager Software User's Guide* (B005–0000–1518).

OPOS Installation

If you install the RPSW and install OPOS 2.2, then you are installing an older release version of OPOS over it; the install lets you install because the "product name" has changed from OPOS to Retail Platform Software for Windows, and the old installation cannot detect the newer release. The real problem comes if you then try to upgrade that older version you just installed back to the newer version. The install thinks the newer version is already there and does not upgrade. If you get into this situation, uninstall both the older and the newer releases of OPOS, and then reinstall.

Prerequisite of the RPSW

Before installing the RPSW, install the following:

- Windows Installer 3.0
- Microsoft SNMP Service

Windows Installer

When installing RPSW, the installer checks whether the Windows Installer version installed on the system is at least version 3.0. If there is no Windows Installer installed on the system or if the version installed is prior to version 3.0, the installer displays a prompt requesting the user to install the latest version of the Windows Installer before installing RPSW.

Microsoft SNMP Service

If you use SNMP, ensure that you have installed the Microsoft SNMP Service before installing the RPSW. The RPSW installation does not ask any questions about the SNMP installation, but some Microsoft SNMP parameters are configured by the RPSW install for use with the RSM SNMP agent. With RPSW 2.3 or later, only the RSM SNMP agent is valid. The SNMP LPIN D370–0512–0100 cannot be used with RPSW 2.3 or later. For additional information on setting up and using SNMP, refer to *RSM SNMP Configuration* on page 102.

Installing the Retail Platform Software for Windows

This section explains how to install the RPSW. Installing RPSW has two setup types: Standard and Custom. For more information about the Custom setup type, refer to *Custom Setup* on page 24.

Note: The images in this section show the installation of the RPSW release version 5.2.0.0 on a Windows 7 Professional 64–bit system.

To install the RPSW, follow these steps:

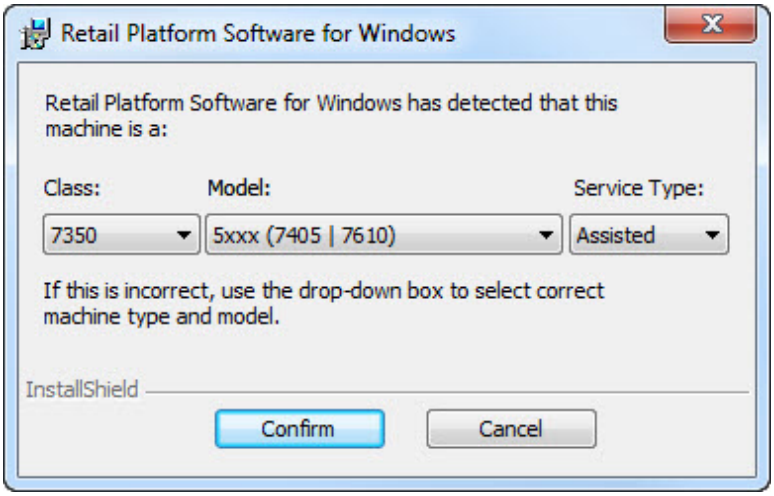
1. Browse for and double–click the installation file, which can be any of the following:
   - **`Retail Platform Software for Windows.exe`**
   - **`Retail Platform Software for Windows.msi`**

Note: If you are running on Windows 7 operating system, you must install the RPSW install package through the Run as Administrator option. If you do not run the installation program as Administrator, the install does not recognize the terminal type and some necessary components of the RPSW software are not installed properly.

To install RPSW as Administrator, perform any of the following:

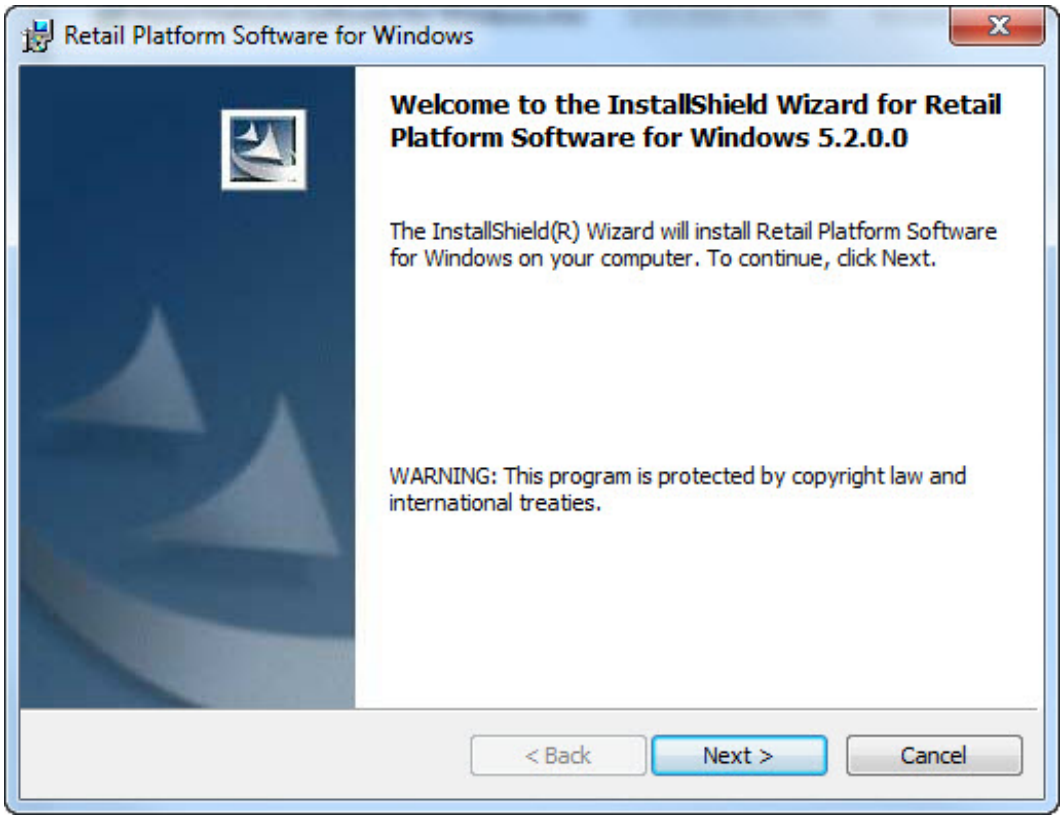
- Right–click the `.exe` version of the install package (`Retail Platform Software for Windows.exe`) and select **Run as administrator**.
- Launch a DOS command prompt with administrative privileges and run the MSIEXEC executable on the `.msi` version of the install package.

After launching the installer, the system displays this window.



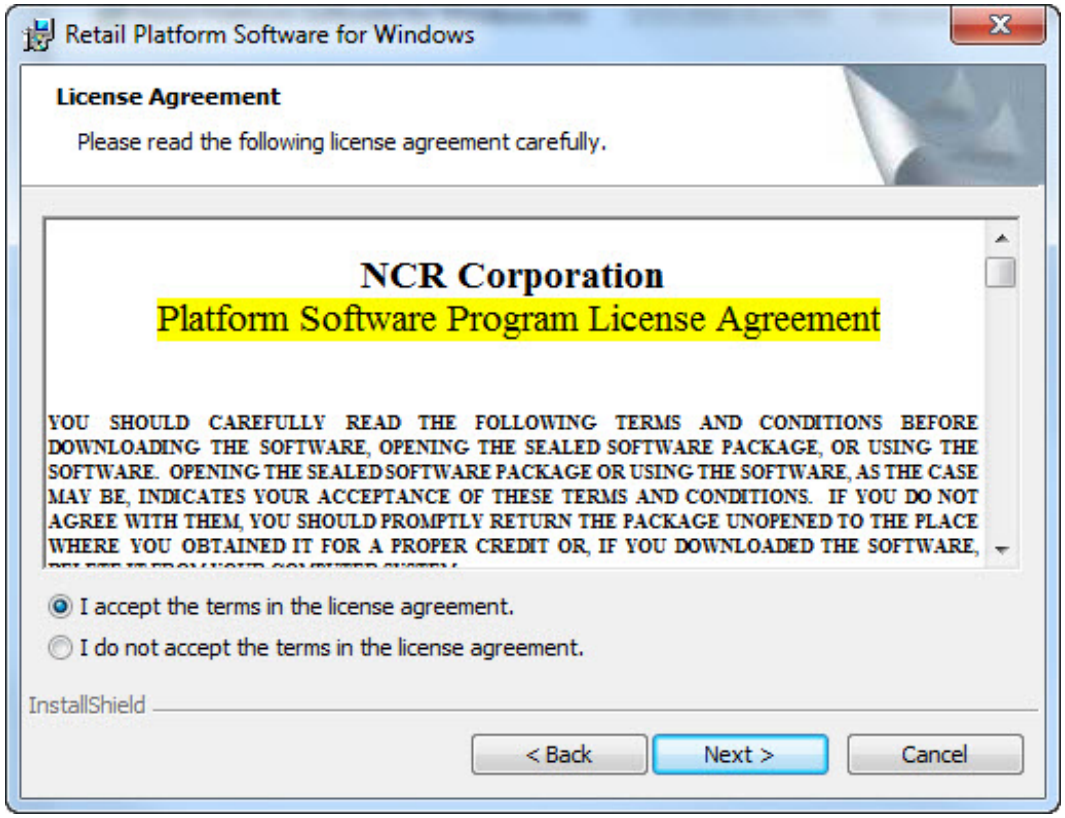
2. The RPSW detects the current configuration. Ensure that the following configurations are correct:
   - **Class**
   - **Model**—defines the type of system where you are installing the RPSW.
   - **Service Type**—can be any of the following:
     - Assisted—includes terminals 7403, 7443, 7446, 7449, 7452, 7453, 7454, 7456, 7457, 7458, 7459, 7460, 7600, 7601, 7610, 7611, 7643, 7649, 7606, and 7616.
     - Self—includes terminals 7350, 7401, 7402, 7404, and 7409.

     The only difference between these two terminal service types is the set of Printer Finite State Machine definition files (used by State of Health) that are installed by default. These files minimize the State of Health changes on an assisted terminal because an operator is present to fix the problem. For example, a paper low status is generated on a Self–Service system indicating the printer on the unattended system needs attention. This type of alert is not necessary, or even undesirable, for systems where a cashier is present to handle the condition.
3. Select **Confirm**. The system displays the Welcome window.

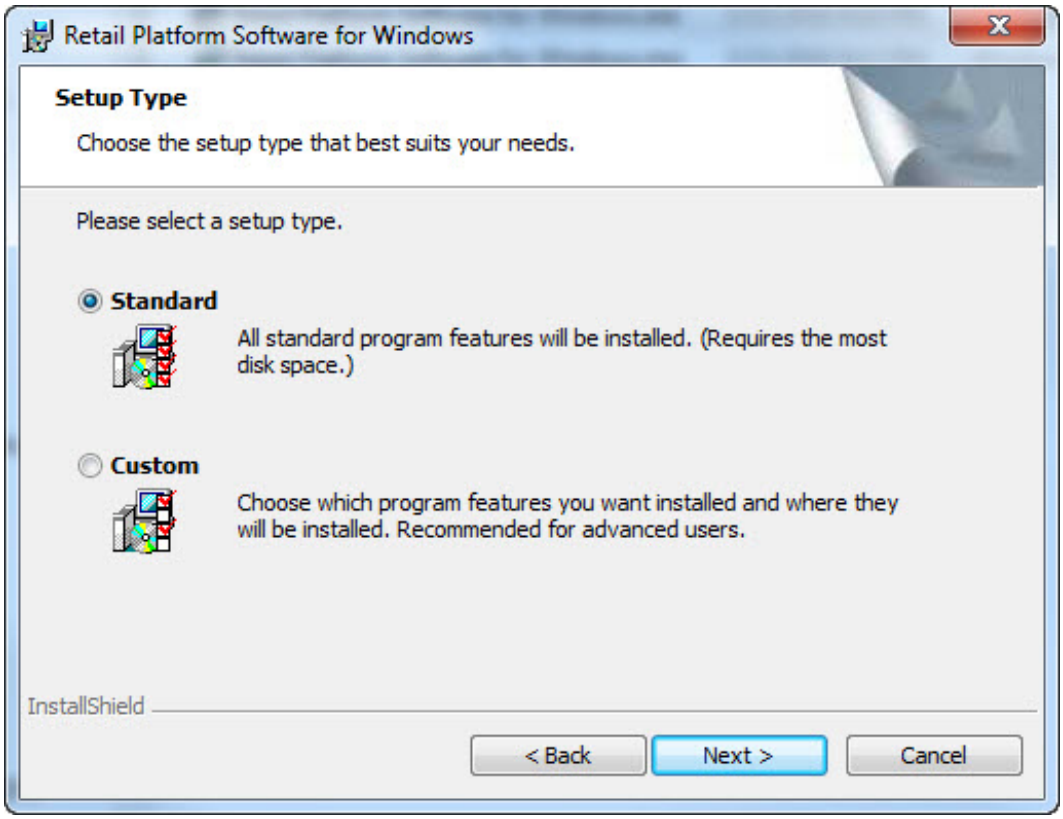


4. Select **Next**.

5. If you have a previous version of OPOS or Logs and Tallies that are currently installed, the system displays a window with options for dealing with the existing installation. Select **Next**.
6. The system displays the License Agreement window. Select **I accept the terms in the license agreement**, and then select **Next**.

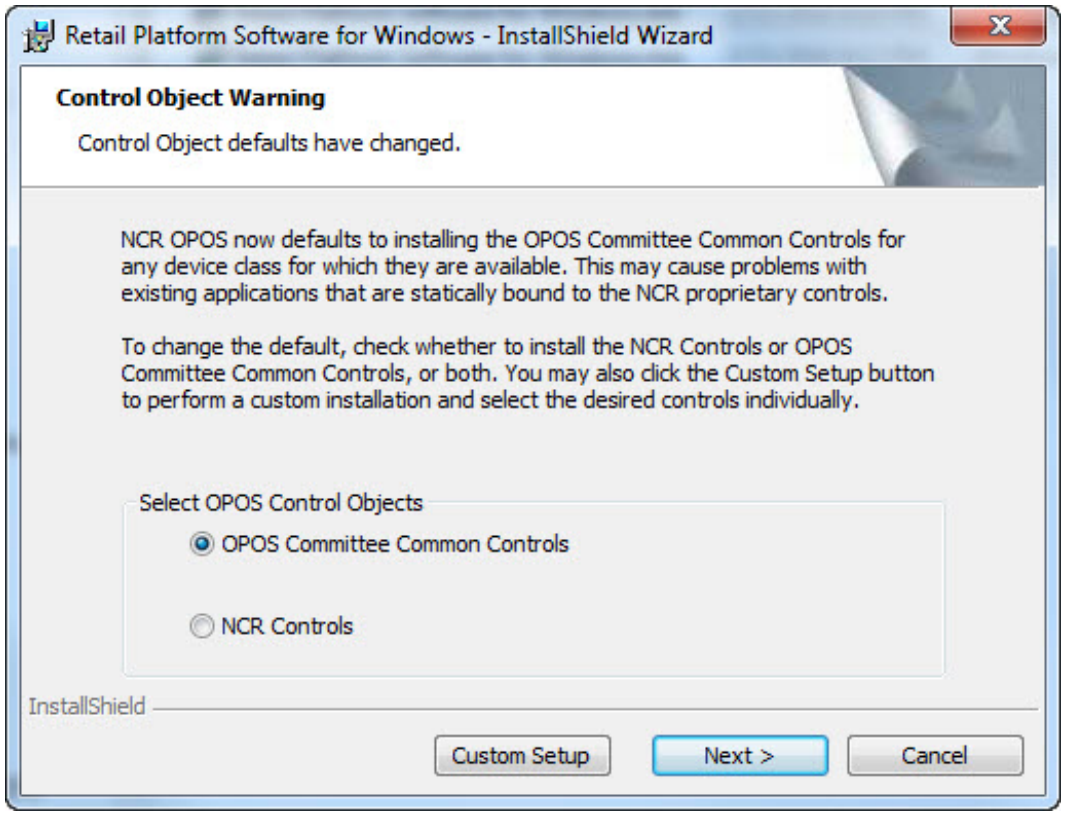


7. The system displays the Setup Type window. Select the type of installation, whether **Standard** or **Custom**, and then select **Next**.



Note: A different section in this publication is created to provide more information about the **Custom** setup type. For more information about the Custom setup, refer to *Custom Setup* on page 24.

8. If you selected the Standard setup type, the Control Object Warning window is displayed.

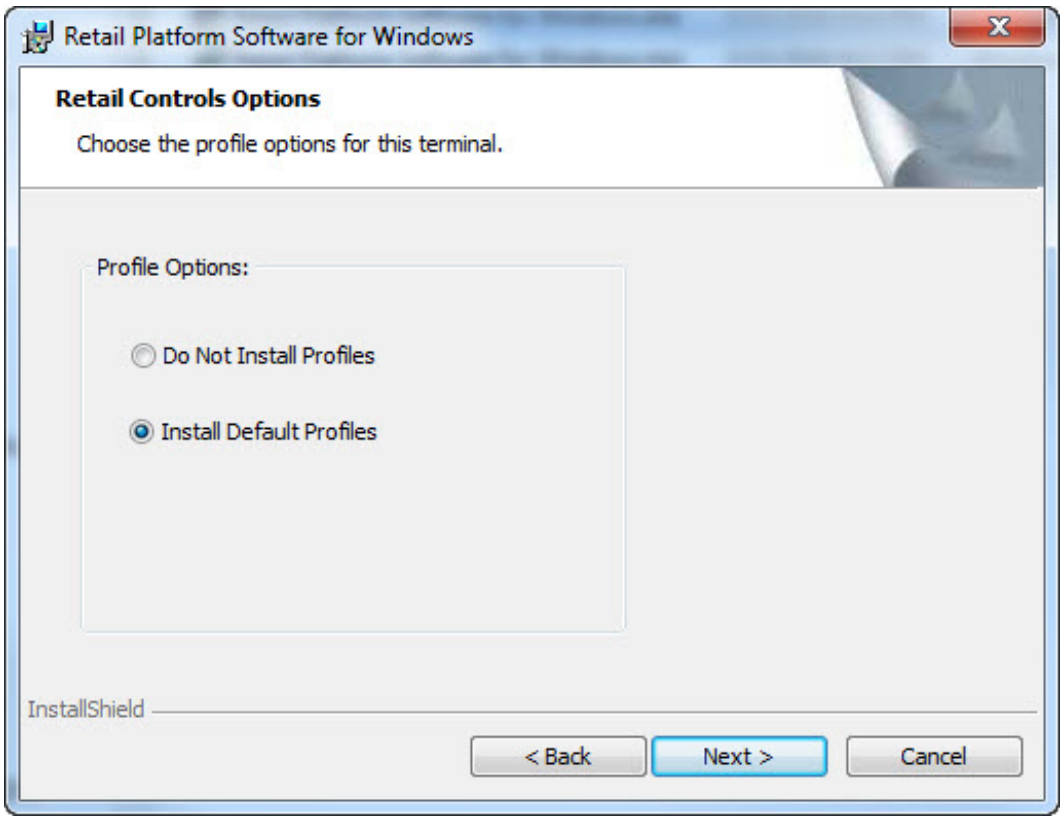


Select the OPOS Control Objects you want to install:

- **OPOS Committee Common Controls**—enables the feature for OPOS 1.14.1 Specification Compliant Common Control Objects.
- **NCR Controls**—enables the feature for OPOS 1.4 Specification Compliant Control Objects.

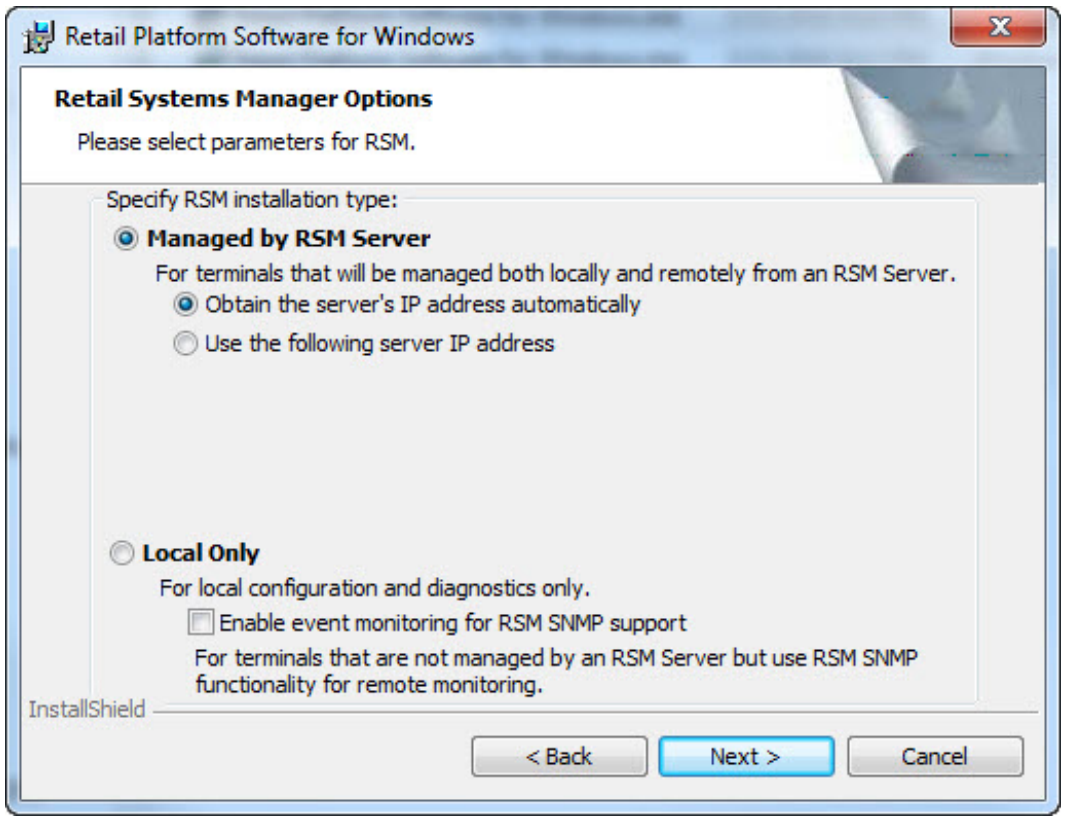
9. Select **Next**.

The system displays the Retail Controls Options window.



10. Select any of the following Profile Options:
    - **Do Not Install Profiles**—indicates that none of the OPOS Profiles are installed. This option is commonly used where the solution provider installs all of the profiles that are needed for a specific customer.
    - **Install Default Profiles**—refers to the option that is most suitable for new installations.
    - **Use Saved Profiles** (Upgrading only)—displays only if you are upgrading OPOS and you want to use the same profiles that the old version of OPOS used. These profiles are saved at the start of the RPSW installation.
11. Select **Next**.

The system displays the Retail Systems Manager Options window.



12. Select the RSM installation type:

    - **Managed by RSM Server**—refers to the option where you can optionally identify the RSM SE server's name or IP address so that the system communicates with a specific server.

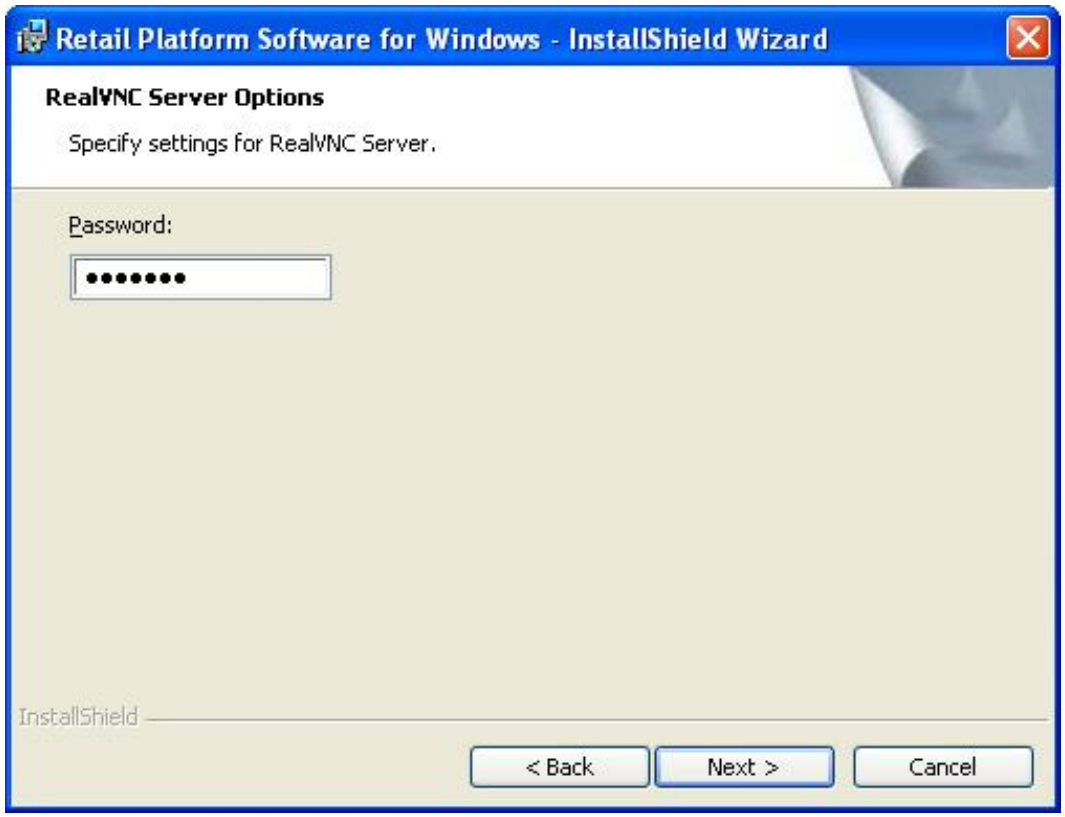
      In a Dual Server environment, the name or IP address for both RSM SE servers would be entered. If you do not specify a server, the system automatically finds one on the network. If you do not know your server name or IP address, see your system administrator. In a Dual Server environment with Command Center, NCR recommends that the server name or IP address is set to the PXE Image Loader servers to simplify role changes for Command Center. In other PXE Image Loader configurations, there is no need to configure the client as managed.

- **Local Only**—refers to the option where no RSM SE server is present. If you plan to use SNMP or Command Center in this configuration, select the option **Enable event monitoring for RSM SNMP support**.

  If the check box for event monitoring is selected, the NCRFSM module is enabled for processing the event log to generate alerts for State of Health and Critical Events. On unmanaged systems, this functionality is required only if RSM SNMP or Command Center is used. Selecting this check box sets registry setting *[HKEY_LOCAL_MACHINE\SOFTWARE\NCR\NCR Store Minder Client\CurrentVersion\StartFSM]* to T to enable NCRFSM, which is the same as it would be set on a managed system. The setting is only available in RPSW 4.0.1.0 and up. If a system is installed as unmanaged and later changed to managed, this setting may need to be configured manually to enable NCRFSM.

13. Select **Next**.

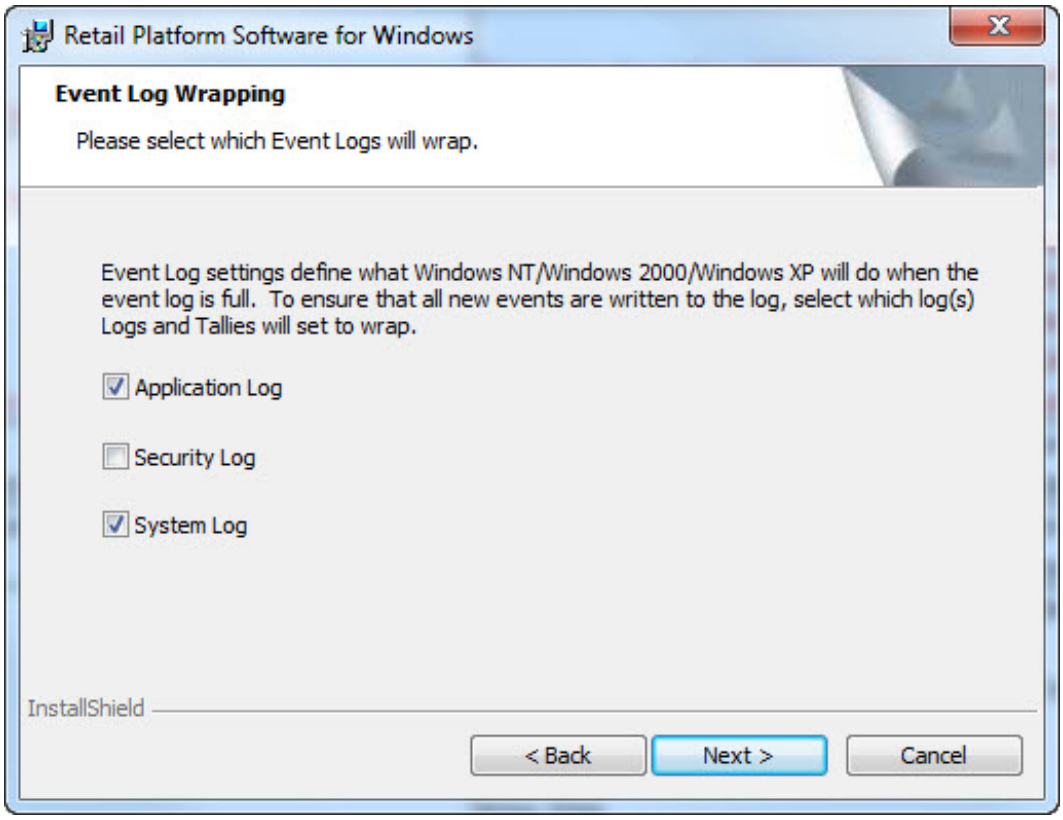
In a Custom installation, if you selected to install RealVNC, the system displays the RealVNC Server Options window.



Note: Selecting to install RealVNC in the RPSW installation is not supported for systems running on the Windows 7 operating system.

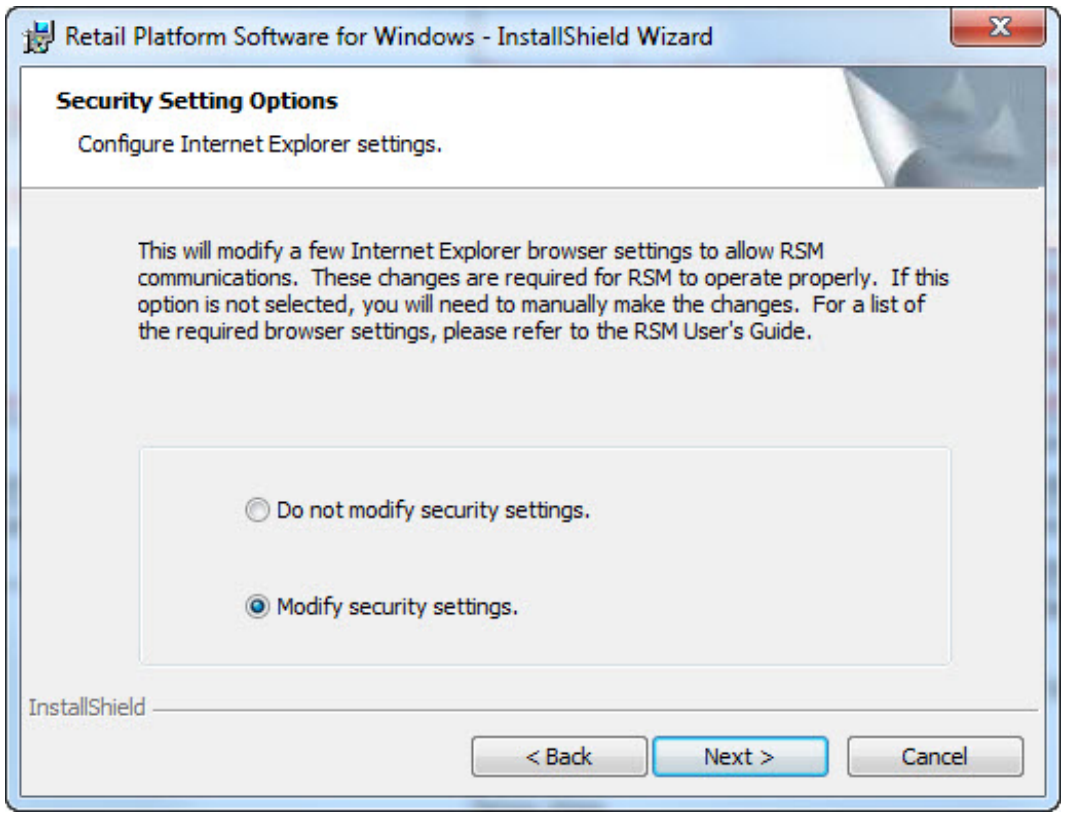
14. Enter the **Password** for accessing this system from a remote location using the RealVNC program.
15. Select **Next**.

The system displays the Event Log Wrapping window. RPSW software logs events, and RSM uses these events to report device status. If the event log gets full and does not wrap, events discarded by Windows cannot be used for device statuses.



16. Select which Event Logs you want to wrap when the event log is full.
17. Select **Next**.

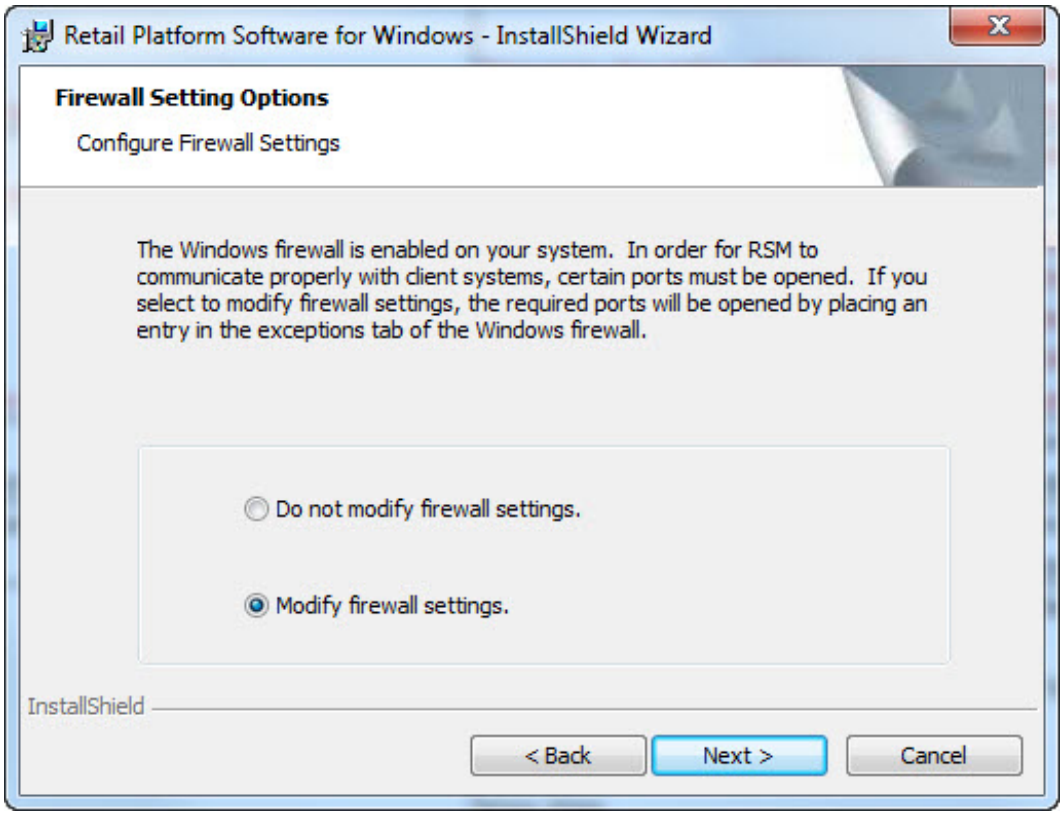
The system displays the Security Setting Options window.



18. Select the Security Setting Options:
    - **Modify security settings**—indicates that the RPSW installation will make the changes for you.
    - **Do not modify security settings**—indicates that if you select this option, or if a patch or another software program changes these values, you need to manually change these settings.

    For more information, refer to *Internet Explorer Security Settings* on page 4.
19. Select **Next**.

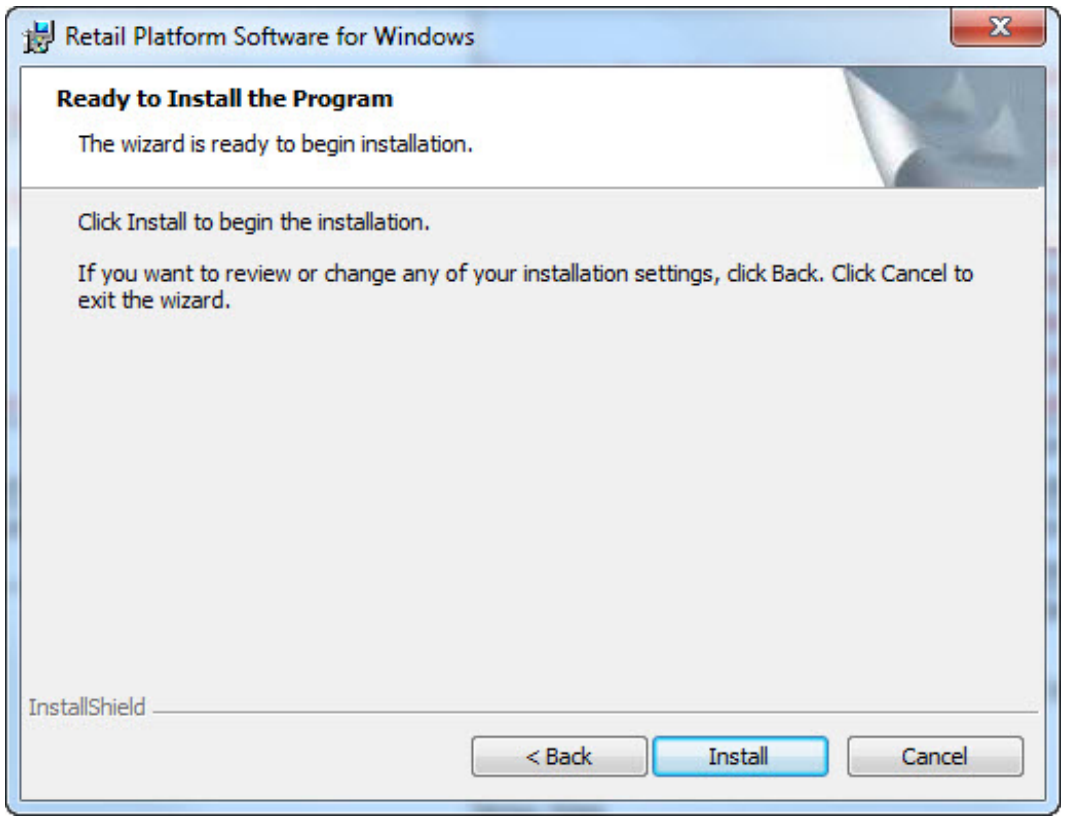
If Windows Firewall is enabled, the system displays the Firewall Setting Options window to set up the ports that can get through the firewall to support RSM.



20. Select the Firewall Setting:
    - **Modify firewall settings**—the RPSW installation opens certain RSM ports.
    - **Do not modify firewall settings**—select this option if another firewall is present, and if you want to manually configure the firewall to open ports for RSM communication.

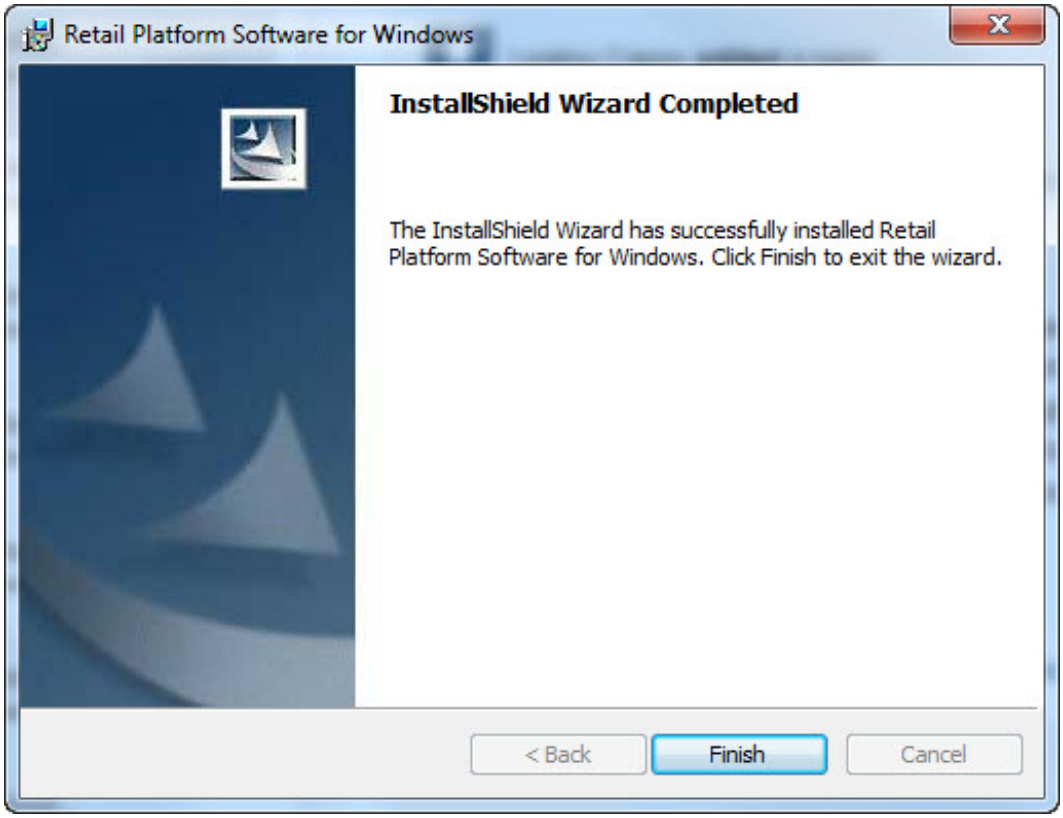
    For more information, refer to *Firewall Settings* on page 5.
21. Select **Next**.

The system displays the Ready to Install the Program window.

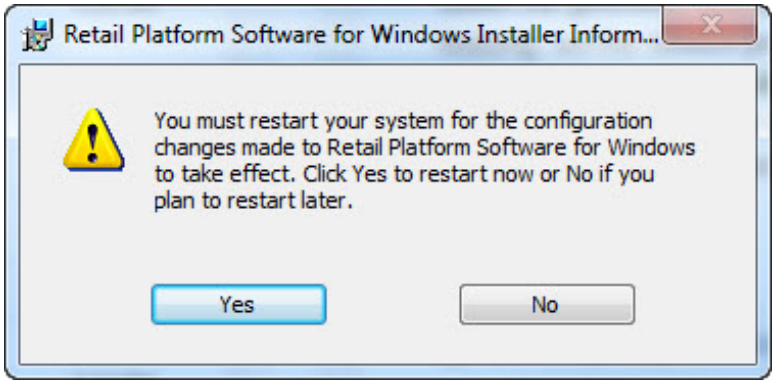


22. Select **Back** if you need to make any changes, or **Install** if you are ready to install the Retail Platform Software for Windows.

23. When the installation is complete, select **Finish**.



The system displays a message stating you should reboot the client terminal.

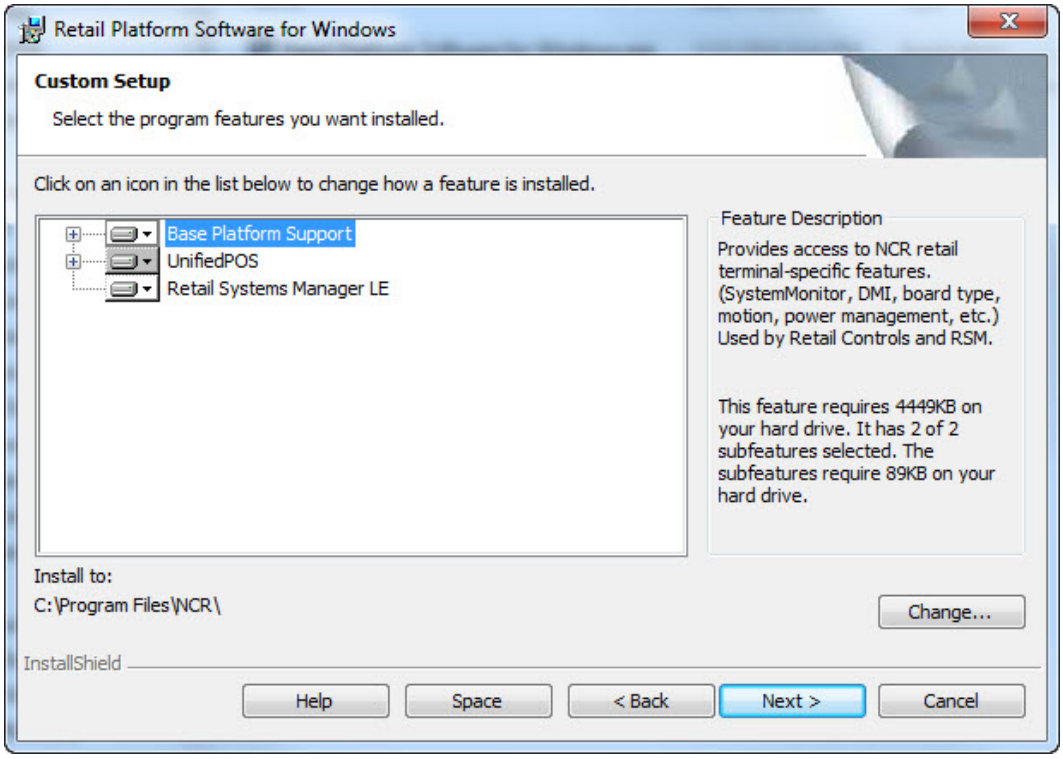


24. Select **Yes**.

Note: After rebooting, if the system and the RSM SE server are connected in a LAN and you selected Managed by RSM Server during installation, the system should automatically become a Managed System.

Custom Setup

The Custom setup type provides the functionality to select the available options that you want to install. If you select the custom setup type in the installation process, the system displays the Custom Setup window.

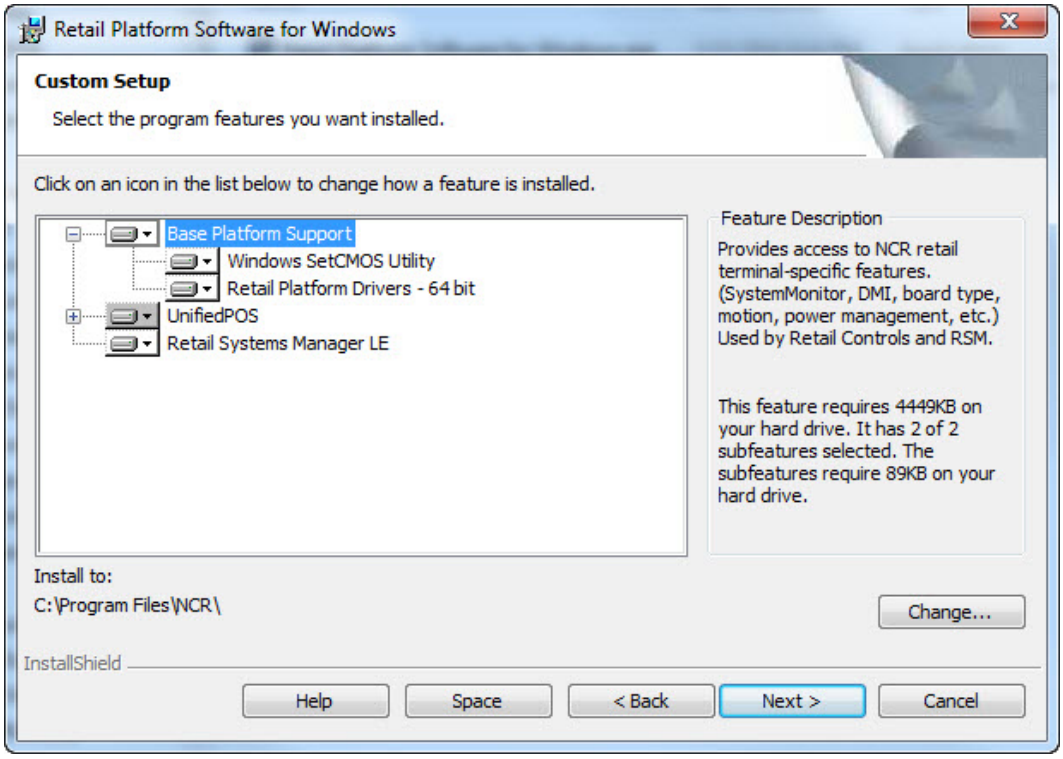


Note: The Predictive Services installation options are no longer available in the RPSW 4.0.1.x and later releases. For these releases, installing the Predictive Services software is possible through a separate LPIN (D370–0955–0100).

Base Platform Support

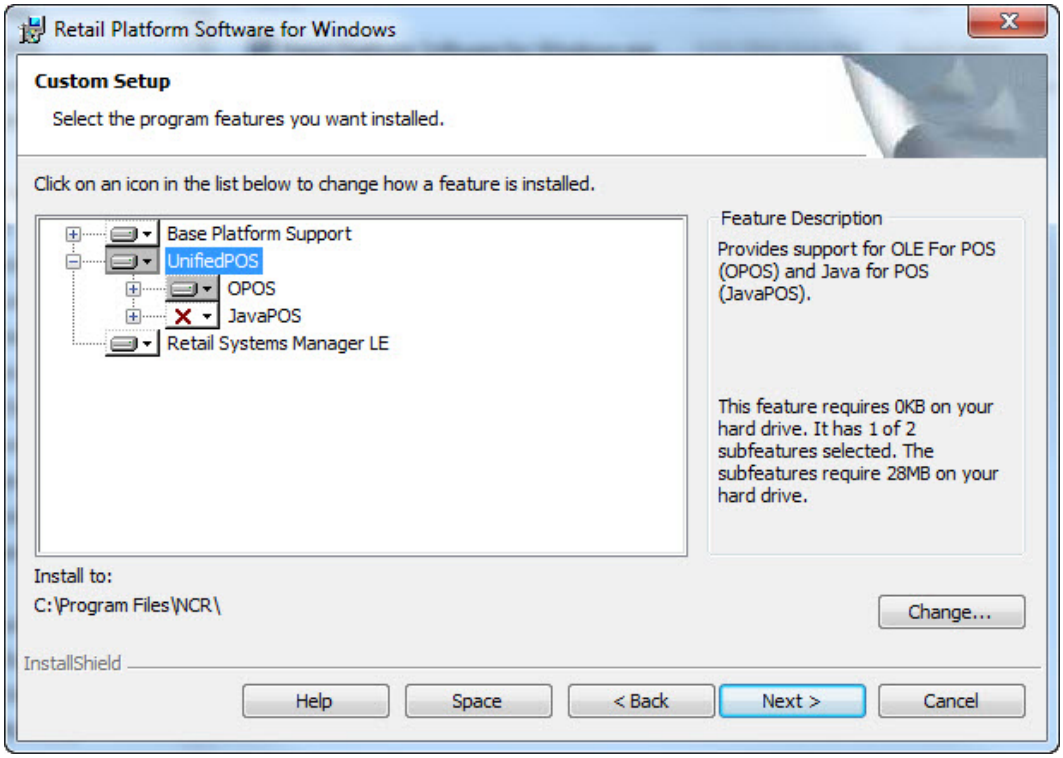
The Base Platform Support contains software for terminal–specific functionality. The Base Platform Support provides functionality used by some peripherals software, RSM, and Command Center. Additionally, it provides the following support:

- Windows SetCMOS Utility—provides the functionality to modify the PC BIOS setup parameters.
- Retail Platform Drivers – 64 bit



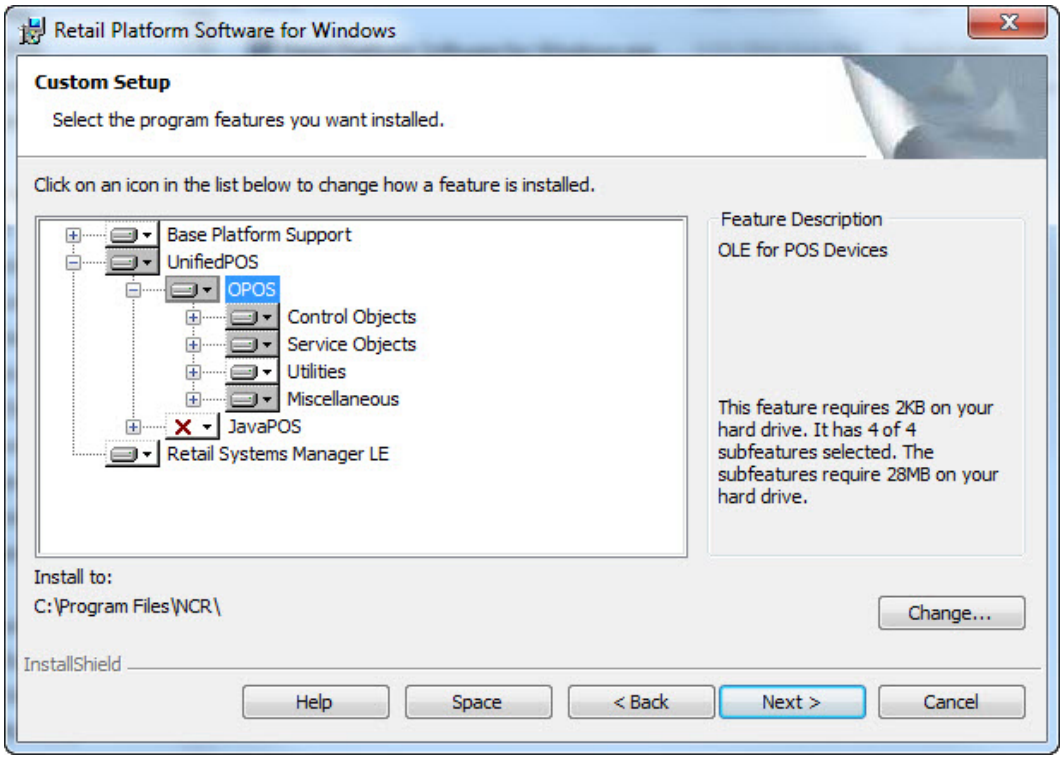
UnifiedPOS

The UnifiedPOS feature provides support for OLE for POS (OPOS) and for Java for POS (JavaPOS).



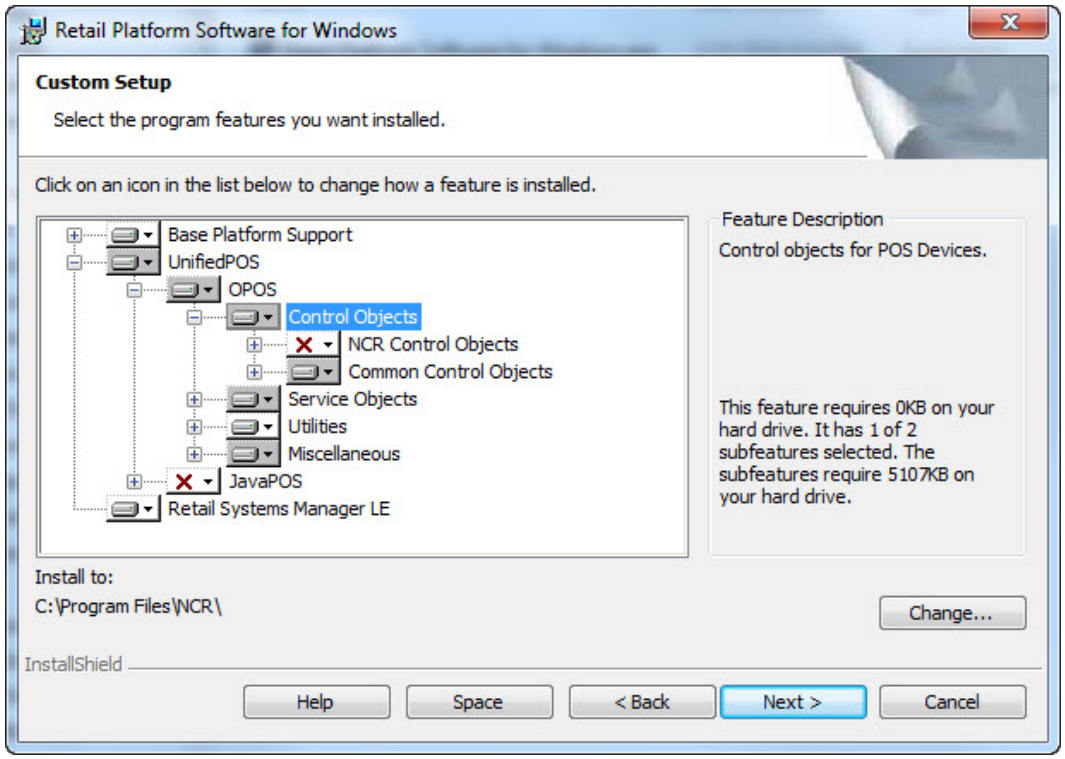
NCR OPOS

NCR OPOS is an industry standards interface for accessing and configuring the retail peripherals. NCR OPOS provides interactive and non–interactive diagnostics for analyzing problems with the peripherals.



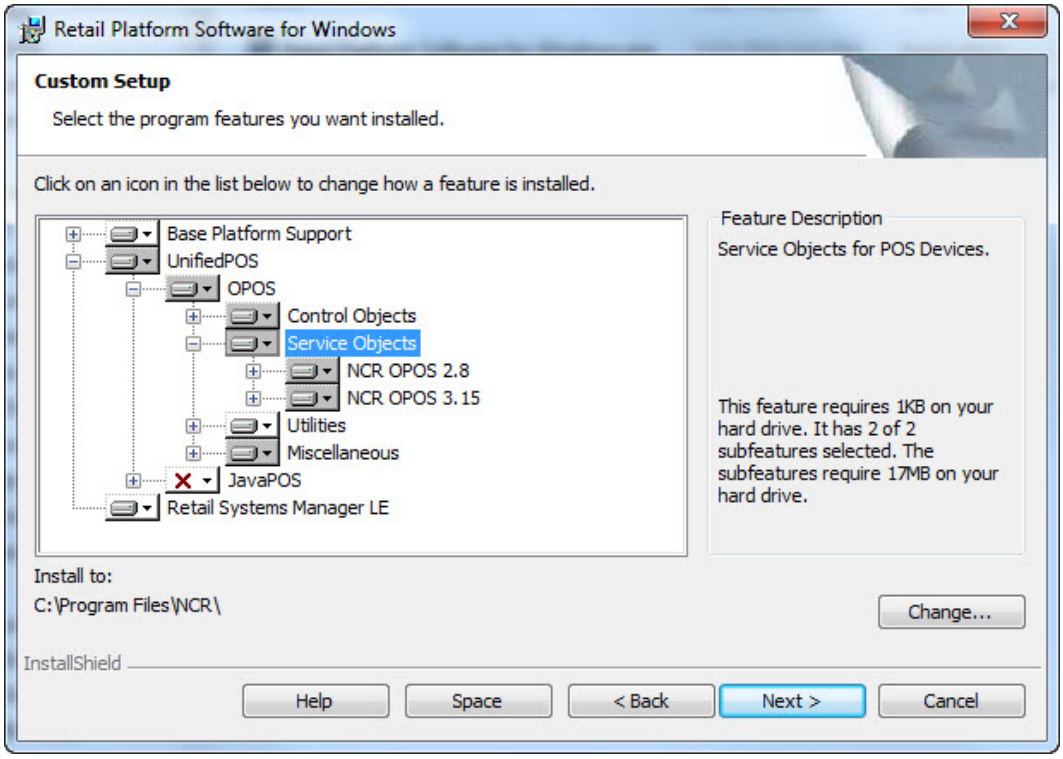
NCR OPOS includes the followed components:

- **Control Objects**

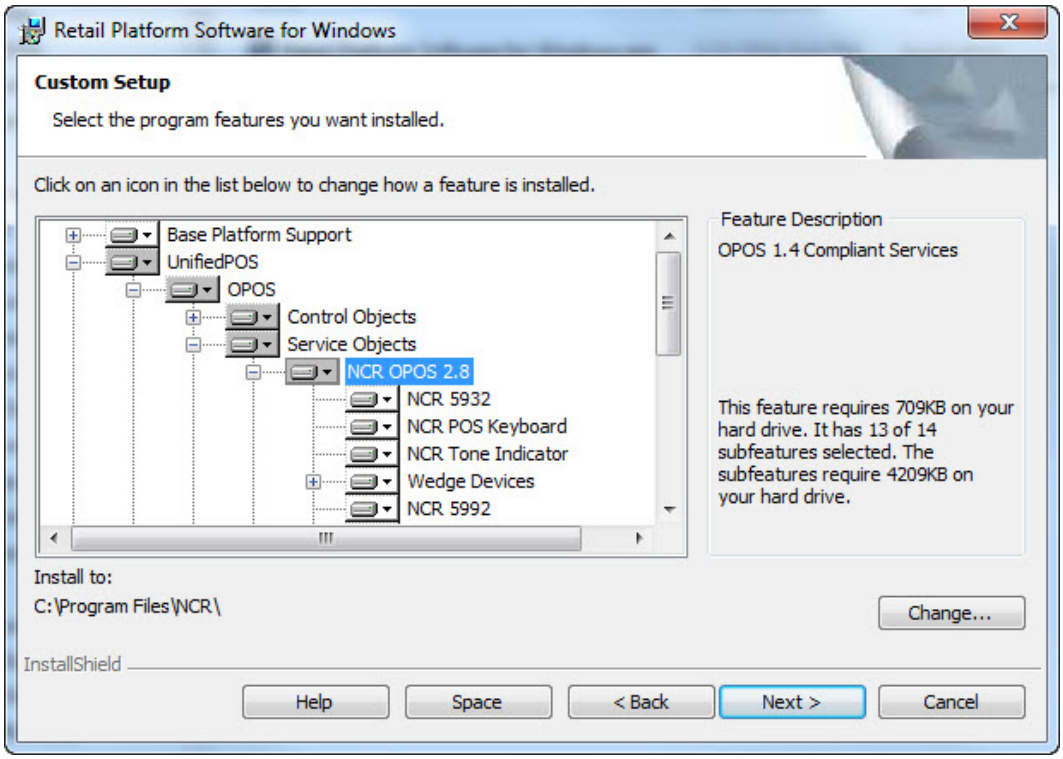


  - NCR Control Objects—1.4 Specification Compliant Control Objects. NCR Controls are listed individually.
  - Common Control Objects—1.14.1 Specification Compliant Common Control Objects. Common Control Objects are listed individually.

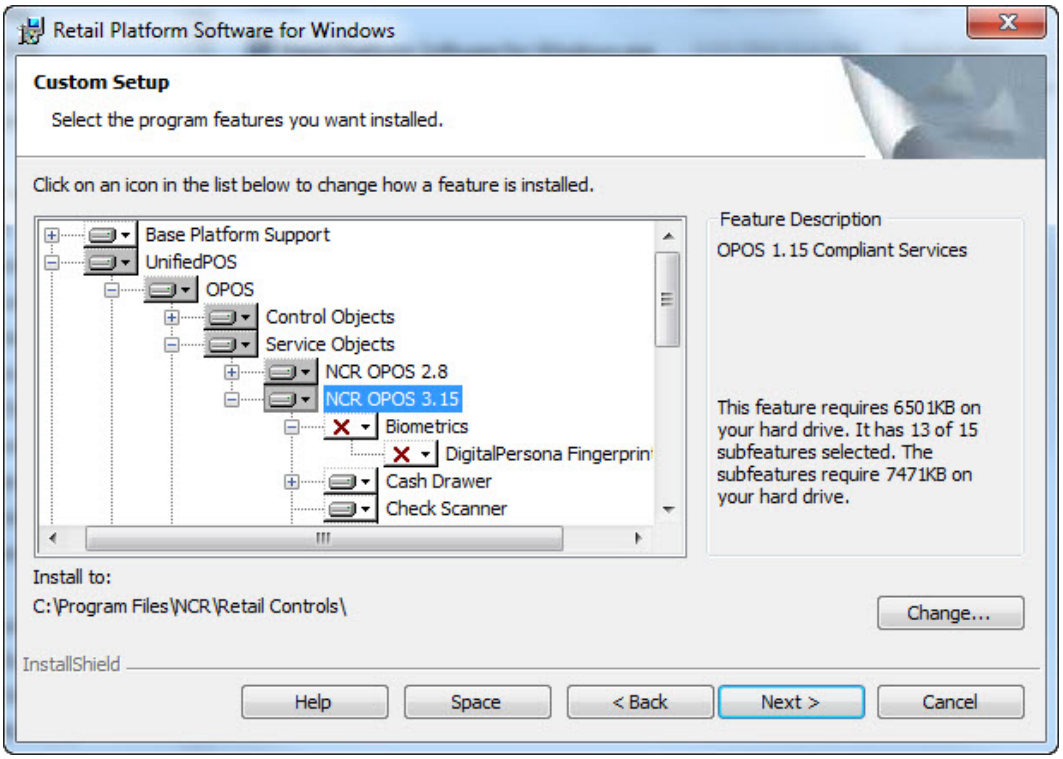
- **Service Objects**



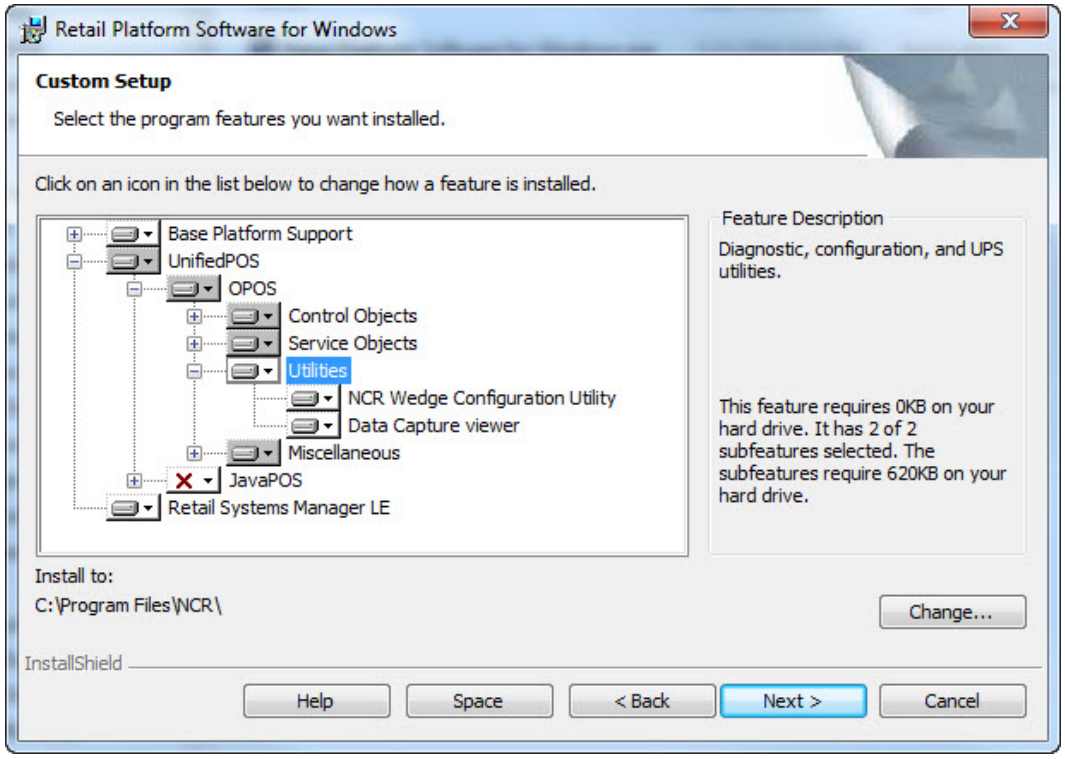
- NCR OPOS 2.8—OPOS 1.4 Compliant Services. It supports all terminals. Updates to this feature have been capped. This feature is not being updated as new features are added to the various terminals. For information on the NCR OPOS 2.8 service objects, refer to *OPOS 2.8 Controls* on page 34.



- NCR OPOS 3.15—OPOS 1.15 Compliant Services. It supports RealPOS 20 (RP20), 30, 70, 80, 80C, and newer terminals. For information on the NCR OPOS 3.15 service objects, refer to *OPOS 3.15 Controls* on page 36.

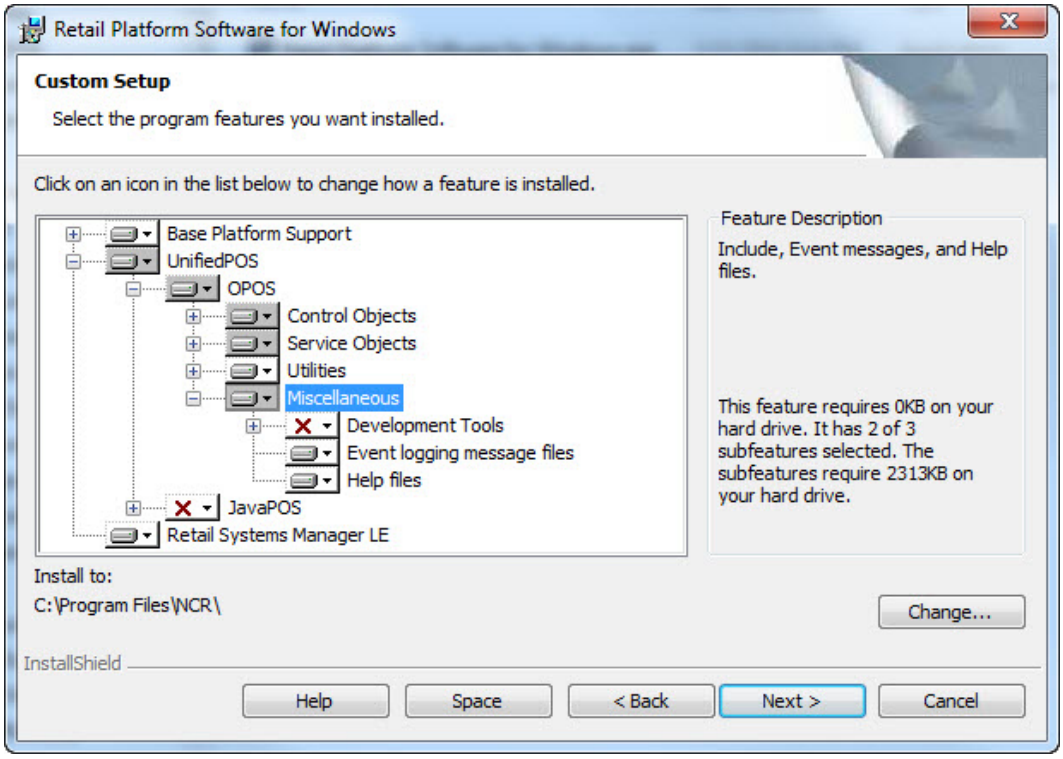


- **Utilities**



- NCR Wedge Configuration Utility—provides a user–friendly interface to configure various devices attached to the keyboard wedge.
- Data Capture Viewer—displays trace information from NCR Controls.

- **Miscellaneous**



- Development Tools—provides Include files and tools needed for development.
  - Form Designer—provides the functionality to design forms in conjunction with the Form Control.
  - Include Files—includes files for application development.
- Event Logging Message Files—event log message DLL files. These files provide additional details in the event logs.
- Help Files—OPOS Windows Help File version 2.7. This file is not being updated as new features become available.

OPOS 2.8 Controls

The following list displays the NCR OPOS service objects that you can include in the installation:

- NCR 5932—NCR 5932 USB Keylock/MSR/Tone Indicator service object for the 7456 and 7458 terminals.
- NCR POS Keyboard—NCR POS Keyboard service object.
- NCR Tone Indicator—NCR Tone Indicator service object.
- Wedge Devices—NCR Wedge Devices service object.
  - NCR Wedge Kiosk
  - NCR Wedge MSR
  - NCR Wedge Scanner
  - NCR Wedge Driver 64–bit
- NCR 5992—NCR 5992 Form/Line Display/MSR/PIN Pad/Signature Capture service object.
- NCR 7448 Keylock—controls the keylock on the NCR 7448 or a USB keylock.
- NCR Cash Drawer—controls the Cash Bases DRUR01, MPU, and the Tellermate SmarTill cash drawers through serial connection and the 7401, 7448, 7453, 7454, 7455, 7456, 7458, and 7460 Cash Drawer using the I/O port connection. This service object supports drawers that are connected to the workstation.
- NCR CashDrawer/MICR/POSPrinter—supports drawers that are connected to the printer kick–out port.
- NCR Hard Totals—store totals information on Disk or in CMOS (for a retail workstation).
- NCR Integrated MSR—NCR Integrated MSR service object.
- NCR International Line Display—International–VFD Line Display service object. It controls the International version of the 5972 Line Display.
- NCR Line Display—line display service object for non–International–VFD models.
- NCR Motion Sensor—detects motion on the NCR 7401, 7403, 7404, 7454, and 7455.
- NCR Scanner/Scale—NCR 78xx–series Scanner/Scale service object.

The following table displays the support for OPOS 2.8 Controls:

UnifiedPOS Control	Devices Supported
Cash Drawer (On Printer)	NCR 7167, NCR 7168, NCR 7197, NCR 7198
Cash Drawer (Integrated)	NCR 7446–1xxx, NCR 7446–3xxx, NCR Darlington, NCR RP20 7443, NCR RP21 7443, NCR 7402
Keylock	NCR 5932, NCR 5953
Line Display	NCR 7402, NCR 744x, NCR 7610, NCR 7611, NCR 5972, NCR 5992
MICR Printer	NCR 7167, NCR 7168
MSR	NCR 5932, NCR 5953–6xxx, NCR 5932–2xxx, NCR 7403, NCR 7409, NCR 7404, NCR 7402, NCR RP20–7443, NCR RP21–7443, NCR 5992
PIN Pad	NCR 5992
POS Keyboard	NCR 5932
POS Printer	NCR 7167, NCR 7168, NCR 7198, NCR F301, NCR F306, NCR F309, NCR K590
Scale	NCR 7876
Scanner	NCR 7892, NCR 7883, NCR 7884, NCR 7876, HHP3800G (2357), HHP4600G, HHP5600G&3800G (2357), HHP5600G&3800R, HHP5620G&3820R, NCR 7837–1xx, NCR 7837–3xx
Signature Capture	NCR 5992
Tone Indicator	NCR 5932, NCR 5953, NCR 7403, NCR 7409

OPOS 3.15 Controls

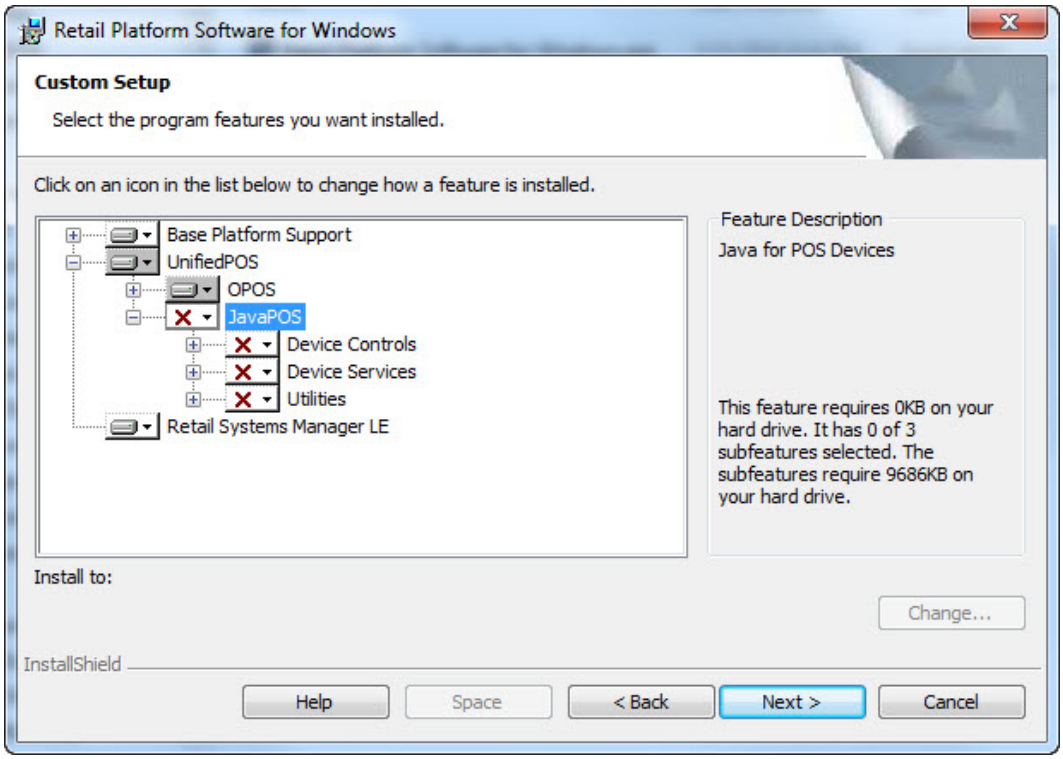
The following table displays the support for OPOS 3.15 Controls:

UnifiedPOS Control	Devices Supported
Biometrics (Fingerprint Reader)	NCR 7610
Cash Drawer (On Printer)	NCR 7167, NCR 7168, NCR 7197, NCR 7198
Cash Drawer (Integrated)	NCR 7402 Darlington, NCR 7403, NCR 7404, NCR 7443, NCR 7446, NCR 7449, NCR 7456, NCR 7457, NCR 7458, NCR 7459, NCR 7606 Pocono, NCR 7643, NCR 7600, NCR 7601, NCR 7649 RP23, NCR 7610, NCR 7611, NCR Talladega
Check Scanner	NCR 7167
Hard Totals	Disk–based Media
Image Scanner	NCR 7879
Keylock	NCR 5932 USB Keyboard, NCR 5953 USB Dynakey, or 5954 USb Dynakey
Line Display	NCR 5972 VFD, LCD, and Occular LCD (Serial only for all models), NCR 7402 APA, NCR 7402 2x20, NCR 7403 2x20, NCR 7443, NCR 5975 2x20, NCR 5975, NCR 7611 2x20, NCR 7610 2x20, NCR 5976
MICR	NCR 7167, NCR 7168, NCR 7156
Motion Sensor	NCR 7402, NCR 7403, NCR 7404, NCR 7409
MSR	NCR 5932 USB Keyboard, 5953 USB Dynakey, or 5954 USB Dynakey, NCR 5953–6xxx, NCR 5953–85xx, NCR 5966, NCR 7403, NCR 7409
PIN Pad	NCR 5992
POS Keyboard	NCR 5932
POS Printer	NCR 7156, NCR 7158, NCR 7167, NCR 7168, NCR 7197, NCR 7198, K590, 7342–F306, 7342–F307, 7342–F309, H600
Hydra Printer	NCRK5XX, NCRMod34, NCRH6XX
Scale	NCR 7872, NCR 7875, NCR 7876, NCR 7878, NCR 7874

UnifiedPOS Control	Devices Supported
Scanner **Note:** Please note of the following options: • USB—OS supported HID USB • NCR USB—USB scanner connected through a Virtual Serial COM port emulation driver. Requires additional driver install.	• For Serial, NCR USB, or USB connection types: NCR 7872, NCR 7873, NCR 7874, NCR 7875, NCR 7876, NCR 7878, NCR 7883, NCR 7884, NCR 7892, NCR 2356, NCR 7893 • For Serial or NCR USB connection types: NCR 7837, NCR 7838, NCR 7880, NCR 7882, NCR 2357, NCR 3800, NCR 4600, NCR 5600/20 • For Serial connection type only: NCR 7832 (Serial) • For USB connection type only: NCR 7404EP Advantage (USB)
Signature Capture	NCR 5992
Tone Indicator	NCR 5932 USB Keyboard, NCR 5953 USB Dynakey, or 5954 USB Dynakey, NCR 7403, NCR 7409

NCR JavaPOS

JavaPOS is a wrapper application for OPOS that is used to write Java applications using the OPOS Retail Controls.



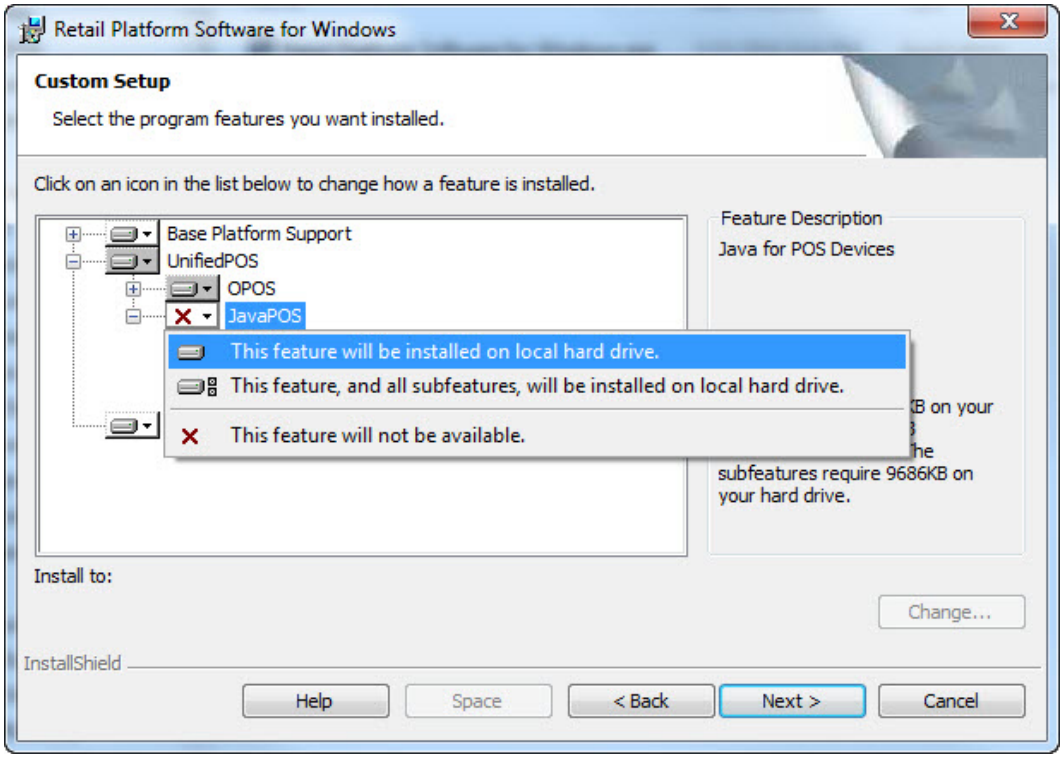
NCR JavaPOS includes the following components:

- Device Controls
  - JavaPOS Common Controls 1.13.2—JavaPOS common controls released by the UPOS committee.
- Device Services
  - NCR JavaPOS 2.0 with NCR Legacy Loading Scheme—uses registry entries for peripheral configuration parameters.
  - NCR JavaPOS 2.2 with JCL Support—uses XML file entries for peripheral configuration parameters.
  - NCR JavaPOS 3.x—supports the NCR RealPOS 20, 30, 70, 80, 80C and newer terminals. Updates to this feature will parallel the NCR OPOS 3.x updates.
- Utilities
  - JCL Editor—the Java editor released by the UPOS committee.

Installing the JavaPOS

The default installation for the RPSW installs only OPOS. To use JavaPOS, perform a custom setup. To install JavaPOS through the custom setup, follow these steps:

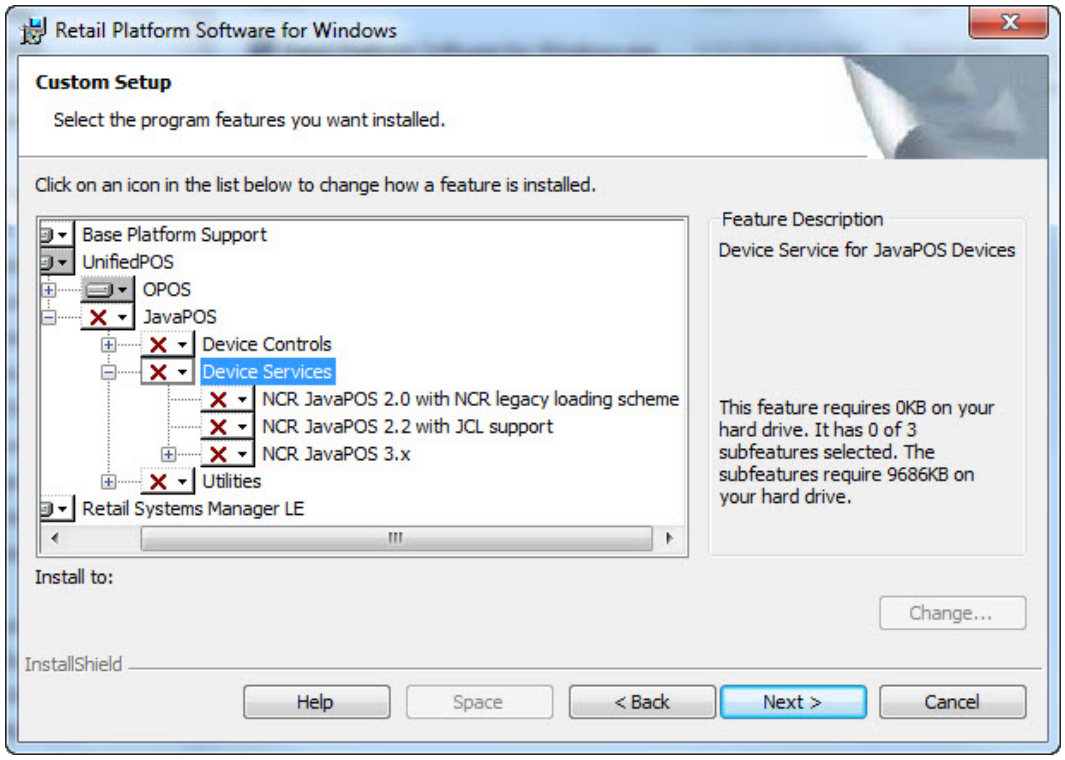
1. On the Custom Setup window, select **UnifiedPOS**, and then select **JavaPOS**. The setup displays the following options:



2. Select **This feature will be installed on local hard drive**.

Note: Selecting this option installs only the JavaPOS 3.x.

3. If you want to install the JavaPOS 2.2 controls or both the JavaPOS 2.2 and 3.x controls, select and expand **Device Services**.



4. Select the versions that you want to install.

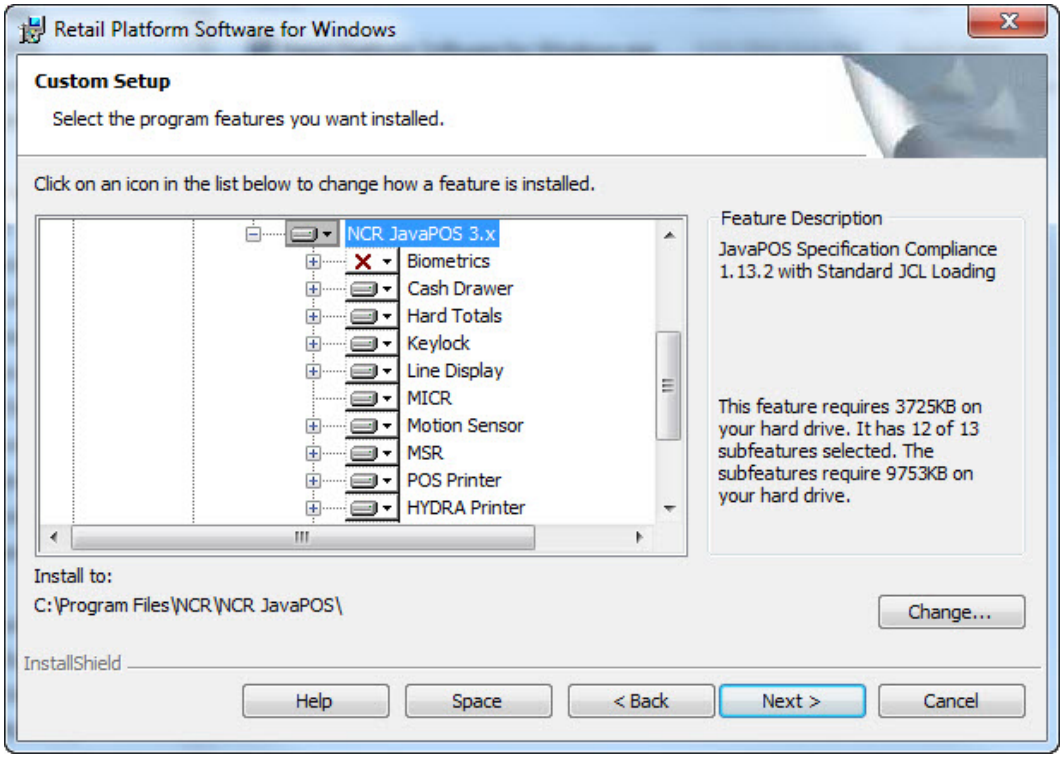
Note: Do not select the JavaPOS 2.0 version. This version is for legacy support only.

5. Select **Next** to continue to the next installation steps.

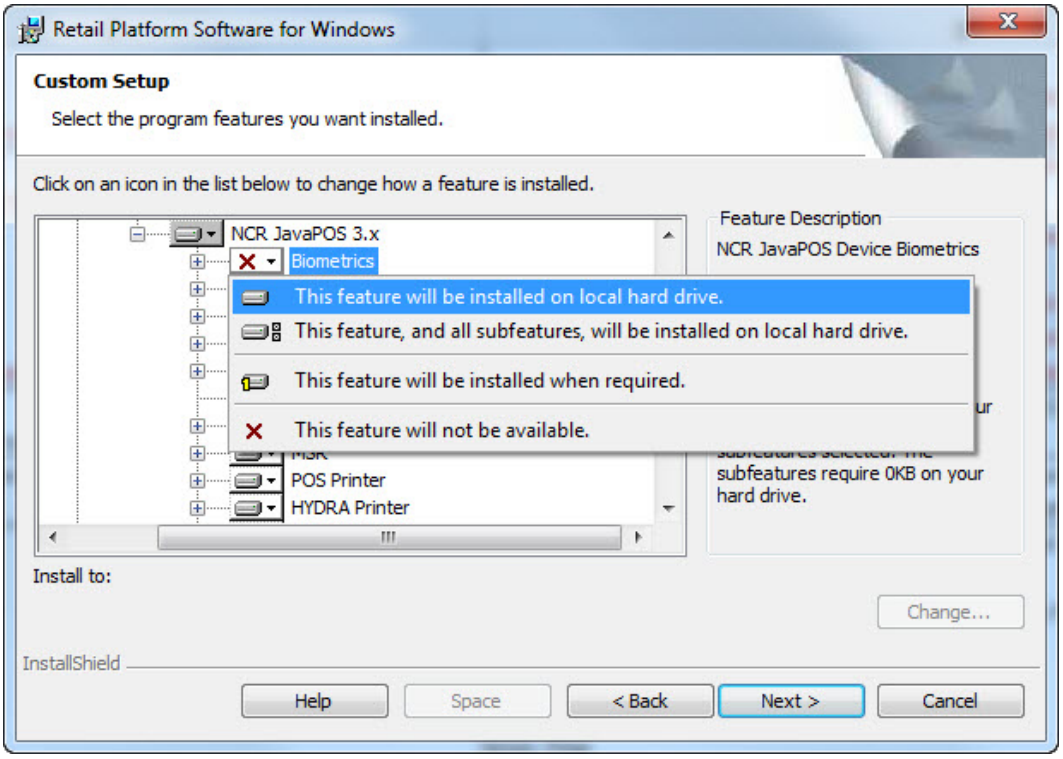
Installing the Biometrics

The Biometrics driver is not automatically installed when you choose to install the JavaPOS 3.x controls. If you need the Biometrics driver, follow these steps:

1. In the Custom Setup window, expand the **NCR JavaPOS 3.x** entry and then select **Biometrics**.



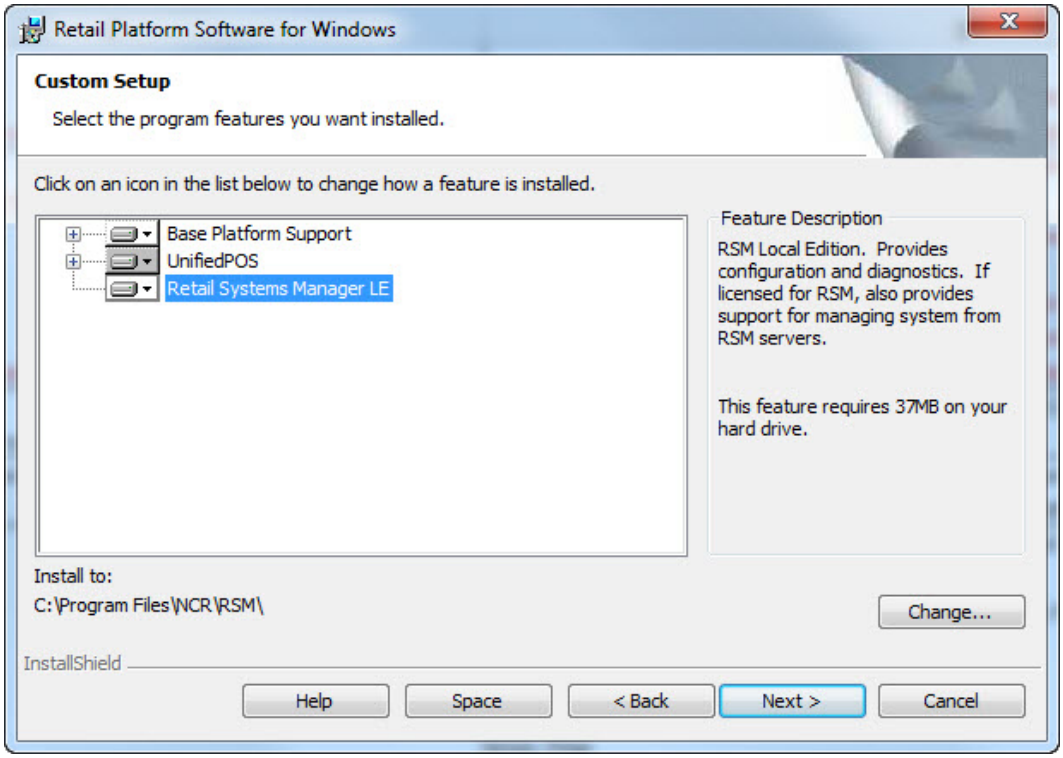
2. Select **This feature will be installed on local hard drive**.



3. Select **Next** to continue to the next installation steps.

Retail Systems Manager Local Edition (RSM LE)

RSM LE provides local configuration and diagnostic capabilities. If licensed, RSM LE also provides support for managing the system from RSM servers.



The RSM LE feature in the RPSW installation provides the option to install RealVNC 3.3.7. This remote control software provides the ability to remotely control a terminal. This feature used to be installed by default, but now you must select it as part of a custom installation.

Note: Selecting to install RealVNC in the RPSW installation is not supported for systems running on the Windows 7 operating system. The sample image above shows RPSW installed on a Windows 7 Professional 64–bit system.

Predictive Services

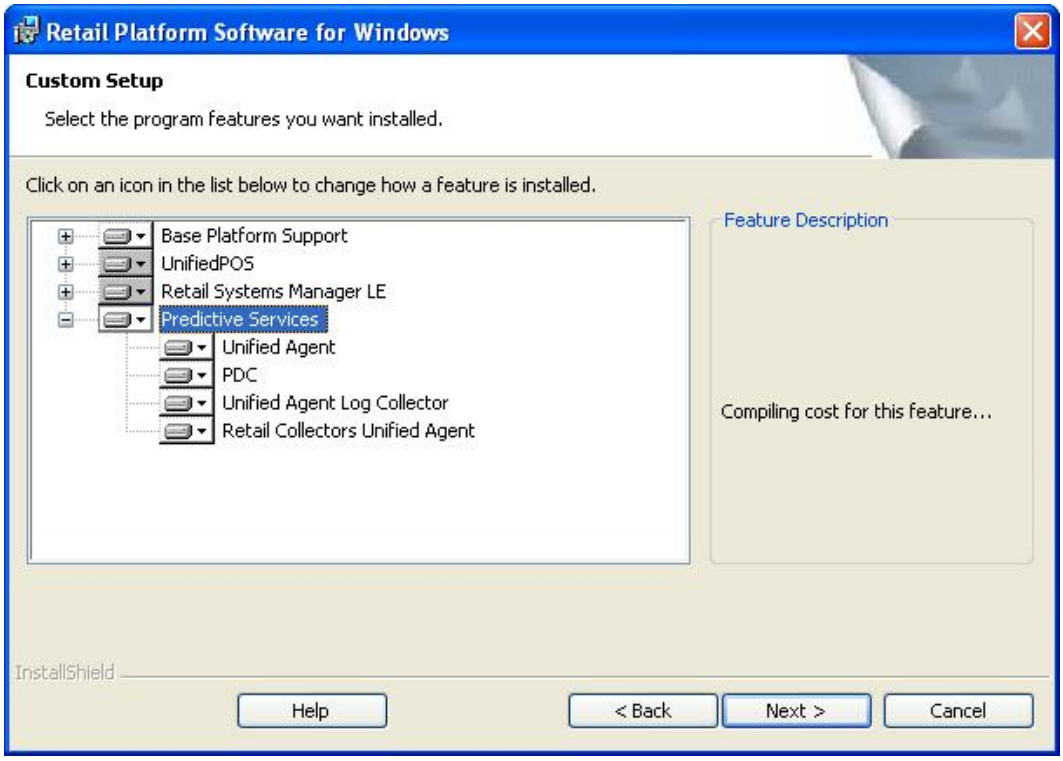
Note: The Predictive Services installation options are no longer available in the RPSW 4.0.1.x and later releases. For these releases, installing the Predictive Services software is possible through a separate LPIN (D370–0955–0100).

Before installing the Predictive Services feature, make sure to install the following software packages on the terminal:

- .Net Framework 3.5 or later
- .Net 2.0 Framework Service Pack 2
- `3rdParty.msi`
- Visual Studio 2005 C Runtime Libraries

The following are the components of the Predictive Services software:

- Unified Agent Service
- Problem Determination Collection (PDC)
- Unified Agent Log Collector
- Retail Collectors for Unified Agent



The UALog Collector component is installed as part of the RPSW installation package.

The packages of the other three components, Unified Agent Service, PDC, and Retail Collectors for Unified Agent, are extracted and ready for installation after the RPSW install process. These packages are found in the NCR APTRA directory of the install folder.

Example: `C:\Program Files\NCR APTRA`

After installing RPSW, install the following three components manually in the following order:

- PDC
- Unified Agent Service
- Retail Collectors for Unified Agent

Installing the Certificates

Install the following certificates to permit the Unified Agent to communicate with the appropriate servers within the NCR network:

- `NCR_IT_Services_CA.crt`
- `ua_css_extranet_prod_v2_192.127.224.16.crt`

To install these certificates, open the command prompt and type the following command lines:

- `Certmgr /add /all NCR_IT_Services_CA.crt /s /r LocalMachine root`
- `Certmgr /add /all NCR_IT_Services_CA.crt /s /r LocalMachine my`
- `Certmgr /add /all ua_css_extranet_prod_v2_192.127.224.16.crt /s /r LocalMachine root`
- `Certmgr /add /all ua_css_extranet_prod_v2_192.127.224.16.crt /s /r LocalMachine my`

Installing Problem Determination Collection (PDC)

To install the PDC component, open the command prompt and type either of the following options depending on the type of installation you want:

- For an interactive install:

  ```
  msiexec /i "PDC.msi"
  ```

- For a silent install:

  ```
  msiexec /i "PDC.msi" /q
  ```

Installing Unified Agent Service

To install the Unified Agent Service component, open the command prompt and type either of the following options depending on the type of installation you want:

- For an interactive install:

```
msiexec /i "UARefWS.msi"
```

- For a silent install:

```
msiexec /i "UARefWS.msi" /q
```

Note: To install the Unified Agent Service package on a Windows 7 operating system configuration, you must launch the install with administrative privileges.

Installing Retail Collectors for Unified Agent

To install the Retail Collectors for Unified Agent component, open the command prompt and type either of the following options depending on the type of installation you want:

- For an interactive install:

```
msiexec /i "Retail Collectors for Unified Agent.msi"
```

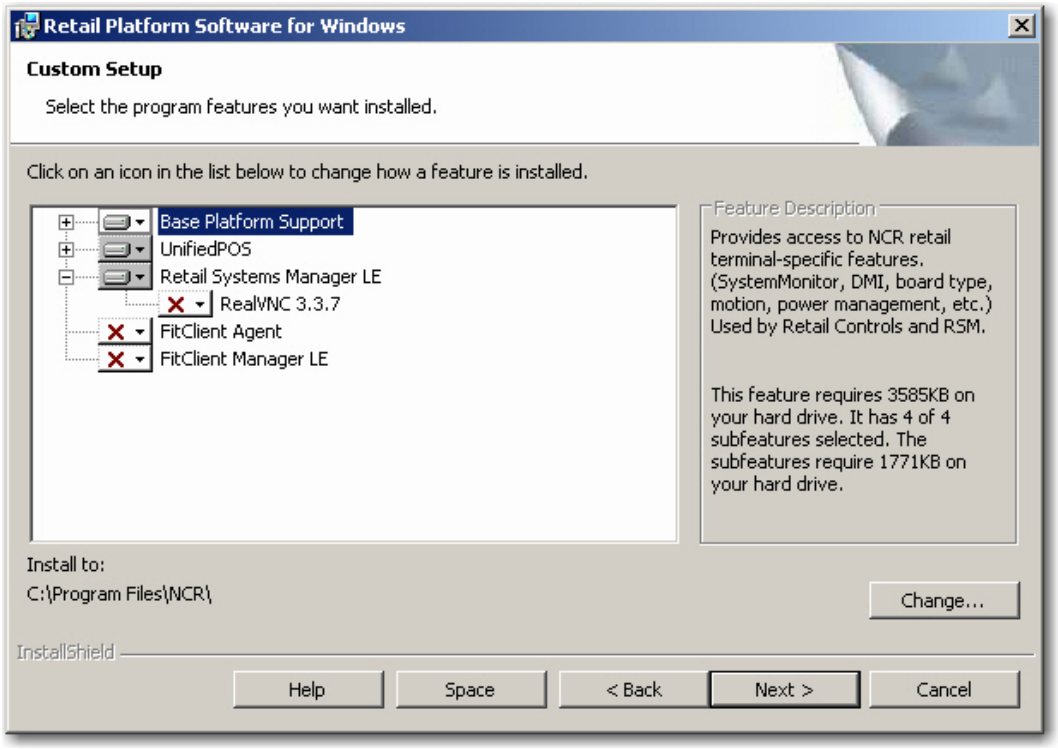
- For a silent install:

```
msiexec /i "Retail Collectors for Unified Agent.msi" /q CONFIGURE_
DEVICE_TYPE=POS
```

Note: You can use the value “SSCO” instead of “POS” for the CONFIGURE_DEVICE_TYPE parameter during the silent install.

FitClient

FitClient is used only on legacy terminals. It is not supported in RPSW 4.0 and later versions. The setup displays the following window during the custom installation for RPSW versions that are below 4.0.



FitClient Agent

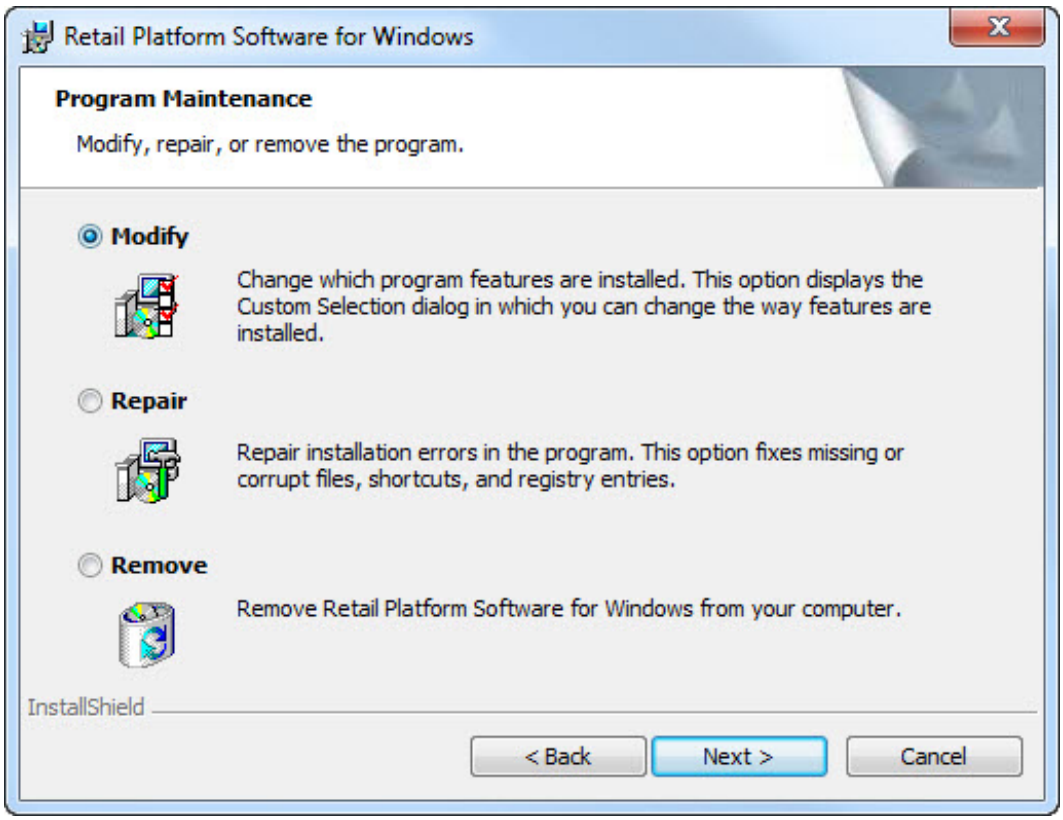
The FitClient Agent feature provides communication and synchronization with the FitClient Manager Server. FitClient Agent is only available through a custom install because FitClient Manager has been replaced by RSM.

FitClient Manager LE

FitClient Manager LE provides local configuration and diagnostic capabilities. FitClient is not being updated with new features that are being incorporated into RSM LE. RSM LE is the replacement product for FitClient LE. FitClient LE is only available if you select a Custom Install.

Post–installation Information

If you run the installation program, and the RPSW is already installed on the system, the system displays this window with the following options:



- Modify—select to add or remove components.
- Repair—select to replace corrupt files.
- Remove—select to remove all software, such as RSM, OPOS, JavaPOS, and Base Platform, in the current installation.

RPSW MSI Install Parameters

The `.msi` files provide another method to install applications remotely (from the server). This method can be used to install programs that are built for the Microsoft Windows Installer program (`*.msi`).

There is no user interactivity using Remote Install. Therefore, if the application installation program has parameters that require interaction, you must enter these parameters in the Install Parameters field before installing the Retail Platform Software for Windows (RPSW) on the system.

All properties and values are listed in the `Command line parameters for Retail Platform Software for Windows.doc` file on the installation CD.

Creating a Client Image

The addition of RPSW and RSM to the Gold Drive images saves the user from having to install these products individually, but when you incorporate these Gold Drive images with your applications and then wish to distribute them to multiple terminals, some issues on terminal identification must be considered.

Problem

The NCR Retail Platform Software for Windows (RPSW) reads and stores terminal–based DMI information to the hard disk, either in the registry or in a file. The DMI space (firmware on the processor board) contains information, such as Terminal Serial number, class or model, and so forth. This information is critical because it may be the only way of identifying the terminal and its version.

This process works fine when each terminal's hard drive is built up from scratch at that terminal. Now, with the use of drive duplication software, this process has become an issue because the duplicated terminals can get the DMI information of the source terminal where the image was created. Usually, a master disk image is created on a test terminal and then the software on that terminal is imaged on to all the other terminals. The problem occurs the first time the test terminal is rebooted after the RPSW is installed. During this reboot, the DMI information is read and written to disk (this data is not modified on subsequent reboots). When the image is sent to the other terminals, the DMI values on the disk do not match what is actually in DMI on that terminal.

Impact

When this problem occurs, NCR platform software, such as the Retail Systems Manager (RSM) or Command Center, displays incorrect DMI information for any terminals that have been loaded using the image. In addition, the affected terminals will have an unhealthy state when it detects that the board and disk drive DMI information do not match.

Note: If you do not have RSM State–of–Health, check the event log for NCRHAL events, which indicate that the information does not match.

Action

To create a client image, follow these steps:

1. Install RPSW.
2. Install RPSW patches.
3. Configure any RSM Local Edition (LE) settings that are common across terminals, such as the system Custom Tags, peripheral settings, and so forth.

4. Run the NCRSysPrep utility, which is included with RPSW 2.1.1 or later versions.

   The NCRSysPrep utility can be run for the NCR 7402, 7456, 7457, 7458, and newer terminal images. This utility clears out the data on the terminal's hard drive so that the next time the terminal is loaded or rebooted, the data is read from the processor board on the new terminal. The customer can run the NCRSysPrep on each terminal to clear this error, but the best solution is to run NCRSysPrep on the terminal being imaged. If you reboot the terminal after NCRSysPrep is run and the Base Platform software in RPSW runs again, the data on the hard drive is filled in again and you must run NCRSysPrep again.

5. Run Microsoft SysPrep/fbreseal. Do not reboot after this step is done.

Note: It is important that you run NCRSysPrep before you run the Microsoft sysprep/fbreseal.

6. Create the image. To capture or restore an image, refer to the *NCR Partition Image User's Guide* (B005–0000–1641).

Chapter 3: Introduction to RSM LE

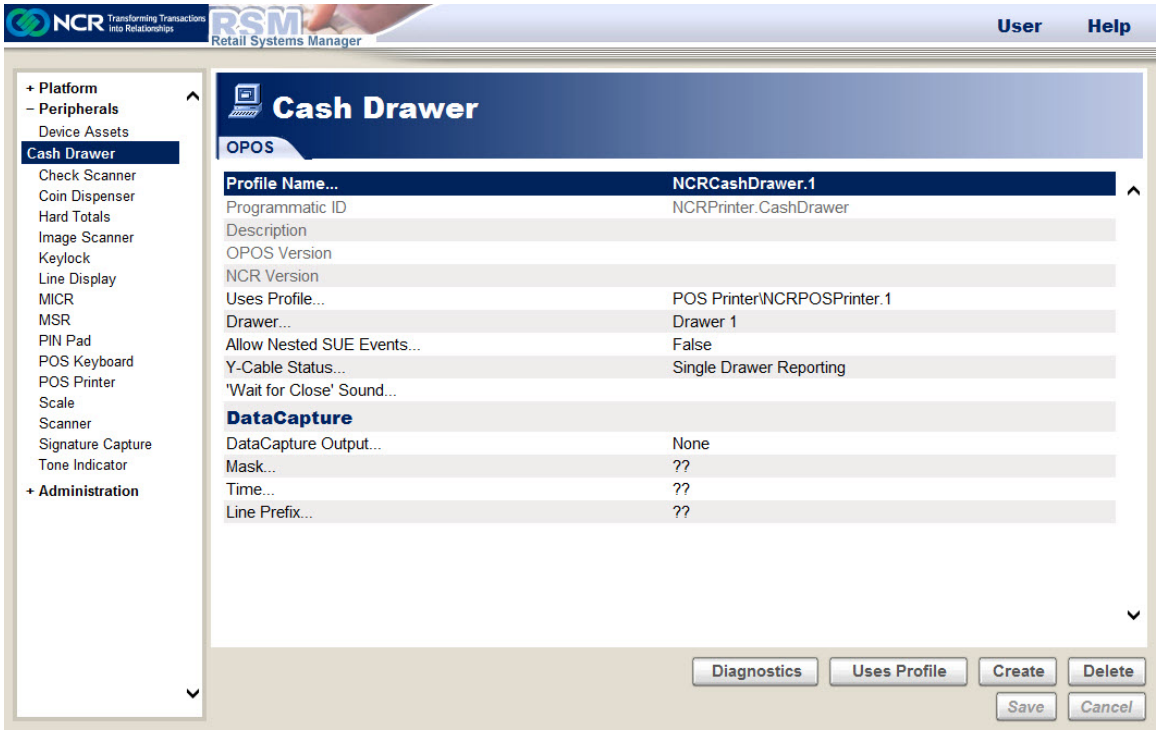
Overview

RSM Local Edition (LE) provides peripheral configuration and local out–of–service diagnostics. If RSM LE is licensed, additional functionalities become available. The following are the characteristics of the RSM LE:

- RSM LE has Every Unit Item (EUI) functionality if there is no RSM license or the RSM license has expired.
- EUI functionality permits you to configure peripherals and run diagnostics only.
- If you are in EUI mode, no logon prompt is displayed when RSM LE starts up.
- Additional functionality is available when you have an RSM license (monitoring and information).
- RSM LE provides SNMP functionality if you are licensed for it.

RSM LE Functionalities

When you start RSM LE in EUI (every unit item) mode, the system displays the following window:



The options available in RSM LE are based on the licensed features. RSM LE normally gets its license from the RSM SE server that it connects to, though it is possible to add an RSM license file to an unmanaged RSM LE system. For more information, refer to *Installing the RSM LE License* on page 61.

RSM LE has EUI functionality when either it has no RSM license or the license has expired. The EUI functionality is typically seen on unmanaged RSM LE systems. The "RSM LE EUI Functionality" and "RSM LE with RSM License" sections describe features that are typically included, but your license file may provide different features.

RSM LE EUI Functionality

If RSM LE does not have an RSM license, the following options are available with EUI functionality:

- Platform—platform devices for your terminal. Some examples include:
  - Audio
  - BIOS
  - Disks
  - Motherboard
  - Network
  - Power States
  - Serial Ports
  - Touch screen
  - Versioning
- Peripherals—OPOS/JavaPOS controls selected during installation. Some examples include:
  - Device Assets
  - Cash Drawer
  - Check Scanner
  - Coin Dispenser
  - Hard Totals
  - Image Scanner
  - Key lock
  - Line Display
  - MICR
  - MSR
  - PIN Pad
  - POS Keyboard
  - POS Printer
  - Scale
  - Scanner
  - Signature Capture
  - Tone Indicator

- Administration
  - RSM Services
    - Customer Number
    - RSM Managed—Enabled or Disabled. Set to Disabled for an unmanaged system.
  - Licensing
    - Current User
    - License File
    - License Expiration
  - Data Capture
    - Configuration—Simple or Advanced
      - Simple
        - Default Setting—No Logging, Error Logging, or Full Logging
      - Advanced
        - Trace Mask Settings
        - Level Mask Settings
    - The list of modules that support data capture. The type of logging can be changed for each one of the devices.

RSM LE with RSM License

If an RSM license is used, additional functionality is provided in RSM LE. The functionality available depends on the license, but it may include the following functionalities:

- Monitor
  - State Of Health
  - Connectivity
  - Event Logs
  - Tallies
  - Processes
  - Services
- Platform
  - Audio
  - BIOS
  - Disks
  - Memory
  - Motherboard
  - Network
  - Operating System
  - Power States
  - Serial Ports
  - Software
  - Touchscreen
  - Versioning
- Peripherals—the same as available for EUI RSM LE
- Administration
  - RSM Services
  - Licensing
  - Alerting
  - Critical Events
  - Tally Thresholds
  - OS Monitoring
  - Data Capture

Note: If Command Center is used, OS Monitoring is automatically licensed even if an RSM license file is not installed.

Logging on to RSM LE

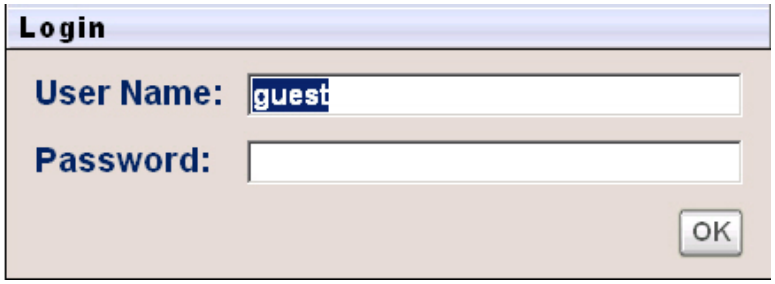
To log on to RSM LE, follow these steps:

1. Start RSM LE by performing any of the following:
   - Select the desktop icon for RSM LE.
   - Open a browser on the system and type the path to the RSM website.

     Example: `C:\Prgram Files\NCR\RSM\Website\ConsoleLE.htm`

   If RSM is operating in Every Unit Item (EUI) mode, you are not prompted for a logon window, but you are automatically logged on with privileges to configure peripherals and run diagnostics only.

   If RSM LE is managed and licensed, the Login window is displayed.



2. Enter the **User Name** and **Password**.

Note: The following are the logon types when accessing RSM LE:

- NCRRetailer—permits access to the features you have licensed. You obtain the User Name and Password information from NCR. The NCRRetailer logon has a password that changes daily.
- NCRService—used by NCR personnel. It has full access to all the features in the system. The NCRService logon has a password that changes daily.
- Guest—does not require a password, but only gives you read–only access to licensed features.

3. Select **OK**. The main window is displayed.

The RSM LE user interface displays the different available features. These features are discussed in the next sections.

Note: The functionality present is based on the license file, and the unlicensed features are not available.

Installing the RSM LE License

The license file must be installed at the highest RSM tier. When you install the license file at the highest tier, it is automatically distributed to the lowest tiers. Within the RSM user interface, the ability to upload license files and configure license settings is restricted to the highest tier of RSM. If RSM LE is managed by an RSM server, the license file must be applied at the highest server tier. If RSM LE is unmanaged, you can install an RSM license at RSM LE to use RSM LE licensed features.

To install an RSM LE license, perform the following:

1. Set the Customer Number.
2. Add the license file.

Setting the Customer Number

The Customer Number is unique for each RSM customer and is required to activate an RSM license.

Note: If the RSM LE is managed, the Customer Number can only be configured at an RSM server and cannot be changed at the RSM LE tier.

To set the Customer Number at an unmanaged RSM LE, follow these steps:

1. In the RSM LE user interface, select **Administration→RSM Services**.
2. Select **Customer Number** and then enter your Customer Number.
3. Select **Save** to save the new Customer Number value.

Adding the License file

You can add the license file through the following:

- through the RSM LE user interface (UI)
- through manual copying

Note: Only one customer license file may be present. If replacing the existing license file with a new one, delete the old customer license file.

Warning: Delete only the customer–specific license file. Do not delete the `default.dat` or `cepriv.dat` license files to avoid triggering an installation repair.

Adding an RSM LE license file through the UI

To add an RSM LE license file through the user interface, follow these steps:

1. In the RSM LE user interface, select **Administration→Licensing**.
2. Select **Add** and then browse for and select the license file.
3. Select **Copy**. If the file is successfully uploaded, a message appears accordingly.

Adding an RSM LE license file through manual copying

For RSM 4.0 and later releases, place the license file in the following path:

%ALLUSERSPROFILE%\NCR\RSM\Website\XML

The %ALLUSERSPROFILE% variable is an environment variable that points to different locations depending on the operating system.

Note: For RSM releases earlier than 4.0, place the license file in the C:\Program Files\NCR\RSM\Website\XML directory.

Chapter 4: Using the RSM LE

Overview

This chapter provides information on how to use RSM LE and its different components:

- Monitor
- Administration
- Peripherals
- Platform

Note: The functionality present is based on the license file. The unlicensed features are not available.

Using the Monitor section

The Monitor section of the RSM LE user interface displays the following components:

- State of Health
- Connectivity
- Event Logs
- Tallies
- Processes
- Services

Note: The Monitor section is not included in the RSM LE EUI functionality without a license.

State of Health

The State of Health screen is the first screen that displays after you log on.

RSM has the ability to determine the state of health of managed components. State of health determination is derived using events logged by managed components. These events are then driven through a finite state machine to determine the current state of health. NCR terminals and peripherals have been instrumented to log the events needed to drive this state machine and permit RSM to determine their current state of health.

State of Health is a key component of RSM and therefore is easily visible from the RSM user interface. At RSM LE, State of Health monitors the peripherals attached to the system, and reports problems that are encountered from the platform devices.

The State of Health screen displays information about the current status of a system such as the following alerts:

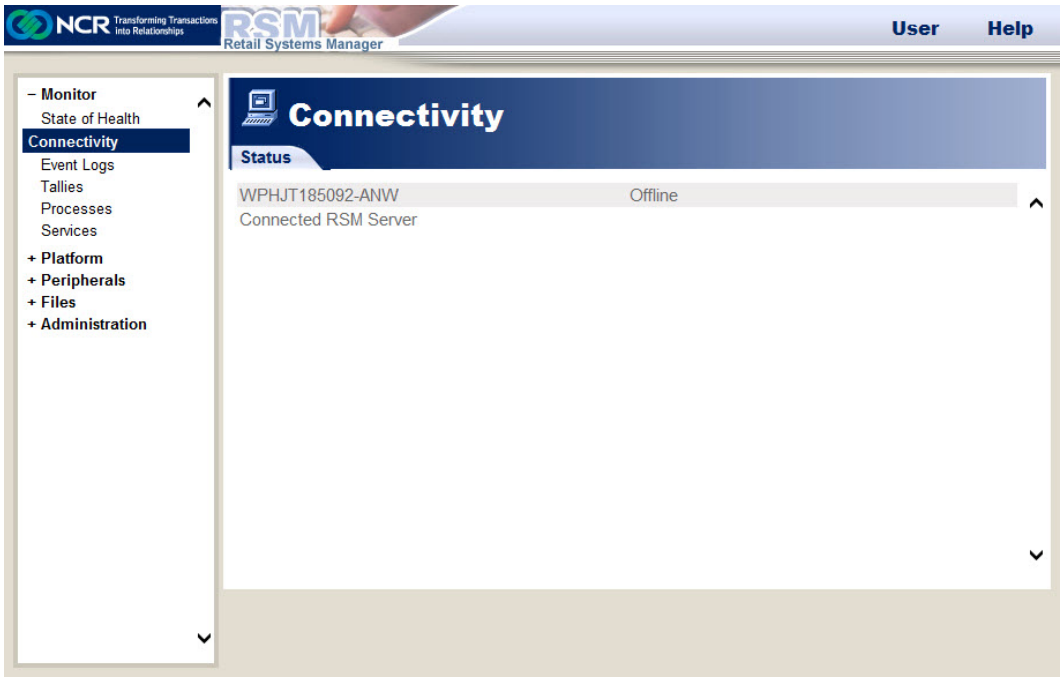
- State Of Health Alerts—refers to the alerts that are defined by the information provided by the Retail Controls, Platform devices, or RSM software. State Of Health does not require that the Alert configuration parameters be defined. The State of Health alerts include the following alerts:
  - Healthy Alerts
  - Attention Soon Alerts
  - Attention Now Alerts
- Event Alerts—refers to the alerts that are set up for events that are specific to an application or device. Event alerts are set up at the System level and include the following alerts:

- Informational Events Alerts
- Warning Events Alerts
- Error Events Alerts

- Tally Alerts—refers to the alerts that contain information on the counts of the number of times a certain operation is performed for a certain device. Tally alerts are set up at the System level and include the following alert:
  - Tally Threshold Alerts

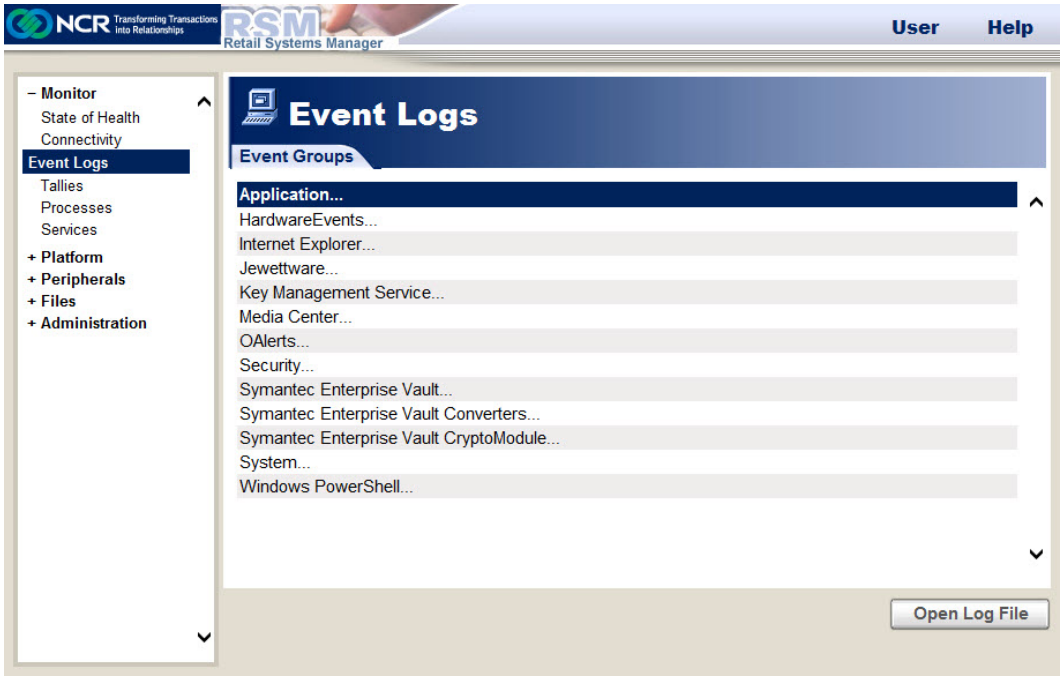
Connectivity

The Connectivity screen displays the current connection status to RSM SE or PXE Image Loader.



Event Logs

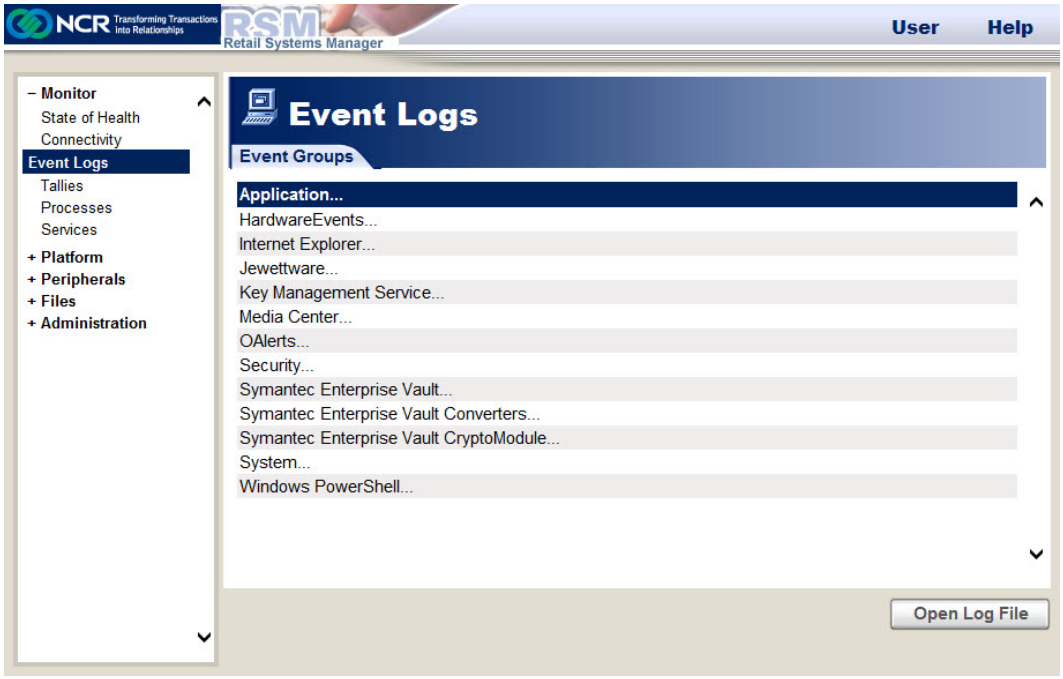
The Event Logs section displays significant events that occurred in the system that the RSM application needs to notify the users about. RSM provides you the functionality to view all the events of all the event log types available in the system.



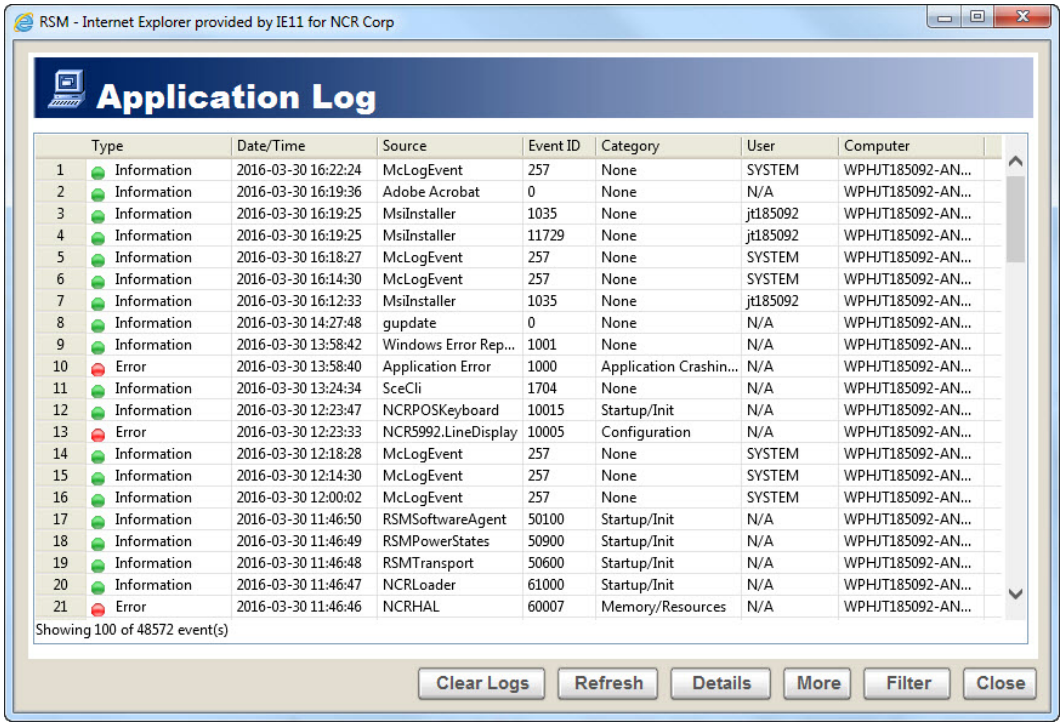
Viewing Events

To view the events of a system, follow these steps:

1. On the RSM Console, select **Monitor→Event Logs**. The Event Logs section displays the available event log types.



2. Select the event log type you want to view. The RSM Event Viewer displays the events of the selected event log type. In this example, Application Log is selected.



	Type	Date/Time	Source	Event ID	Category	User	Computer
1	Information	2016-03-30 16:22:24	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
2	Information	2016-03-30 16:19:36	Adobe Acrobat	0	None	N/A	WPHJT185092-AN...
3	Information	2016-03-30 16:19:25	MsiInstaller	1035	None	jt185092	WPHJT185092-AN...
4	Information	2016-03-30 16:19:25	MsiInstaller	11729	None	jt185092	WPHJT185092-AN...
5	Information	2016-03-30 16:18:27	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
6	Information	2016-03-30 16:14:30	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
7	Information	2016-03-30 16:12:33	MsiInstaller	1035	None	jt185092	WPHJT185092-AN...
8	Information	2016-03-30 14:27:48	gupdate	0	None	N/A	WPHJT185092-AN...
9	Information	2016-03-30 13:58:42	Windows Error Rep...	1001	None	N/A	WPHJT185092-AN...
10	Error	2016-03-30 13:58:40	Application Error	1000	Application Crashin...	N/A	WPHJT185092-AN...
11	Information	2016-03-30 13:24:34	SceCli	1704	None	N/A	WPHJT185092-AN...
12	Information	2016-03-30 12:23:47	NCRPOSKeyboard	10015	Startup/Init	N/A	WPHJT185092-AN...
13	Error	2016-03-30 12:23:33	NCR5992.LineDisplay	10005	Configuration	N/A	WPHJT185092-AN...
14	Information	2016-03-30 12:18:28	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
15	Information	2016-03-30 12:14:30	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
16	Information	2016-03-30 12:00:02	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
17	Information	2016-03-30 11:46:50	RSMSoftwareAgent	50100	Startup/Init	N/A	WPHJT185092-AN...
18	Information	2016-03-30 11:46:49	RSMPowerStates	50900	Startup/Init	N/A	WPHJT185092-AN...
19	Information	2016-03-30 11:46:48	RSMTransport	50600	Startup/Init	N/A	WPHJT185092-AN...
20	Information	2016-03-30 11:46:47	NCRLoader	61000	Startup/Init	N/A	WPHJT185092-AN...
21	Error	2016-03-30 11:46:46	NCRHAL	60007	Memory/Resources	N/A	WPHJT185092-AN...

Note: The RSM Event Viewer user interface is designed to look and function similar to the Windows Event Viewer user interface.

The RSM Event Viewer displays all the event logs of the selected event log type in a table with the following event data:

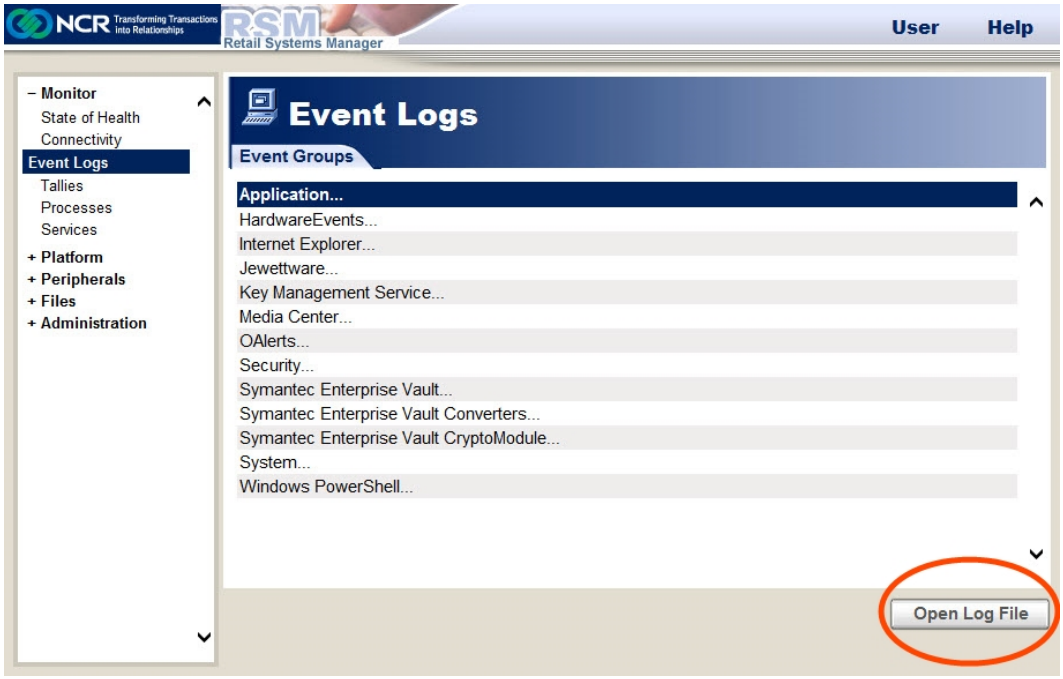
- Type
- Date/Time
- Source
- Event ID
- Category
- User
- Computer

3. Select **More** to view more events in the RSM Event Viewer.
4. Select **Close** to close the RSM Event Viewer.

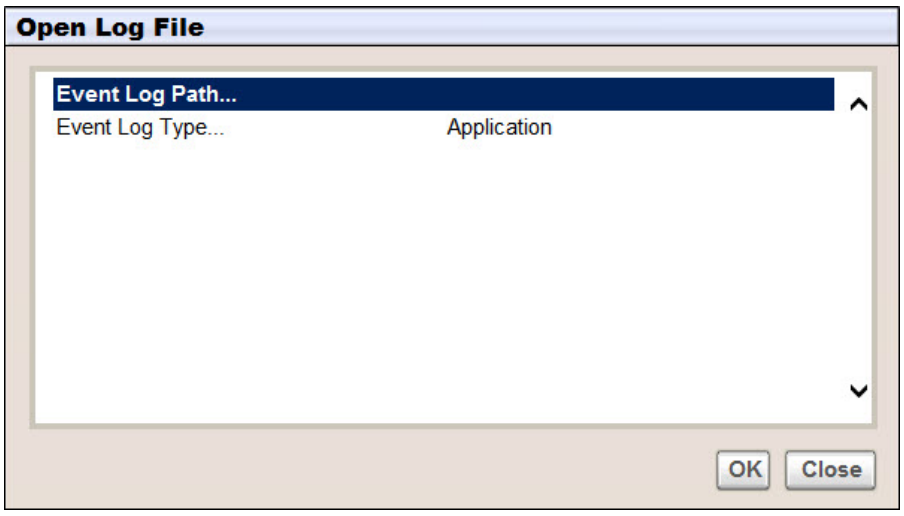
Viewing Exported Event Logs

The RSM application provides the functionality to view the events of an exported event log. To view the events of an exported event log, follow these steps:

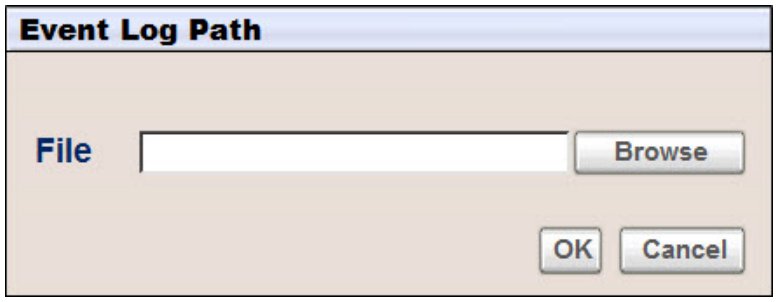
1. On the Event Logs section of the RSM Console, select **Open Log File**.



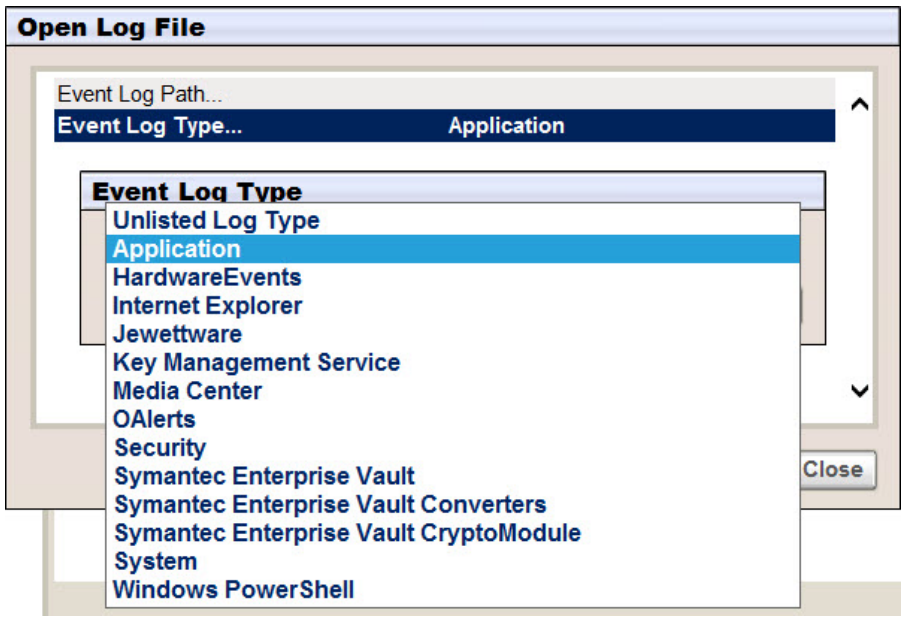
2. The system displays the Open Log File window. Double–click **Event Log Path**.



3. The system displays the Event Log Path window. Browse for and select the event log file you want to view, and then select **OK**.



4. On the Open Log File window, double–click **Event Log Type**. The system displays the Event Log Type window.



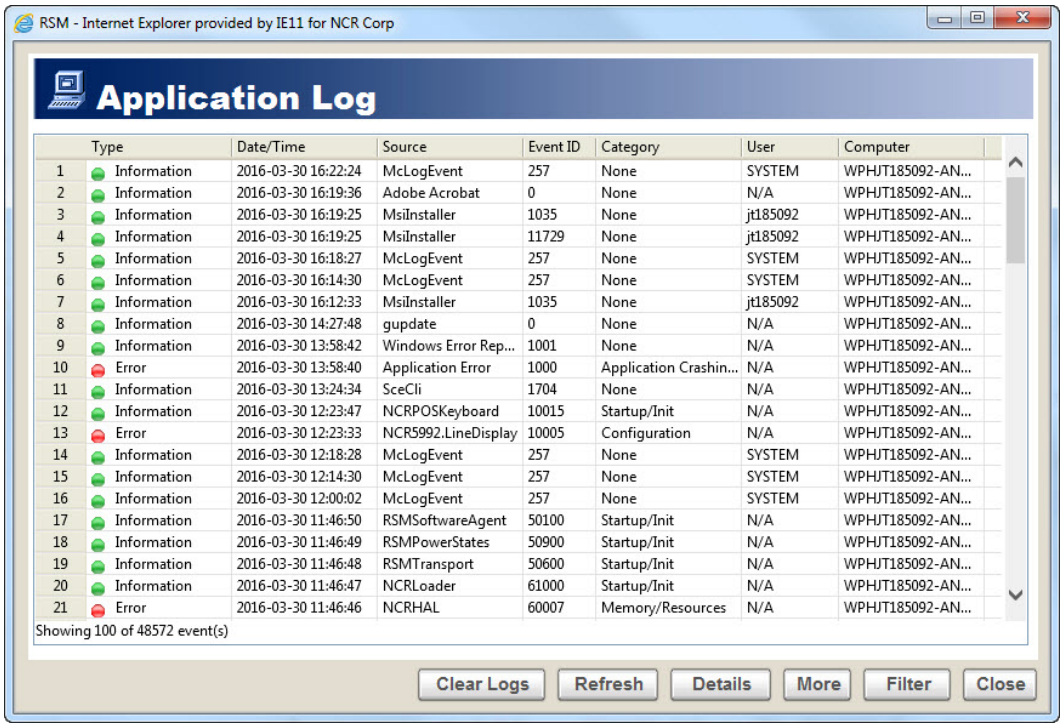
5. Select the Event Log Type from the drop–down list, and then select **OK**.
6. Select **OK** in the Open Log File window. The RSM Event Viewer displays the events of the exported log file.

Note: You cannot view `.evtx` files exported from newer operating systems, such as Windows 7, on operating systems that do not support `.evtx` files.

Viewing Event Details

To view the details of each of the events displayed in the RSM Event Viewer, follow these steps:

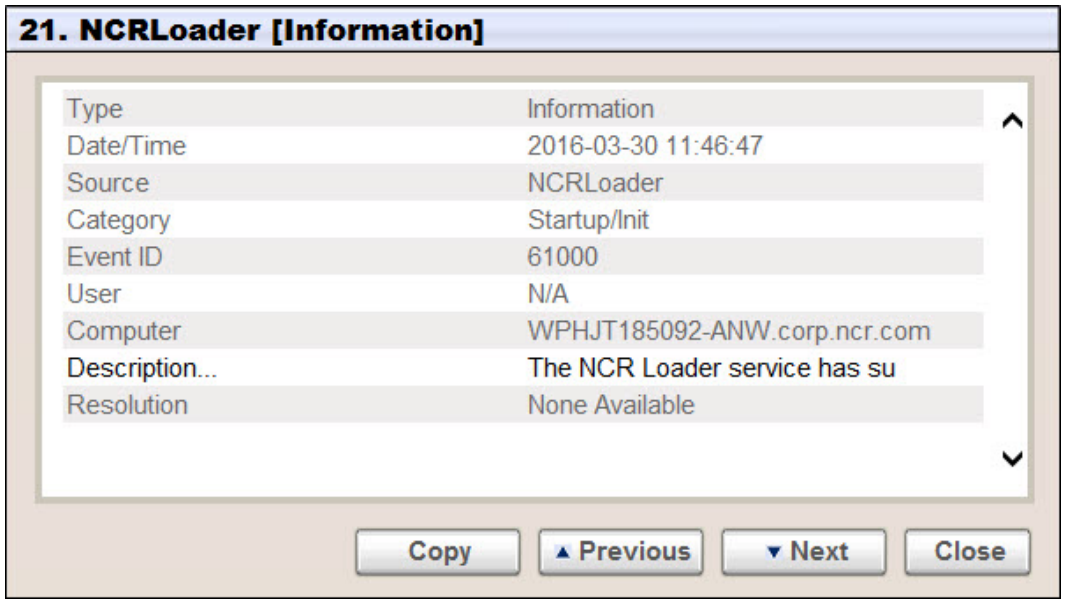
1. On the Event Logs section of the RSM Console, double–click the event log type you want to view. In this example, Application Log is selected.



	Type	Date/Time	Source	Event ID	Category	User	Computer
1	Information	2016-03-30 16:22:24	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
2	Information	2016-03-30 16:19:36	Adobe Acrobat	0	None	N/A	WPHJT185092-AN...
3	Information	2016-03-30 16:19:25	MsiInstaller	1035	None	jt185092	WPHJT185092-AN...
4	Information	2016-03-30 16:19:25	MsiInstaller	11729	None	jt185092	WPHJT185092-AN...
5	Information	2016-03-30 16:18:27	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
6	Information	2016-03-30 16:14:30	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
7	Information	2016-03-30 16:12:33	MsiInstaller	1035	None	jt185092	WPHJT185092-AN...
8	Information	2016-03-30 14:27:48	gupdate	0	None	N/A	WPHJT185092-AN...
9	Information	2016-03-30 13:58:42	Windows Error Rep...	1001	None	N/A	WPHJT185092-AN...
10	Error	2016-03-30 13:58:40	Application Error	1000	Application Crashin...	N/A	WPHJT185092-AN...
11	Information	2016-03-30 13:24:34	SceCli	1704	None	N/A	WPHJT185092-AN...
12	Information	2016-03-30 12:23:47	NCRPOSKeyboard	10015	Startup/Init	N/A	WPHJT185092-AN...
13	Error	2016-03-30 12:23:33	NCR5992.LineDisplay	10005	Configuration	N/A	WPHJT185092-AN...
14	Information	2016-03-30 12:18:28	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
15	Information	2016-03-30 12:14:30	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
16	Information	2016-03-30 12:00:02	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
17	Information	2016-03-30 11:46:50	RSMSoftwareAgent	50100	Startup/Init	N/A	WPHJT185092-AN...
18	Information	2016-03-30 11:46:49	RSMPowerStates	50900	Startup/Init	N/A	WPHJT185092-AN...
19	Information	2016-03-30 11:46:48	RSMTransport	50600	Startup/Init	N/A	WPHJT185092-AN...
20	Information	2016-03-30 11:46:47	NCRLoader	61000	Startup/Init	N/A	WPHJT185092-AN...
21	Error	2016-03-30 11:46:46	NCRHAL	60007	Memory/Resources	N/A	WPHJT185092-AN...

2. The system displays the RSM Event Viewer. Perform any of the following:
   - Select the event from the RSM Event Viewer, and then select **Details**.
   - Double–click the event from the RSM Event Viewer.

The system displays the Event Details window. In this example, RSMPowerStates is selected.



The Event Details window displays the following information:

Information	Refers to
Type	The type of event. The event types are the following: • Error • Warning • Information • Success Audit • Failure Audit
Date/Time	The date and time when the event occurred.
Source	The software that logged the event.
Category	The classification of the event.
Event ID	The number that identifies the particular event for this source.
User	The name of the user when the event occurred.
Computer	The name of the computer where the event occurred.
Description	The description of the event.
Resolution	The details about the meaning and actions to take regarding the event. The system displays the resolution information only if you have the license to view resolution information.

Information	Refers to
Binary Information	The binary information of the selected event. Binary information displays only when it is available for the selected event. The following binary information displays when available: • Data Size • Byte Data • Word Data

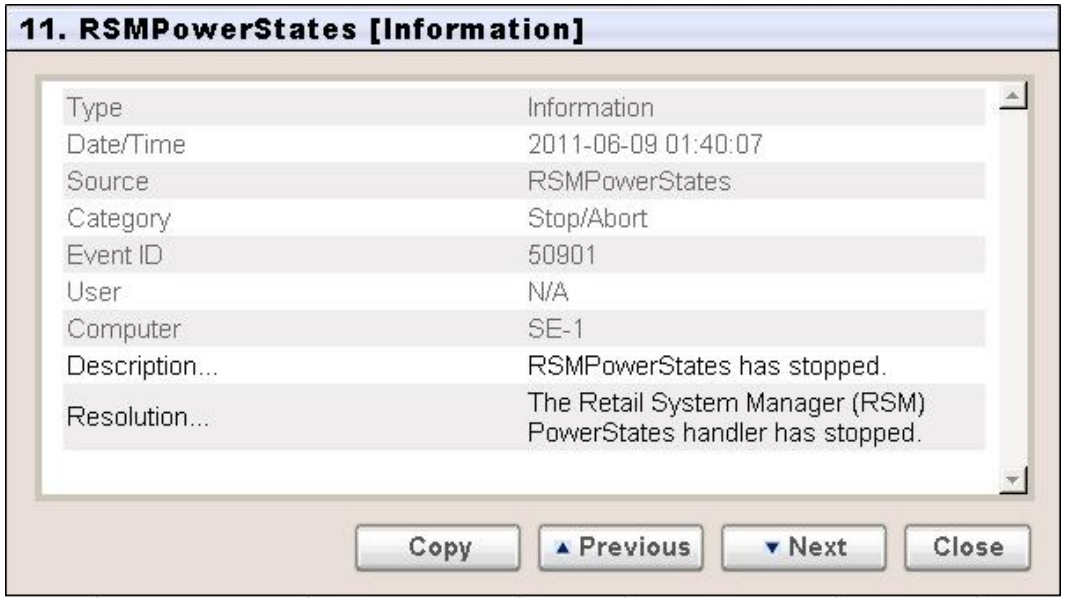
The Event Details window displays the following options:

Option	Used To
Copy	Copy event details to clipboard. For more information, refer to *Copying Event Details to Clipboard* on the next page.
Previous	Display the event details of the event that comes before the currently displayed event as listed in the RSM Event Viewer.
Next	Display the event details of the event that comes next to the currently displayed event as listed in the RSM Event Viewer.
Close	Close the Event Details window.

Copying Event Details to Clipboard

To copy the event details that display in the Event Details window to the clipboard, follow these steps:

1. On the Event Details window, select **Copy**.

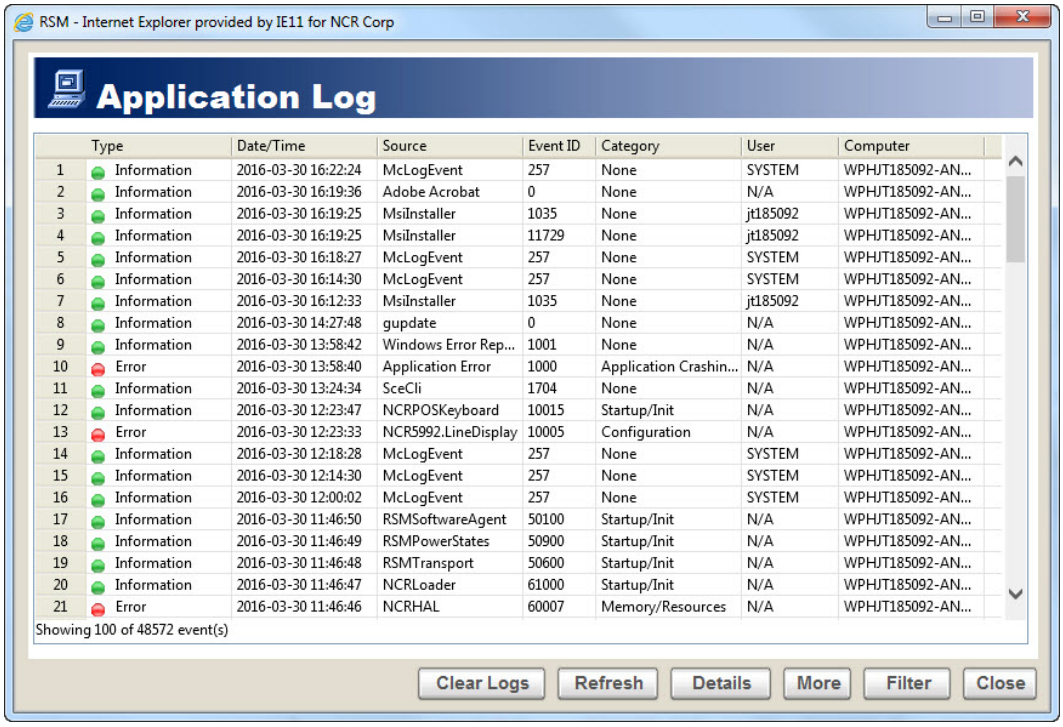


2. Open an editor, such as Notepad.
3. Select **Ctrl+V** or **Edit→Paste** to paste the event details on the editor.

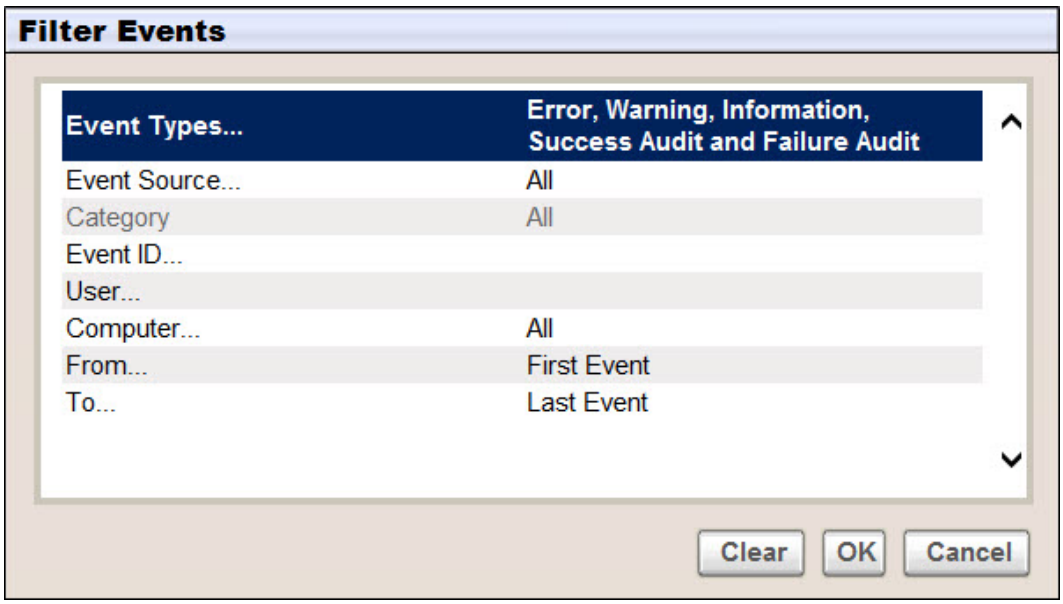
Filtering Events

You can filter the events in the RSM Event Viewer to display a subset of events. To filter events in the RSM Event Viewer, follow these steps:

1. On the Event Logs section of the RSM Console, double–click the event log type you want to view. In this example, Application Log is selected.
2. The system displays the RSM Event Viewer. Select **Filter**.



The system displays the Filter Events window.



3. Filter the events displayed in the RSM Event Viewer according to the following event information:
   - Event Type
   - Event Source
   - Category
   - Event ID
   - User
   - Computer
   - From
   - To
4. Select **OK**. The RSM Event Viewer then displays the events according to the filter criteria you selected.

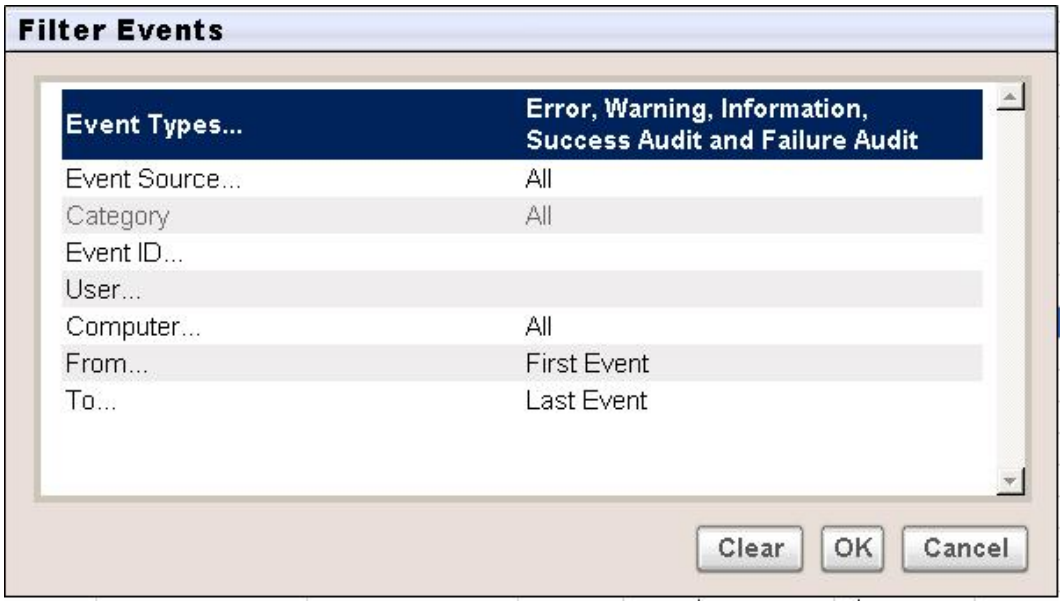
Filtering Events by Date and Time

You can filter events in the RSM Event Viewer by date and time through the From and To options in the Filter Events window. You can filter events by date and time to display according to any of the following:

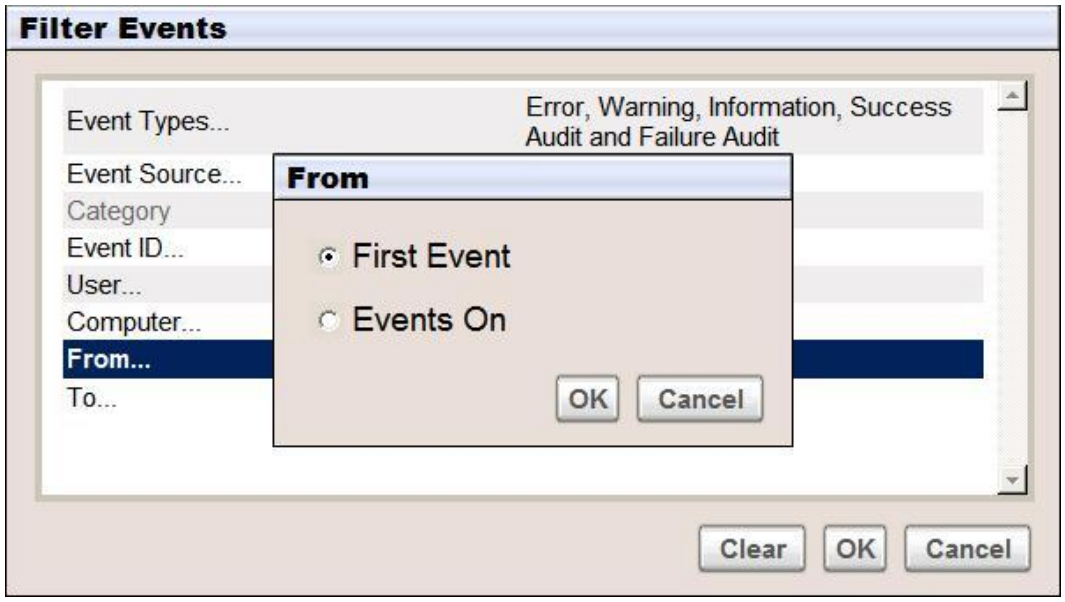
- From the first event logged in the system up to the last event logged in the system.
- From the first event logged in the system up to a specific date and time.
- From a specific date and time up to the last event logged in the system.
- From a specific date and time up to another date and time.

To filter events by date and time, follow these steps:

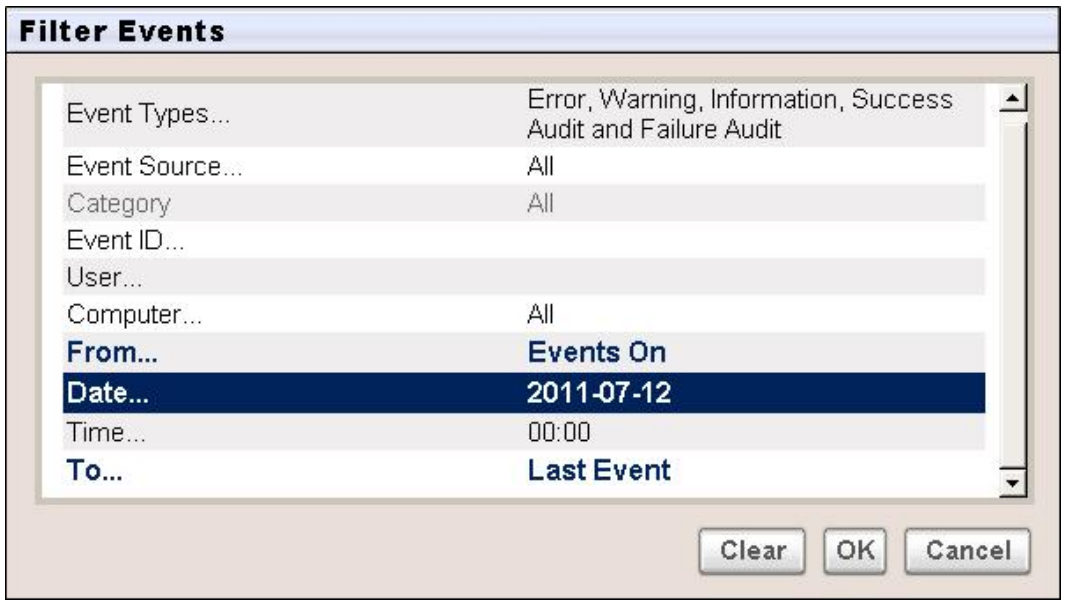
1. On the Filter Events window, double–click **From**.



2. The system displays the From window. Select whether you want to filter from the **First Event** or from the **Events On** a specific date and time.

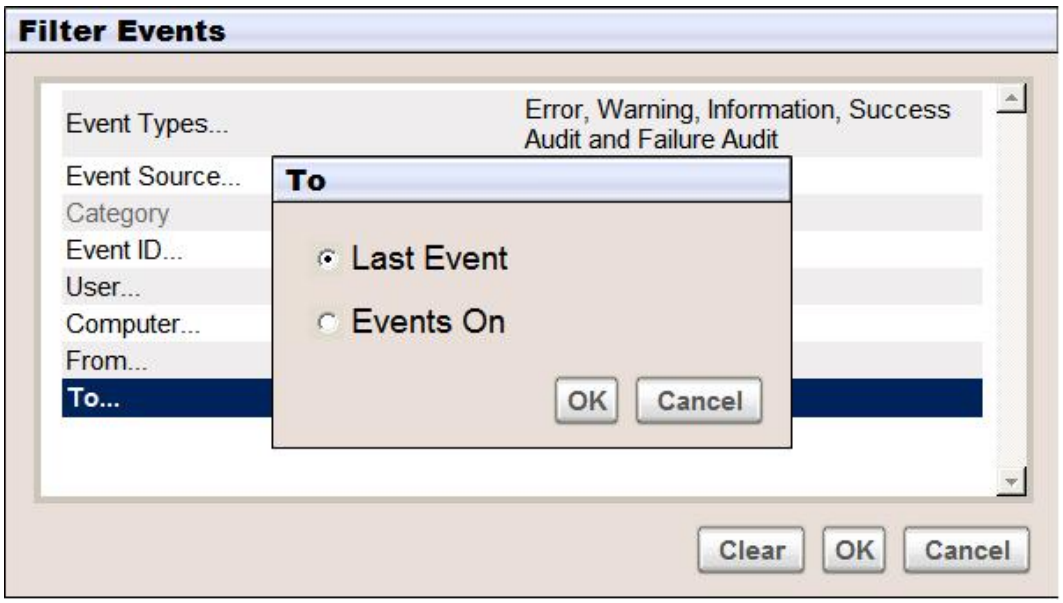


3. Select **OK**. If you selected Events On, the Filter Events window additionally displays the Date and Time options.



4. Select the **Date** and the **Time** from when the events will be filtered.

5. Double–click **To**. The system displays the To window.

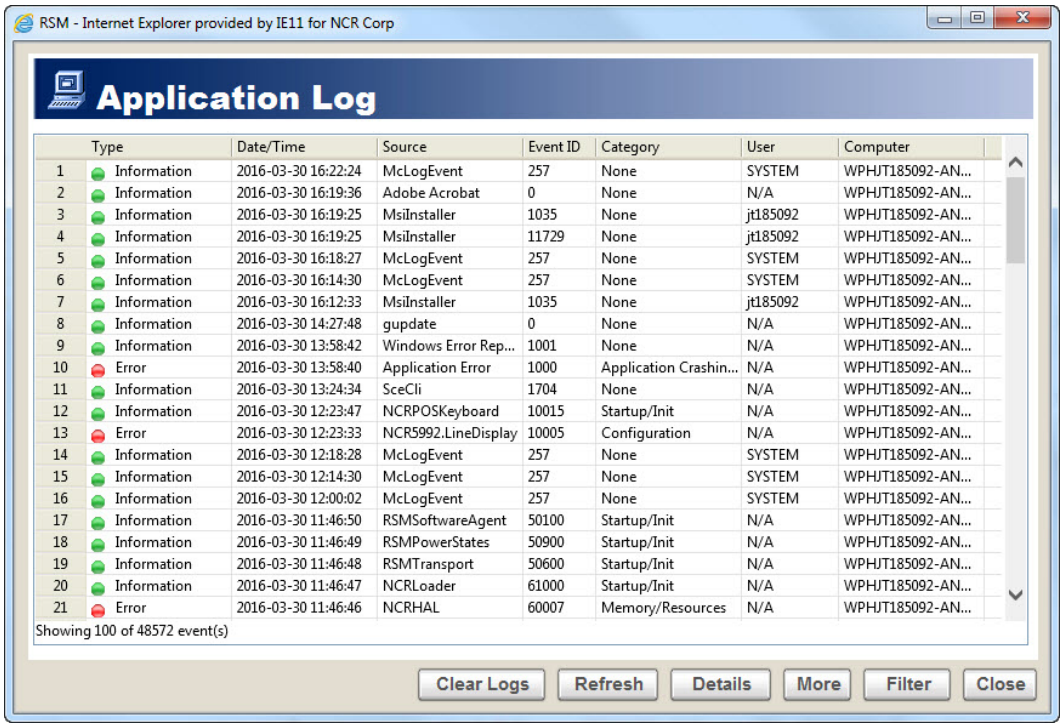


6. Select whether you want to filter up to the **Last Event** or up to the **Events On** a specific date and time.
7. Select **OK**. If you selected Events On, the Filter Events window additionally displays the Date and Time options.
8. Select the **Date** and the **Time** of up to when the events will be filtered.
9. Select **OK**. The RSM Event Viewer then displays the events according to the filter criteria you selected.

Updating Event Logs

While you are viewing the events in the RSM Event Viewer, the RSM application does not update the information that displays in the RSM Event Viewer unless you refresh it.

Select **Refresh** in the RSM Event Viewer to update the information with new events.



	Type	Date/Time	Source	Event ID	Category	User	Computer
1	Information	2016-03-30 16:22:24	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
2	Information	2016-03-30 16:19:36	Adobe Acrobat	0	None	N/A	WPHJT185092-AN...
3	Information	2016-03-30 16:19:25	MsiInstaller	1035	None	jt185092	WPHJT185092-AN...
4	Information	2016-03-30 16:19:25	MsiInstaller	11729	None	jt185092	WPHJT185092-AN...
5	Information	2016-03-30 16:18:27	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
6	Information	2016-03-30 16:14:30	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
7	Information	2016-03-30 16:12:33	MsiInstaller	1035	None	jt185092	WPHJT185092-AN...
8	Information	2016-03-30 14:27:48	gupdate	0	None	N/A	WPHJT185092-AN...
9	Information	2016-03-30 13:58:42	Windows Error Rep...	1001	None	N/A	WPHJT185092-AN...
10	Error	2016-03-30 13:58:40	Application Error	1000	Application Crashin...	N/A	WPHJT185092-AN...
11	Information	2016-03-30 13:24:34	SceCli	1704	None	N/A	WPHJT185092-AN...
12	Information	2016-03-30 12:23:47	NCRPOSKeyboard	10015	Startup/Init	N/A	WPHJT185092-AN...
13	Error	2016-03-30 12:23:33	NCR5992.LineDisplay	10005	Configuration	N/A	WPHJT185092-AN...
14	Information	2016-03-30 12:18:28	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
15	Information	2016-03-30 12:14:30	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
16	Information	2016-03-30 12:00:02	McLogEvent	257	None	SYSTEM	WPHJT185092-AN...
17	Information	2016-03-30 11:46:50	RSMSoftwareAgent	50100	Startup/Init	N/A	WPHJT185092-AN...
18	Information	2016-03-30 11:46:49	RSMPowerStates	50900	Startup/Init	N/A	WPHJT185092-AN...
19	Information	2016-03-30 11:46:48	RSMTransport	50600	Startup/Init	N/A	WPHJT185092-AN...
20	Information	2016-03-30 11:46:47	NCRLoader	61000	Startup/Init	N/A	WPHJT185092-AN...
21	Error	2016-03-30 11:46:46	NCRHAL	60007	Memory/Resources	N/A	WPHJT185092-AN...

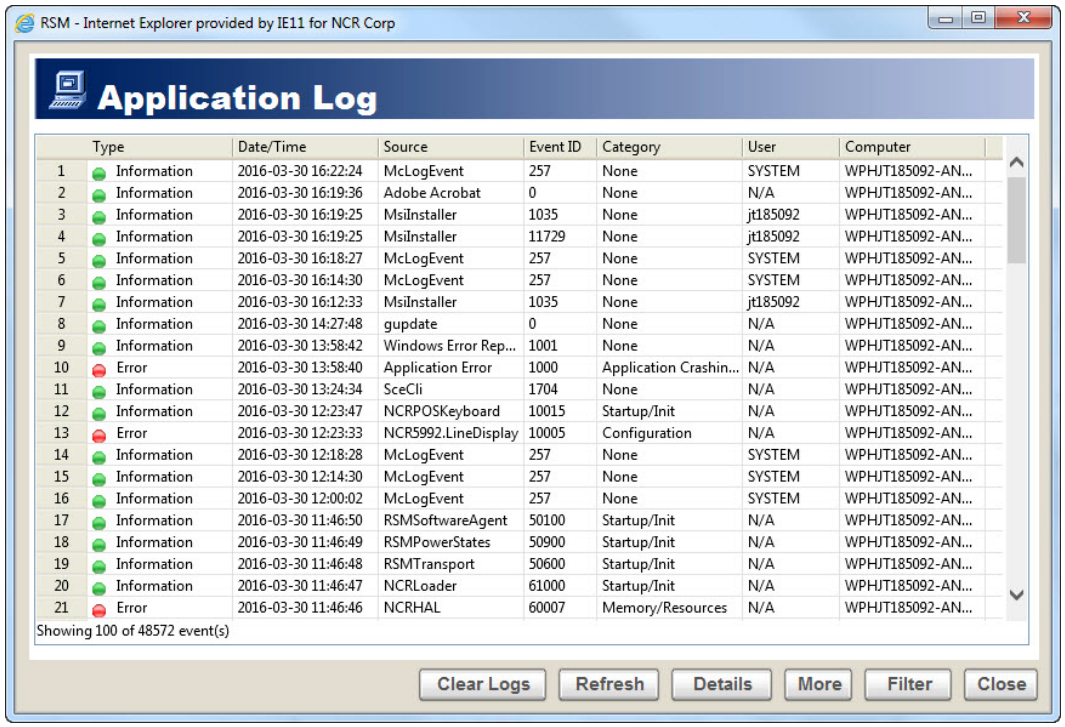
Sorting Event Logs

You can sort the events displayed in the RSM Event Viewer by clicking a specific column header. For example, clicking the Type header sorts the events by type alphabetically.

Clearing Event Logs

You can clear the events of an event log through the RSM Event Viewer. To clear the events of an event log, follow these steps:

1. On the RSM Event Viewer, select **Clear Logs**.



2. The system displays a confirmation window. Select **Yes** to clear the events.

Tallies

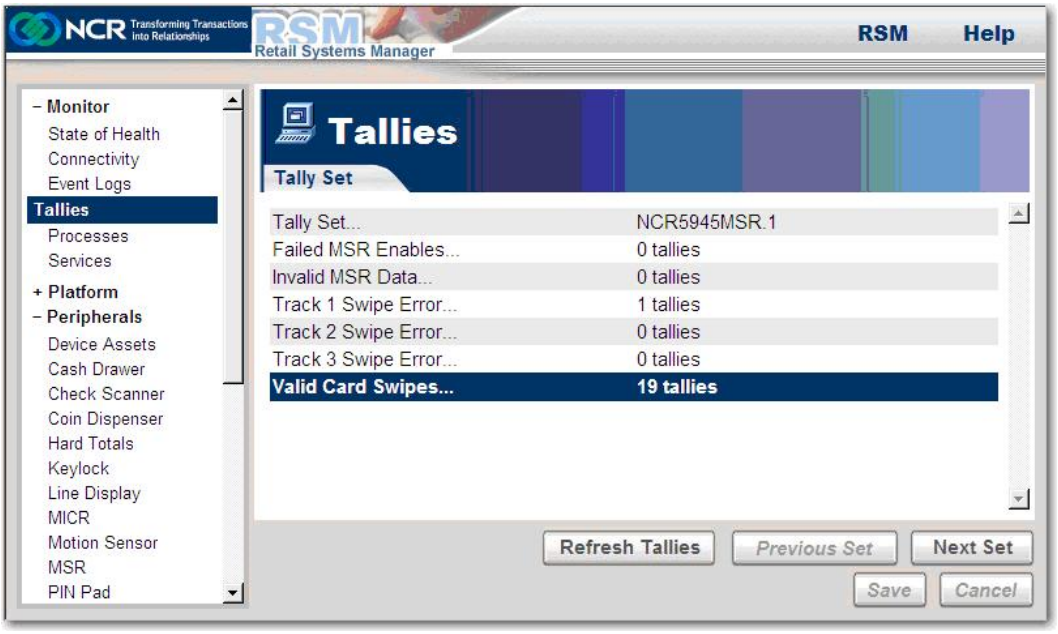
Tallies are available when RPSW is installed and licensed with RSM. Tallies are not available with RSM LE EUI functionality. Tallies are maintained for each peripheral. These tallies are counts of both good and bad information that are incremented until reset by a user. The good tallies are used to compare bad to good counts and assist in proactive maintenance of devices. For a listing of the tallies for the various devices, refer to the OPOS Help file or the *NCR Retail Controls 3.x UPOS User's Guide for Windows* (B005–0000–1619).

In addition to the RPSW peripherals, tallies may also be maintained by any software using the NCR Store Minder tally interface to create and increment tallies. For more information, refer to the RSM SDK LPIN (G370–2800–0100).

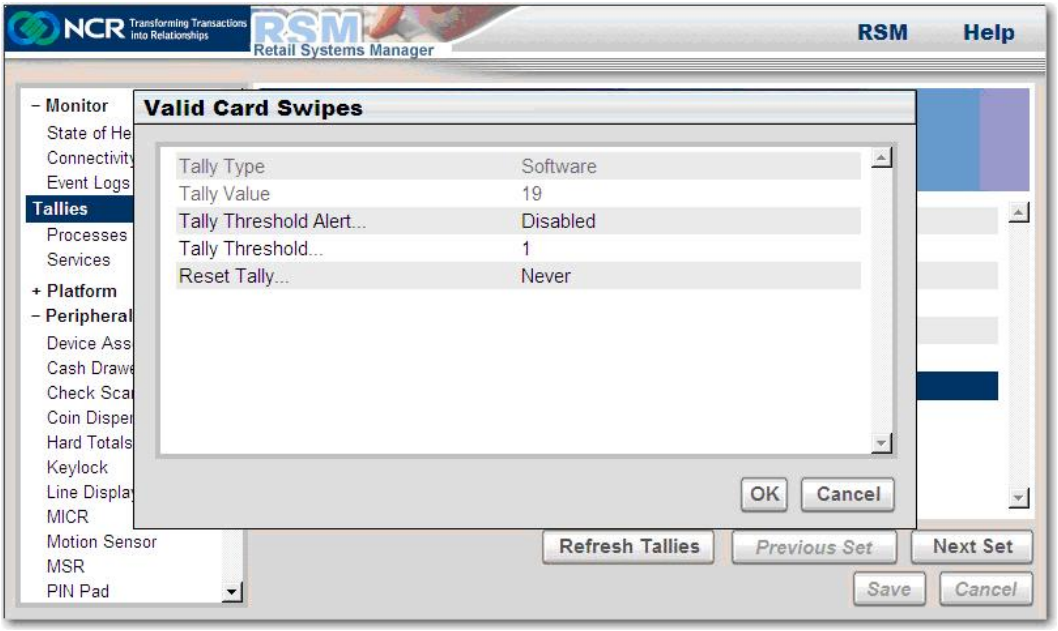
Viewing Tally information

To view information of a tally, follow these steps:

1. On the RSM Console, select **Monitor→Tallies**. The Tallies section displays the available tallies.



2. Select the tally you want to view. The system displays information about the tally.



The window displays the following information:

- Tally Type—refers to the type of tally, which can be either of the following:
- Software—includes the tallies that are maintained by software.

- Hardware—includes the tallies that are maintained on the physical device and retrieved periodically by the peripheral software.
- Tally Value—refers to the current count for the tally.
- Tally Threshold Alert—refers to the status of the alert, whether Enabled or Disabled.
- Tally Threshold—refers to the number of times a certain operation is performed before an alert is sent. For more information, refer to *Tally Thresholds* on page 121.
- Reset Tally—refers to the option of resetting the current tally.

3. Select **OK** to close the window.

Refreshing Tallies

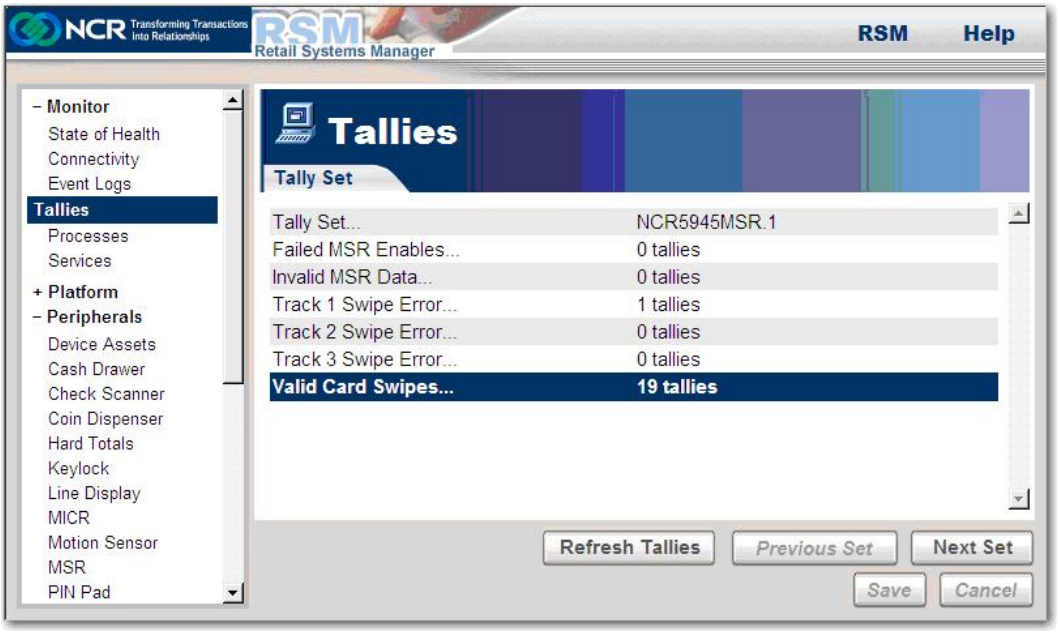
Tallies are initially stored in memory, and the current tally counts are saved to disk periodically. The RSM user interface displays the tally values that are saved on the disk.

The interval for how frequently the tallies are saved to disk can be configured in the RSM user interface by selecting the **System** or **Server**, and then selecting **Administration→Alerting→Tally Save Interval**. The default Tally Save Interval is 60 minutes.

Tallies may increment while using a device, but the updated tally counts may not display in the RSM user interface until the next Tally Save Interval.

To refresh the tallies, follow these steps:

1. On the RSM Console, select **Monitor→Tallies**. The Tallies section displays the available tallies.



2. Select **Refresh Tallies**. The system saves the current tallies in memory to the disk and then displays them on screen.

Note: Prior to RSM and RPSW release 4.0, the *Tally Save Interval* option was called *Tally Flush Interval*, and the *Refresh Tallies* button was called *Flush Tallies*.

Hardware Tallies

For RSM release 3.0 and later, hardware tallies are added to RSM for some 3.x Retail Control peripherals. Hardware tallies must be pulled from the device instead of updating them as they occur like the software tallies. A timer is used to periodically retrieve the hardware tallies when the device is in use. However, the hardware may report hardware tallies at different times depending on the device.

Currently, the following devices are supported:

- Printers
- MICR
- Scale
- Scanner

Note: The minimum firmware version for support of hardware tallies in the 7875 SA, 7876, 7883 SA (All SuperASIC) scanners is 497–0449064, dated 4/17/06.

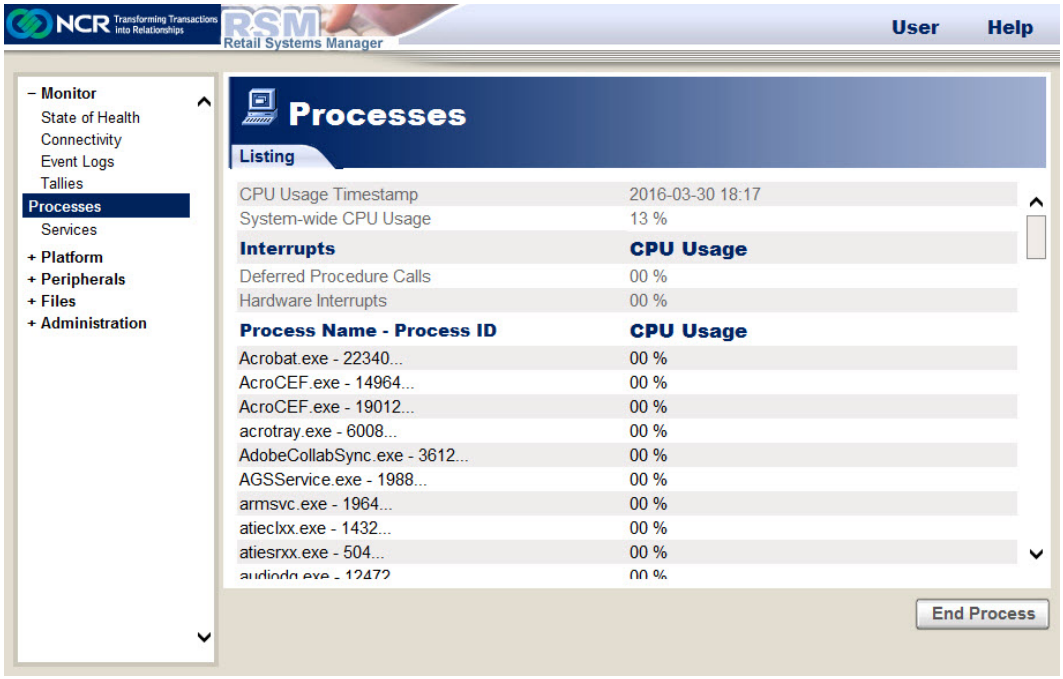
The Printer and MICR hardware tallies are only reported up to every 8 hours. If you print a few lines and wait five minutes, the hardware tally values do not change. To force the hardware tally values to update, print a diagnostic form by opening and closing the cover, while holding the paper feed button. Afterwards, new hardware tally values are reported to RSM at the next update interval.

The Scanner and Scale hardware tallies are written to volatile memory every five minutes and then to non–volatile memory every hour. RSM reads the tallies from volatile memory. If you are using the scanner or scale, the hardware tallies are accurate up to a 5–minute window. But if you unplug the scanner or scale before the hour–interval is up (before hardware tallies are written to non–volatile memory), the count reverts back to the last non–volatile count so the count in RSM could decrease after a device is power–cycled.

Note: A reset of hardware tallies is not supported.

Processes

The system displays the Processes window by selecting **Monitor→Processes**. The Processes window displays the processes that are running and their CPU utilization percentage.



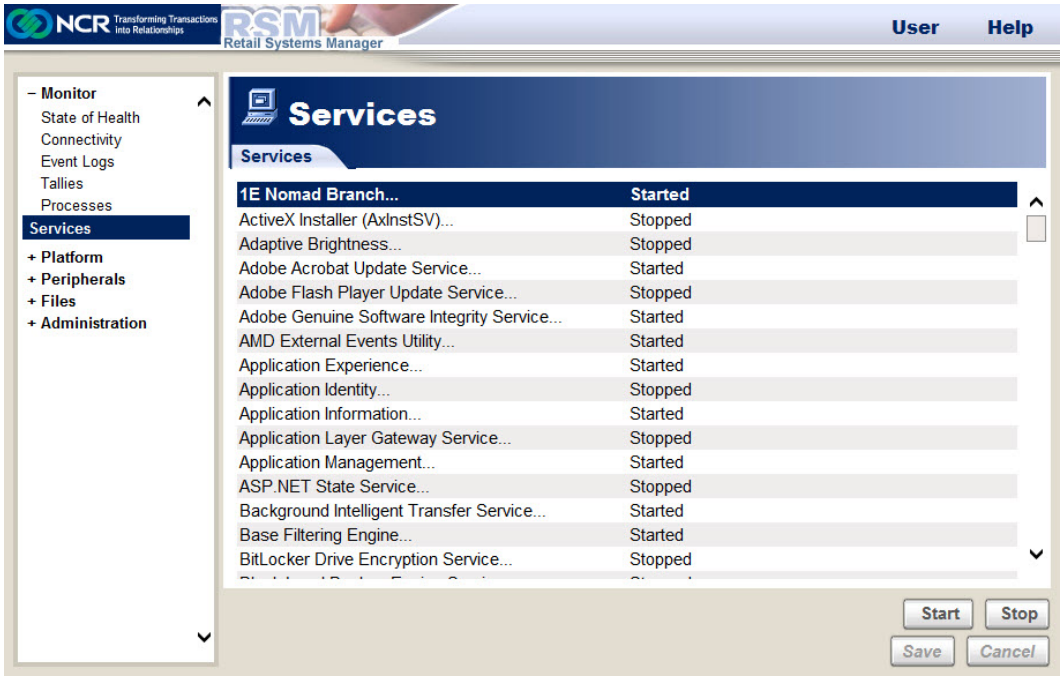
If you select a process from the list, the system displays additional information about the process.

The End Process button is used to stop a process.

Warning: Make sure you understand what a process is doing before stopping it. Unexpected behavior could result.

Services

The system displays the Services window by selecting **Monitor→Services**. The Services window displays the services that are installed and their Stopped or Started state.



If you select a service from the list, the system displays additional information about the service.

You can change the Startup Type of a service by selecting **Start** or **Stop** from the Services window.

Warning: Ensure that you understand what a service is doing before stopping it. Unexpected behavior could result. If you stop the NCRLoader service from the RSM user interface, the RSM user interface stops working. You must restart the service from the Windows Control Panel.

Using the Administration section

The Administration section is included in all versions of RSM LE. The features include the following:

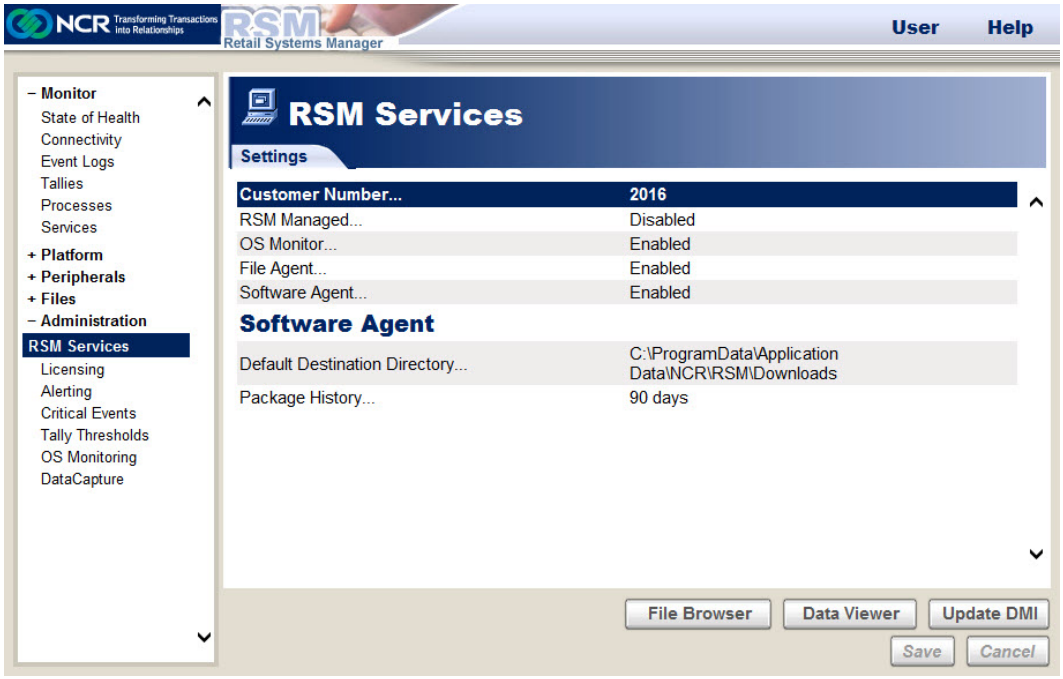
- RSM Services—provides information about the features that are used if RSM LE is a managed system. If RSM LE is unmanaged, you do not need to use any of the following features:
  - Customer Number
  - RSM Managed
  - RSM Server Discovery
  - Connected RSM Server
  - Logical System Name
  - Custom Tags
  - OS Monitor
  - File Agent
  - Software Agent
  - Default Destination Directory
  - Package History
- Licensing—provides information about the licensing. There is nothing you can change in this section if RSM LE is managed by RSM SE. However, you can add a license in this section if RSM LE is not managed by RSM SE. For more information on installing the RSM LE license, refer to *Installing the RSM LE License* on page 61. The license information include the following:
  - Current User
  - License File
  - License Expiration
- Alerting—provides the functionality to change the settings for the logs and tallies and configure the SNMP Agent. The Alerting features include the following:
  - Log Event Types
  - Tally Save Interval
  - SNMP Agent
- Critical Events—provides the functionality to change the threshold information of the various types of critical events. You can also view the meanings of various types of event messages.
- Tally Thresholds—provides the functionality to change the tally threshold values for the various retail peripherals.

- OS Monitoring—provides the functionality to configure the monitoring of system wide CPU and memory usage, disks and files, and processes and services.
- Data Capture—provides the functionality to diagnose or debug problems.

For more information about these features, refer to the next sections.

RSM Services

The Services menu for RSM LE is primarily used with a system that is being managed by an RSM server. If you are running the RSM LE in an unmanaged, local environment, most of the features are not applicable, such as the RSM LE shown in the sample image below.



The system displays the RSM Services section when you select **Administration→RSM Services**. The RSM Services section displays the following information:

Settings	Description
Customer Number	Identifies the customer using RSM. The Customer Number displays on the contract with NCR. The Customer Number is required for activating an RSM license. If RSM LE is managed, the Customer Number is configured at an RSM server and is not changeable at RSM LE. If RSM LE is not managed by an RSM SE server but an RSM license file is used, such as when adding SNMP support, the customer number must be configured at RSM LE to activate the RSM license. For more information, refer to *Installing the RSM LE License* on page 61.

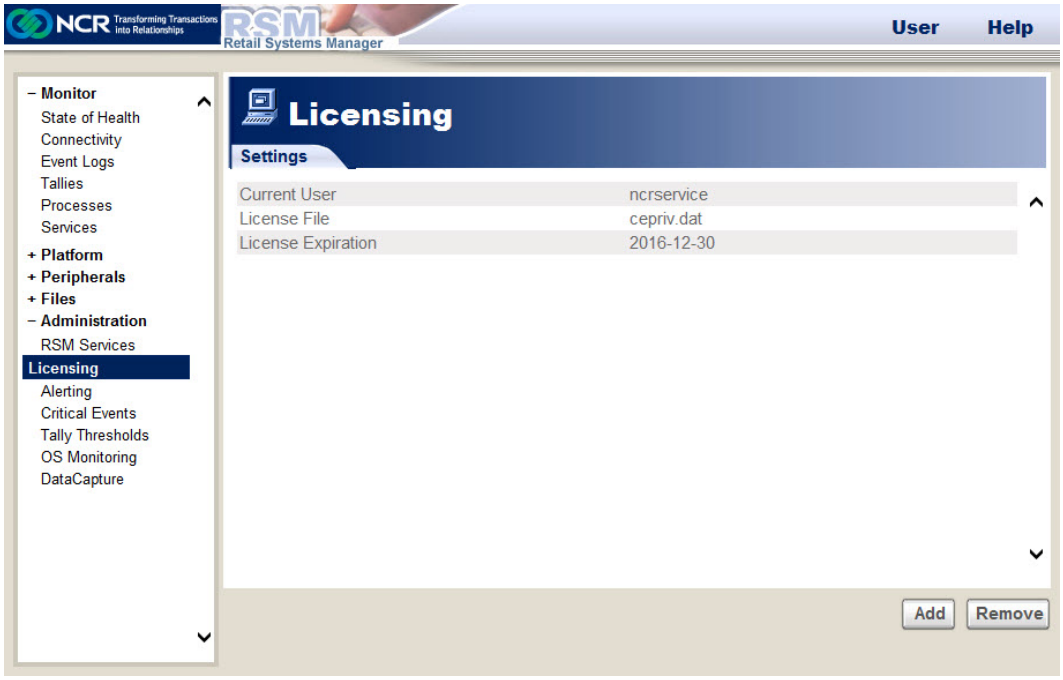
Settings	Description
RSM Managed (Enabled or Disabled)	Indicates whether this system is managed by an RSM SE Server. If this option is set to enabled, it is assumed that an RSM SE Server manages this RSM LE system. If using PXE Image Loader instead of RSM SE: • If using Command Center in a Dual Server configuration, configure RSM LE to be managed by the two PXE Image Loader servers to simplify role changes for Command Center. Otherwise, configure RSM LE as unmanaged.
RSM Server Discovery (Dynamic or Fixed)	Determines if a managed client gets the address of the managing server dynamically or whether you assign a fixed address for the SE or PXE Server.
Connected RSM Server	Displays the last RSM SE or PXE Server that the client communicated with, if managed.
RSM Server (Primary)	Refers to the field for setting the name or IP address of the server if RSM Server Discovery is Fixed.
RSM Server (Secondary)	Refers to the field for setting the name or IP address of the secondary server in a dual server environment.
Logical System Name	Refers to the identifying name for this system that can be used to identify this system by a name other than its computer name at RSM Servers. For example, it may be desirable to use names like Lane 1 or Bakery to identify the location or usage of the system.
Custom Tag	Provides the functionality to group systems managed by RSM SE or RSM EE into various roles such as the functional area in the store, a region in the country, or any other grouping you wish.
OS Monitor (Enabled or Disabled)	Indicates whether the monitoring of the operating system is Enabled or Disabled. This setting is a licensed feature, but it can be used without an RSM SE server. It is automatically licensed if Command Center is used.
File Agent (Enabled or Disabled)	Indicates whether File Agent is Enabled or Disabled to support file distribution packages scheduled from RSM SE or RSM EE. **Note:** If RSM SE is not used, File Agent may be disabled.

Settings	Description
Software Agent (Enabled or Disabled)	Indicates whether Software Agent is Enabled or Disabled to support software execution in packages scheduled from RSM SE and RSM EE servers. **Note:** If RSM SE is not used, Software Agent may be disabled.
Default Destination Directory	Refers to the default destination directory used for packages that contain distributed files but no destination directory is defined in the package.

Licensing

The system displays the Licensing section when you select **Administration→Licensing**. The licensing section displays the current licensing information. If RSM LE is managed by an RSM SE server, these are information fields and cannot be changed on this screen. If the RSM LE is unmanaged, you can add a license file through this section.

Note: For more information on installing the RSM LE license, refer to *Installing the RSM LE License* on page 61.



The Licensing section displays the following licensing information:

- Current User—refers to the user who is currently logged on to this session of RSM LE.
- License File—refers to the name of the license file currently in use.
- License Expiration—refers to the expiration date for the license file. If the license has expired, only EUI functionality is available in RSM LE.

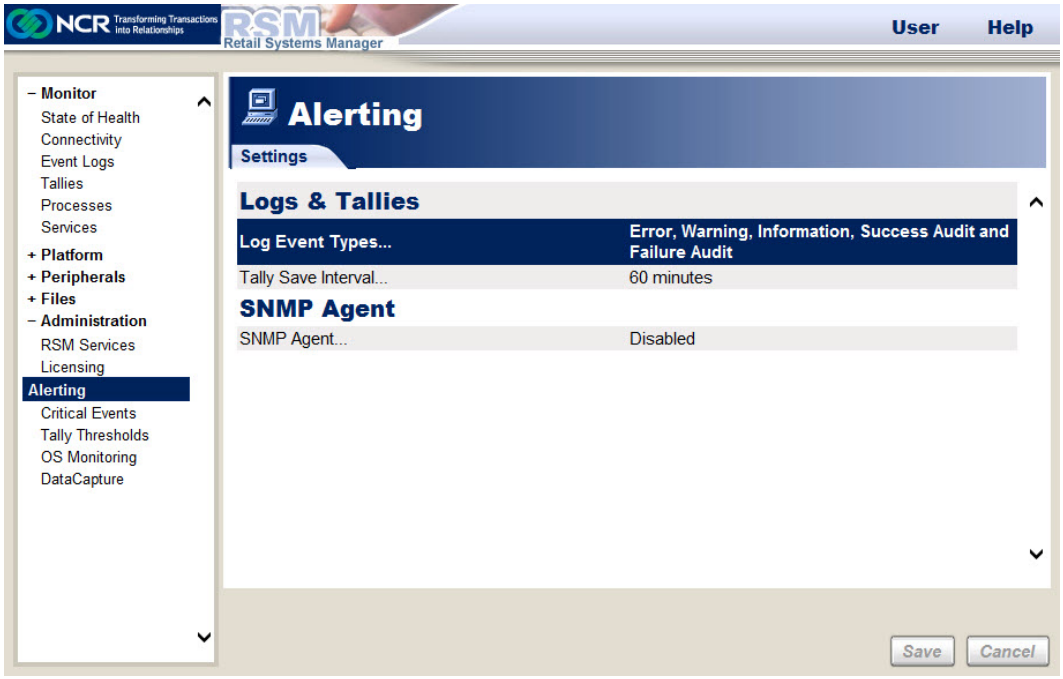
If RSM LE is managed by an RSM SE server, the RSM SE server will generate alerts when the RSM license is near expiration. By default, alerts will not be generated by RSM LE for license expiration because it is handled by the server in managed cases.

For an RSM LE system that is not managed by an RSM SE server but is licensed for reporting alerts through SNMP, you can configure RSM LE to generate Critical Events when the RSM license is near expiration. To configure RSM LE to generate Critical Events, add the following events to the Critical Events configuration:

- RSMTransport event 50605
- RSMTransport event 50606

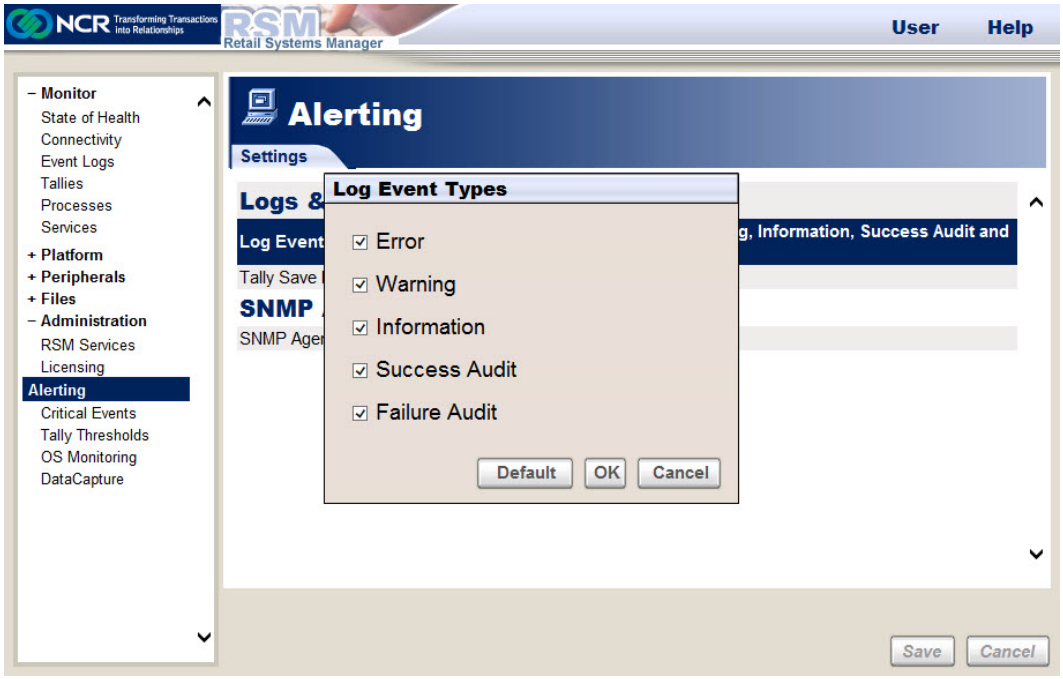
Alerting

The system displays the Alerting section when you select **Administration→Alerting**. The Alerting section provides you the functionality to change the settings for the logs and tallies and configure the SNMP Agent.



Log Event Types

You must select the event types that you want logged to the Windows event log. All types that are not selected are not written to the event log for any event source that uses RSM or Store Minder APIs to log events, but are still used for determining State of Health and critical events. If none of the event types are selected, the event filter is disabled and all event types are logged.



The log event types include:

- Error
- Warning
- Information
- Success Audit
- Failure Audit

Event Filtering Restriction

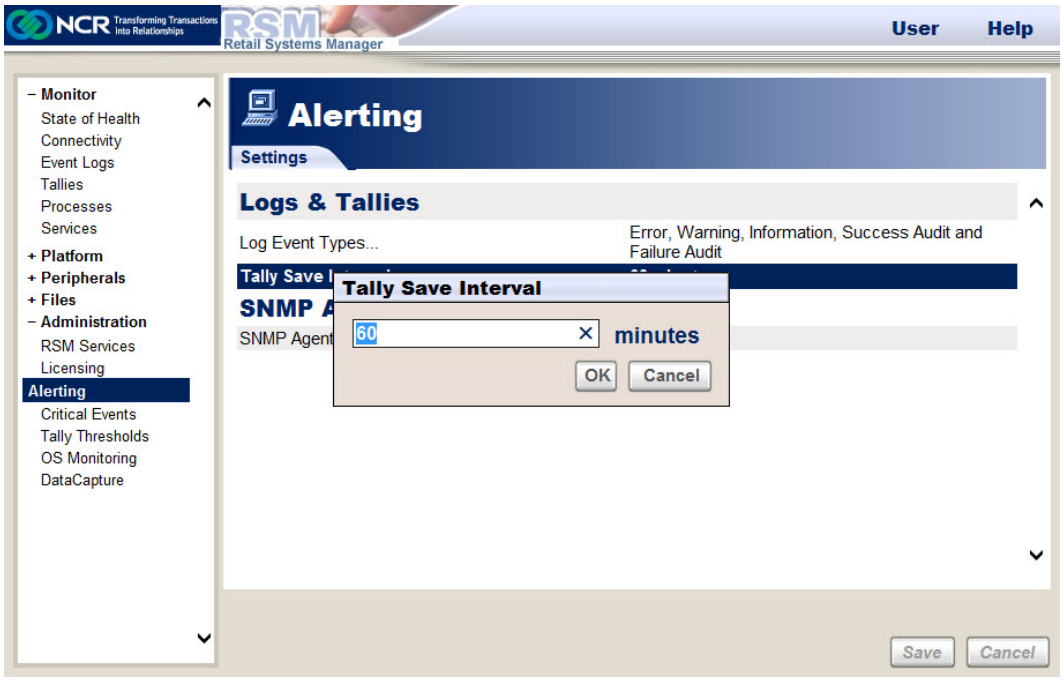
The Log Event Types option provides RSM the functionality to limit what events RPSW or RSM log to the Windows Event Log. Events that are filtered are still used for alert processing in NCRFSM. However, if some events for the same device (for example, printer) are logged very close to the same time and some events are filtered and some events do go to the Windows Event Log, it is possible for the State–of–Health processing in NCRFSM to process them in the wrong order and end in the wrong state. Because of this, filtering of event logs is discouraged when using the State–of–Health feature of RSM, and the default for event logging is to not filter events.

Note: For customers that are not licensed for RSM, SNMP, or Command Center, NCRFSM and State–of–Health are not used, and filtering of events will not cause this problem.

Tally Save Interval

The Tally Save Interval is the frequency at which tally values are saved from memory to persistent storage. The default value is 60 minutes. If Command Center is used, tallies may be saved more frequently than the configured value.

For more information on tallies and how to trigger an immediate save of current tally values, refer to *Tallies* on page 85.



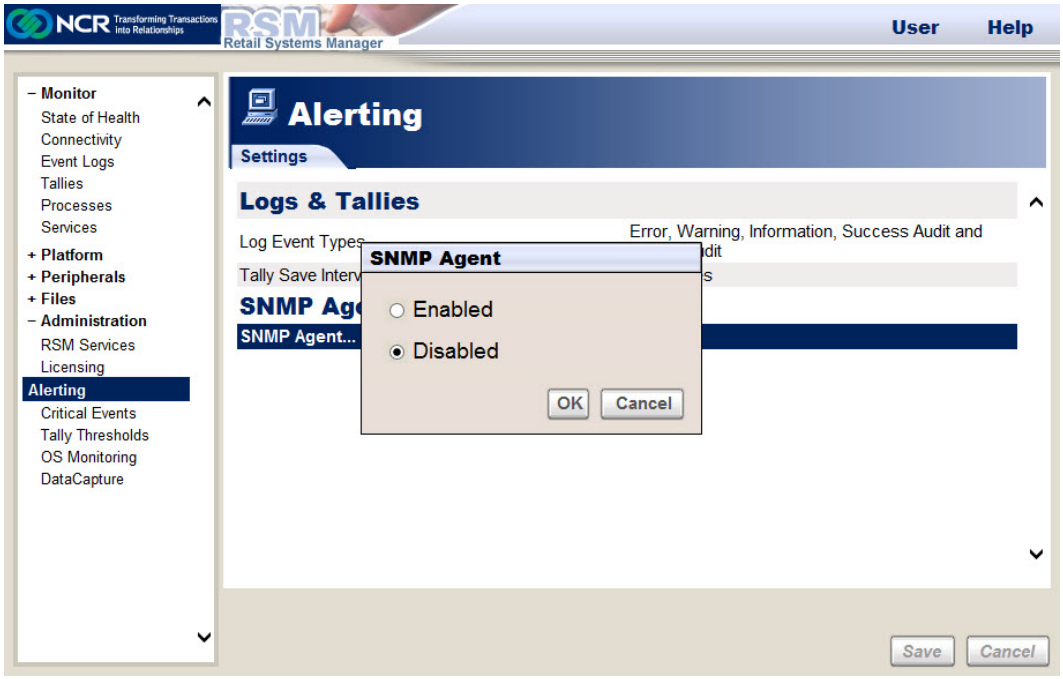
RSM SNMP Configuration

RSM provides SNMP support through RSM LE. Support is provided for SNMP traps only. The monitoring and thresholding is performed by RSM LE. These processes include the monitoring for state of health changes, critical events, and tallies that have exceeded a configured threshold. When these conditions occur, RSM LE has the ability to send an SNMP trap.

An RSM license file with the SNMP feature licensed is required to use the SNMP feature.

Note: The Microsoft SNMP Agent must be running to be able to use the RSM SNMP Agent. If RSM SNMP is not running as expected, you need to manually check whether certain settings in the Microsoft SNMP Service are successfully set. For more information about these settings, refer to *Microsoft™ SNMP Service Settings* on page 169.

The SNMP agent is disabled by default and must be enabled by the user.



After the SNMP agent is enabled, the system displays the various types of traps and other settings.

For additional information on the SNMP Agent, refer to the "RSM SNMP Agent" section in the *NCR Retail Systems Manager Software User's Guide* (B005–0000–1518).

State of Health Alerts

SNMP traps may be sent for State of Health (SOH) changes. There are different traps for the various types and severities of State of Health changes. You may configure which types of traps are sent from the system. For example, you may choose to send Overall alerts for all severities but you may choose to send Device Alerts only for states that require attention.

The types of SOH alerts are described in the sections that follow. For each SOH alert type, the severities are the same. The severities are the following:

- Healthy
- Attention Soon
- Attention Now
- Not Configured
- Unknown

Overall Alerts

Overall traps may be sent for changes in the overall status of the terminal or kiosk. These traps are a roll–up of the statuses of the terminal based on the status of all devices.

The Overall traps may be filtered by severity.

Selecting **Administration→Alerting→SNMP Agent→Suppress Overall Alerts with** displays the Suppress Overall Alerts with window.

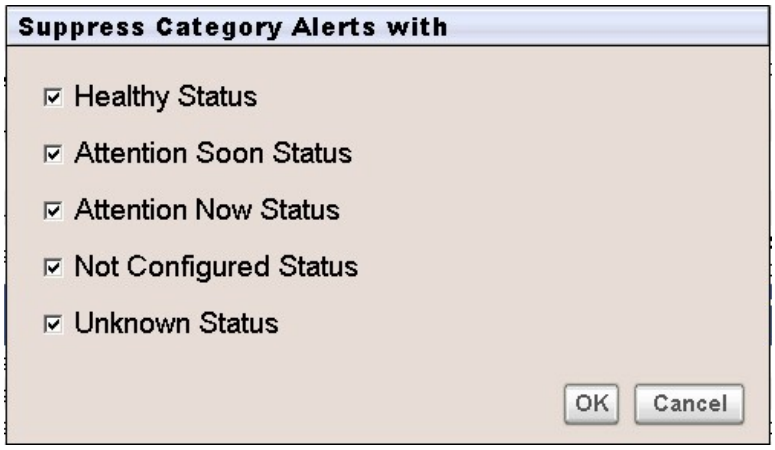
In this window, you can configure which Overall traps should be sent or suppressed. To suppress an alert, select the corresponding alert, and then select **OK**.

Category Alerts

Category traps may be sent for changes in the State of Health categories on the terminal or kiosk. Category is a sub–classification of the terminal, peripheral or peripheral device state. These categories include Configuration, Hardware, Maintenance, OPOS, and UPOS.

The Category traps may be filtered by severity.

Selecting **Administration→Alerting→SNMP Agent→Suppress Category Alerts with** displays the Suppress Category Alerts with window.



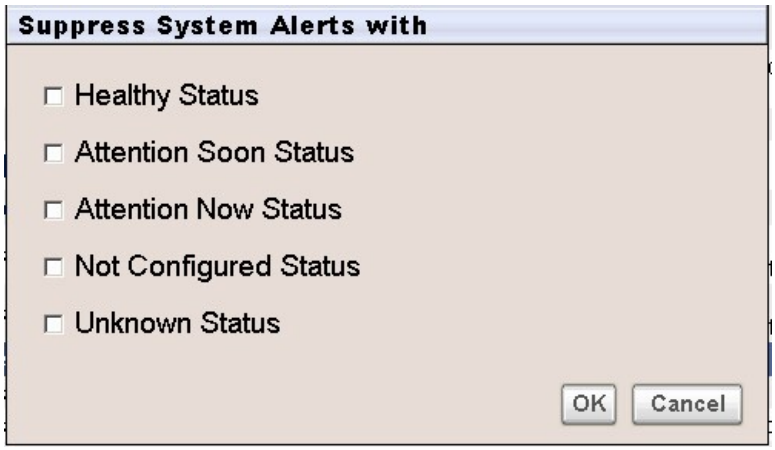
In this window, you can configure which Category traps should be sent or suppressed. To suppress an alert, select the corresponding alert, and then select **OK**.

System Alerts

System traps may be sent for changes in the system State of Health of a terminal or kiosk. This state is the state of the base system, not the state of peripherals or other devices in the system.

The System traps may be filtered by severity.

Selecting **Administration→Alerting→SNMP Agent→Suppress System Alerts with** displays the Suppress System Alerts with window.



In this window, you can configure which System traps should be sent or suppressed. To suppress an alert, select the corresponding alert, and then select **OK**.

Device Alerts

Device traps may be sent for changes in the State of Health for a peripheral or device on a terminal or kiosk. The State of Health for each device on the system is monitored separately.

The Device traps may be filtered by severity.

Selecting **Administration→Alerting→SNMP Agent→Suppress Device Alerts with** displays the Suppress Device Alerts with window.

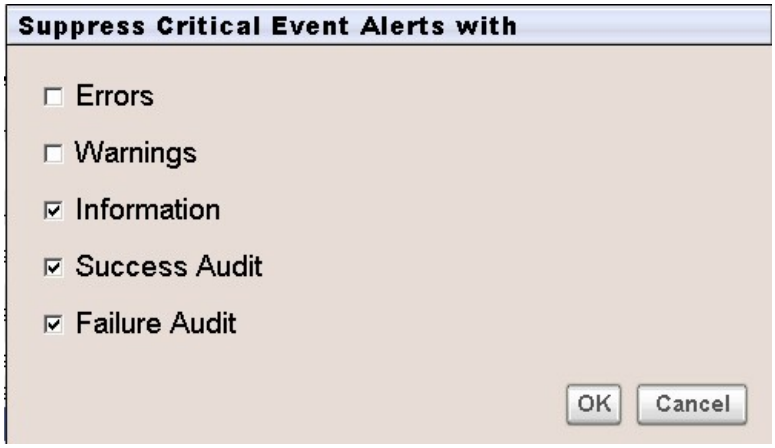
In this window, you can configure which Device traps should be sent or suppressed. To suppress an alert, select the corresponding alert, and then select **OK**.

Critical Event Alerts

Traps may be sent when an event is logged and reaches a configured Critical Event threshold. Although the content of the trap is similar to the Store Minder Event Traps from the NCR Retail SNMP Agent, the Critical Event traps for the RSM SNMP Agent are sent only for events configured as Critical Events through RSM, not for all events logged.

The Critical Event traps may be filtered by severity.

Selecting **Administration→Alerting→SNMP Agent→Suppress Critical Event Alerts with** displays the Suppress Critical Event Alerts with window.



In this window, you can configure which Critical Event traps should be sent or suppressed. To suppress an alert, select the corresponding alert, and then select **OK**.

Tally Alerts

Traps may be sent when a tally reaches a tally threshold configured through RSM.

Note: Tally Threshold Traps are new in the RSM SNMP Agent and were not supported in the NCR Retail SNMP Agent.

The Tally Threshold traps may be filtered.

Selecting **Administration→Alerting→SNMP Agent→Suppress Tally Alerts** displays the Suppress Tally Alerts window.

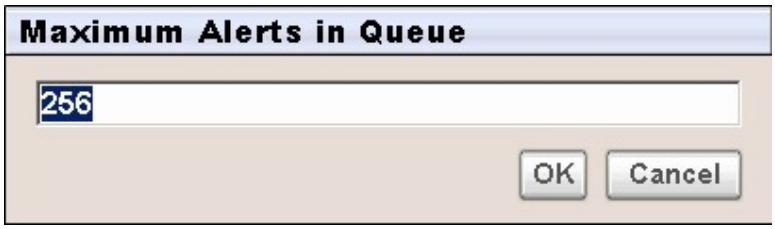
In this window, you can configure whether Tally Threshold traps should be sent or suppressed. To suppress an alert, select the corresponding alert, and then select **OK**.

Trap Queue Configuration

State of Health and Critical Event traps share one queue. Tally traps are in a separate queue. The configuration values below apply to both queues.

Maximum Alerts in Queue

Selecting **Administration→Alerting→SNMP Agent→Maximum Alerts in Queue** displays the Maximum Alerts in Queue window.



Maximum Alerts in Queue defines the length of the internal queue for TRAP events. If the queue becomes full, TRAP events are dropped (based on this value). Possible values are 10 through 1000. Default value is 256.

When Full Queue

Selecting **Administration→Alerting→SNMP Agent→When Queue Full** displays the When Full Queue window.

This option determines the strategy for managing the internal TRAP queue when the queue becomes full and a new TRAP event is created. The possible values are:

- Discard Old Alerts—overwrites older TRAP events. This value is the default value.
- Discard New Alerts—ignores new TRAP events.

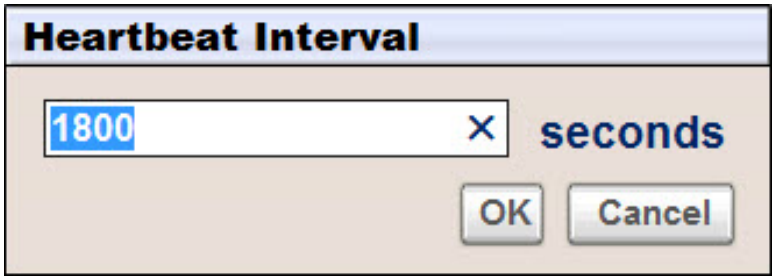
Heartbeat Configuration

This section describes the heartbeat configuration.

Heartbeat Interval

The interval (in seconds) between which the RSM SNMP Agent sends a periodic heartbeat trap. A zero (0) value indicates that no heartbeat trap should be sent. Possible values are 0 through 86400 seconds (24 hours).

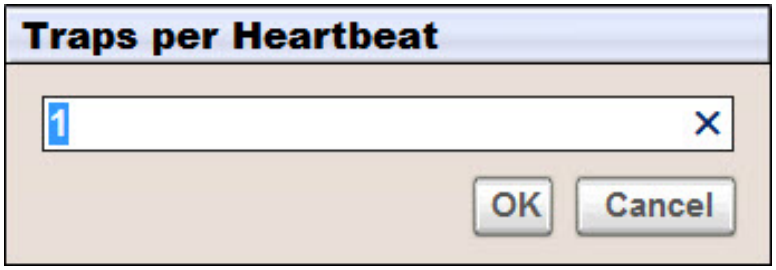
Selecting **Administration→Alerting→SNMP Agent→Heartbeat Interval** displays the Heartbeat Interval window.



Traps per Heartbeat

Traps per heartbeat is the total number of traps to be sent for a single heartbeat. Possible values are 0 through 16.

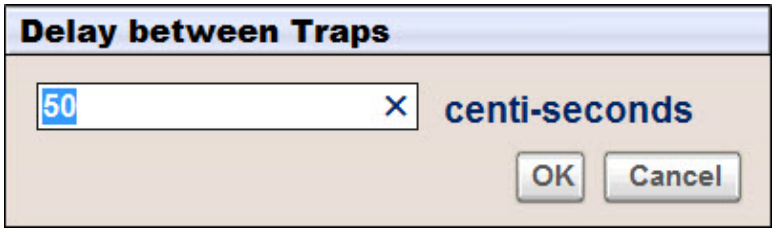
Selecting **Administration→Alerting→SNMP Agent→Traps per Heartbeat** displays the Traps per Heartbeat window.



Delay between Traps

Delay between traps is the time (in centi–seconds) between traps in a single heartbeat. Possible values are 0 through 3000.

Selecting **Administration→Alerting→SNMP Agent→Delay Between Traps** displays the Delay between Traps window.



Trap Reception and Processing

RSM SNMP generates traps to be processed by remote management systems. RSM SNMP traps are not processed by RSM servers. The remote management tool that receives traps must be configured on how to handle each type of trap that can be sent.

The traps sent by the RSM SNMP Agent are defined in `NCRRSMTraps.MIB`. This file is installed in the `C:\Program Files\NCR\RSM` directory when the Retail Platform Software for Windows (RPSW) is installed.

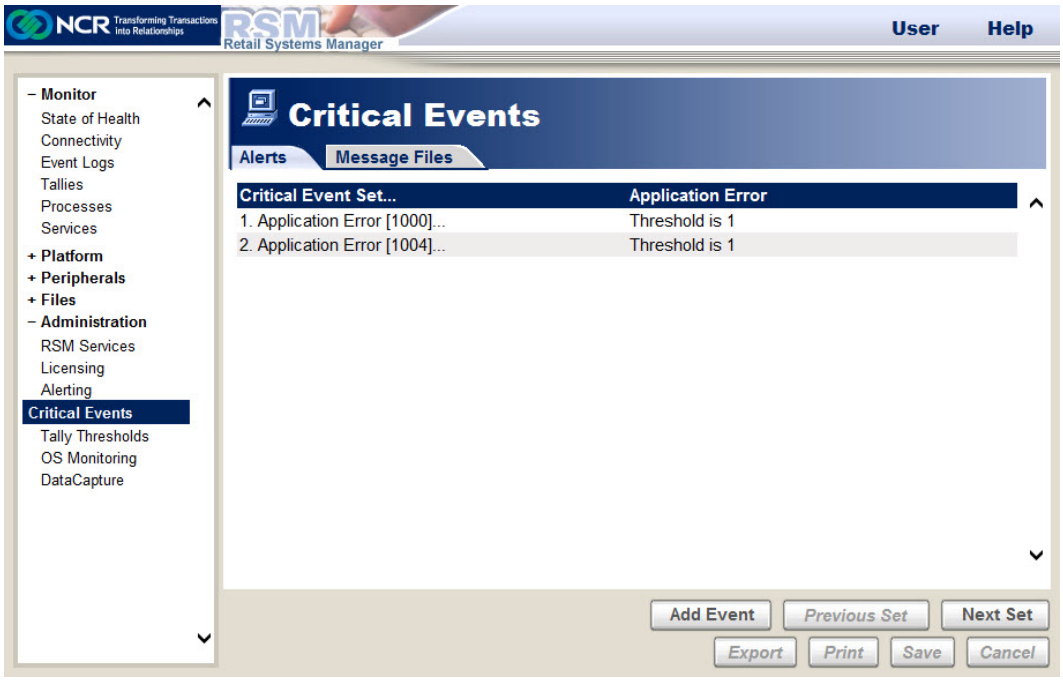
The remote management tool may require that specific rules be set up for specific alerts. In the case of NCR Gateway, rules for handling alerts sent by RSM SNMP are defined based on the default set of alerts. If additional alerts are configured (for example, adding an FSM definition file to define State-of-Health transitions for a new device or configuring additional Critical Events), new rules may need to be added in the remote management tool.

For more information about integrating RSM SNMP with your network management system, refer to the *RSM Software Development Kit*.

Critical Events

The system displays the Critical Events section when you select **Administration→Critical Events**. In the Critical Events section, you can perform the following:

- Change and view the threshold information for the various critical errors that were automatically set up during the RPSW installation.
- Add new events.
- View, export, and print event messages.

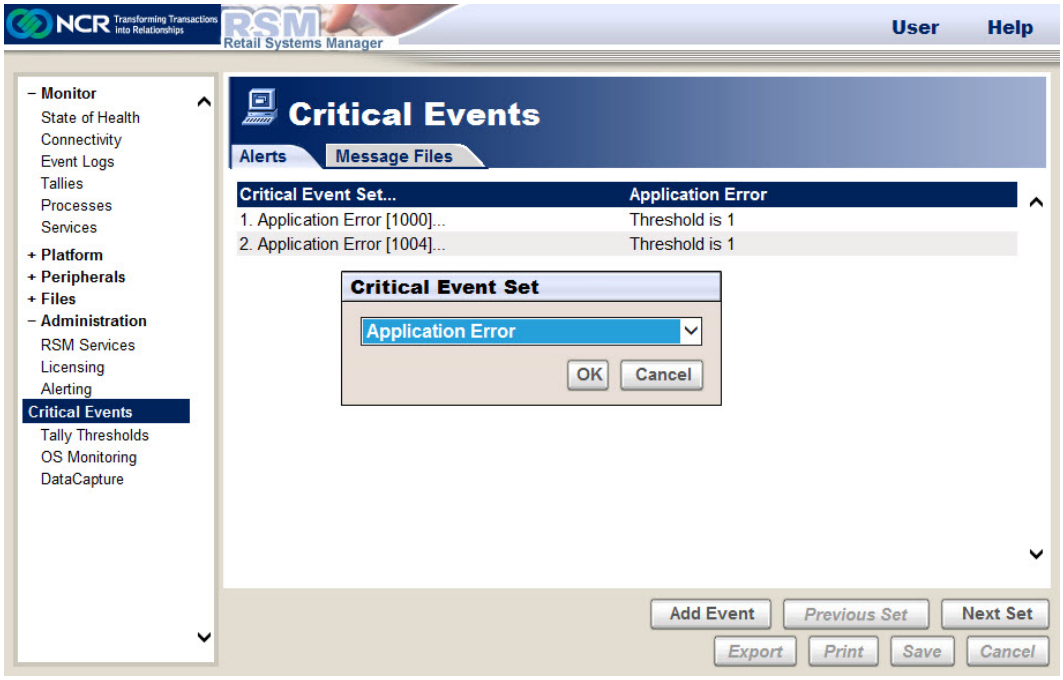


Configuring Critical Events

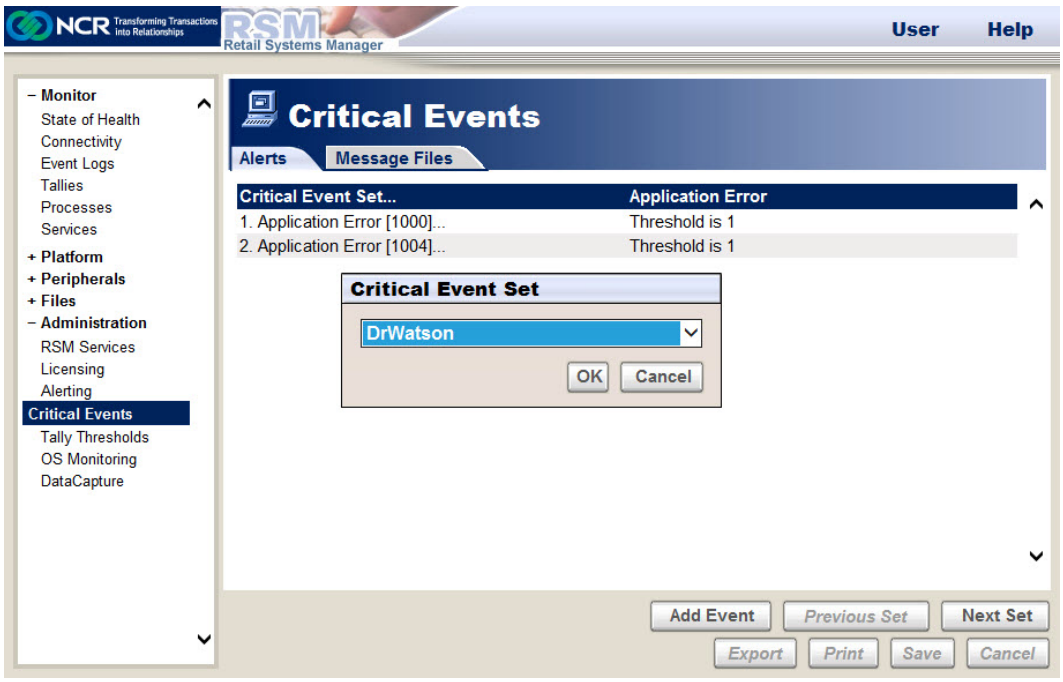
The Critical Events are divided in sets based on the event source. You can view the different event sets by selecting **Next Set** or **Previous Set**.

To configure an event set, follow these steps:

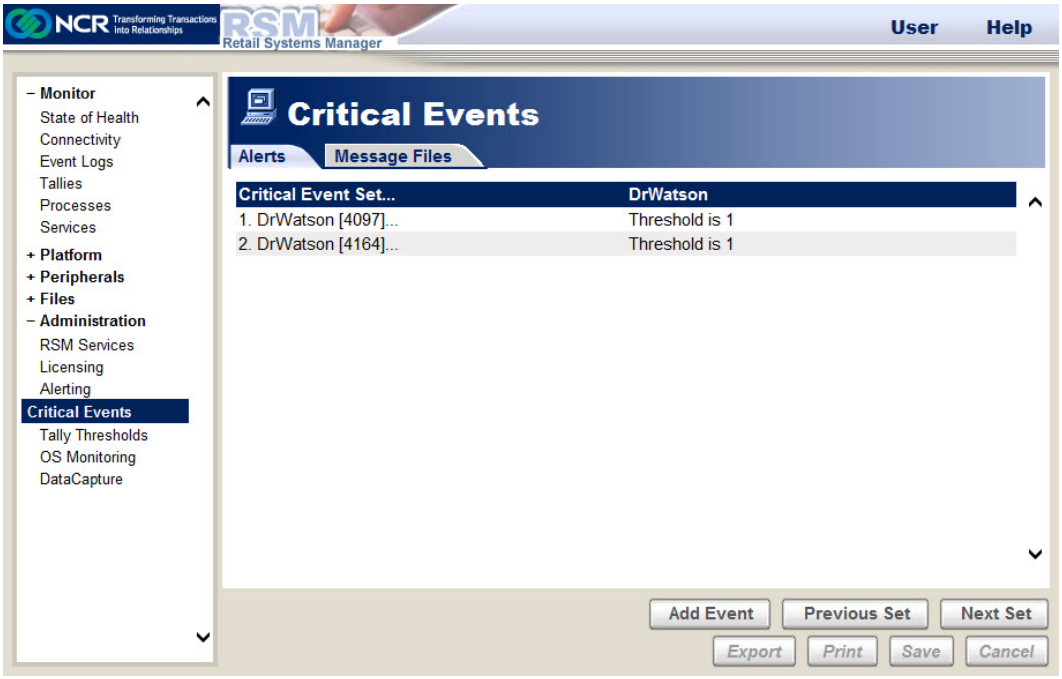
1. Select **Critical Event Set** and use the drop–down list in the Critical Event Set window to select the set.



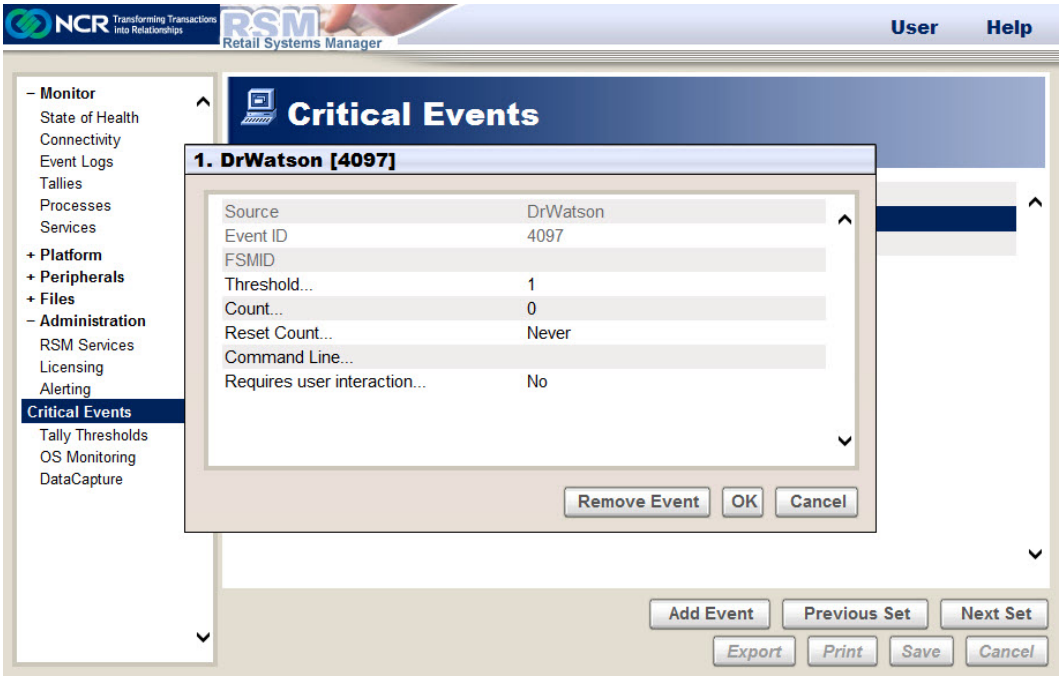
2. Select a specific error and then select **OK**. In this example, DrWatson is selected.



The critical event window displays the critical events of the selected set.



3. Select a critical event.



Selecting a critical event displays the following information:

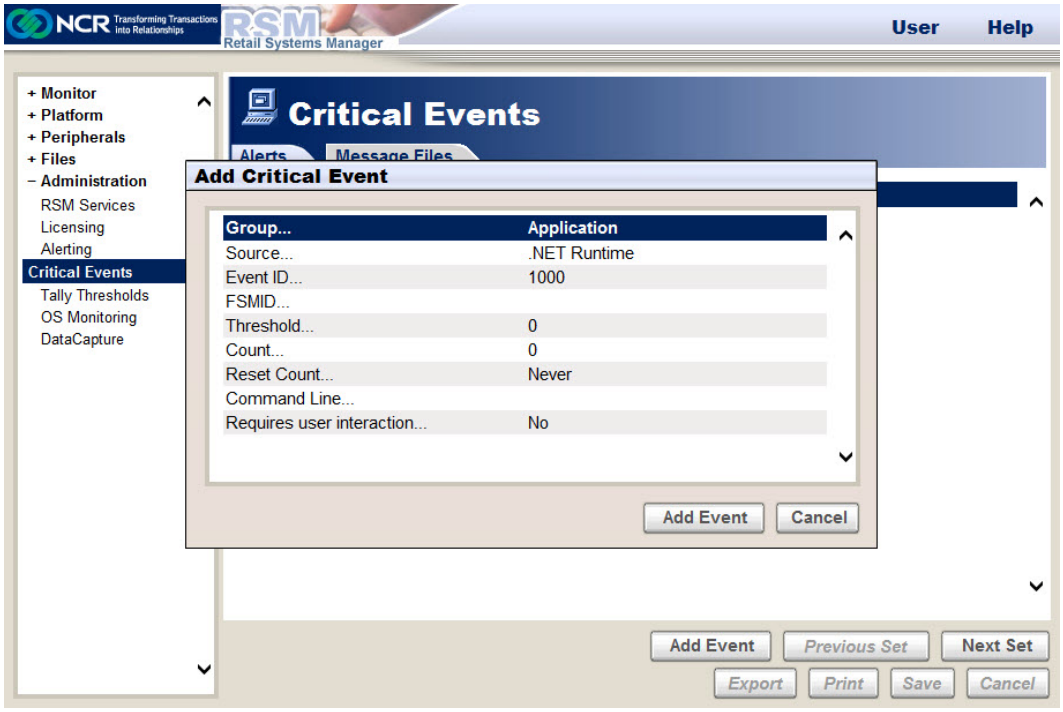
- Source—refers to the event source.
- Event ID—refers to the unique event identifier.

- FSMID—if the event message contains the Finite State Machine ID (FSMID) field to specify the instance of the monitored item (profile name for peripherals, process name for process monitoring, file name for file monitoring), this field can be used to configure a critical event for a specific FSMID.
- Threshold—refers to the number of times the event should occur before an alert is sent.
- Count—refers to the current count of how many times the event has occurred.
- Reset Count—refers to whether to reset the count value when the threshold occurs or to never reset the count.
- Command Line (optional)—refers to the command line to run when the threshold is reached.
- Requires user interaction—refers to whether the Command Line specified for the event requires user interaction.

4. Modify the critical event set's information if necessary, and then select **OK**.

Adding Critical Events

To add new events, select the **Add Event** button. The system displays a window that asks you to select the Group, and then enter the parameters explained in the *Configuring Critical Events* section.

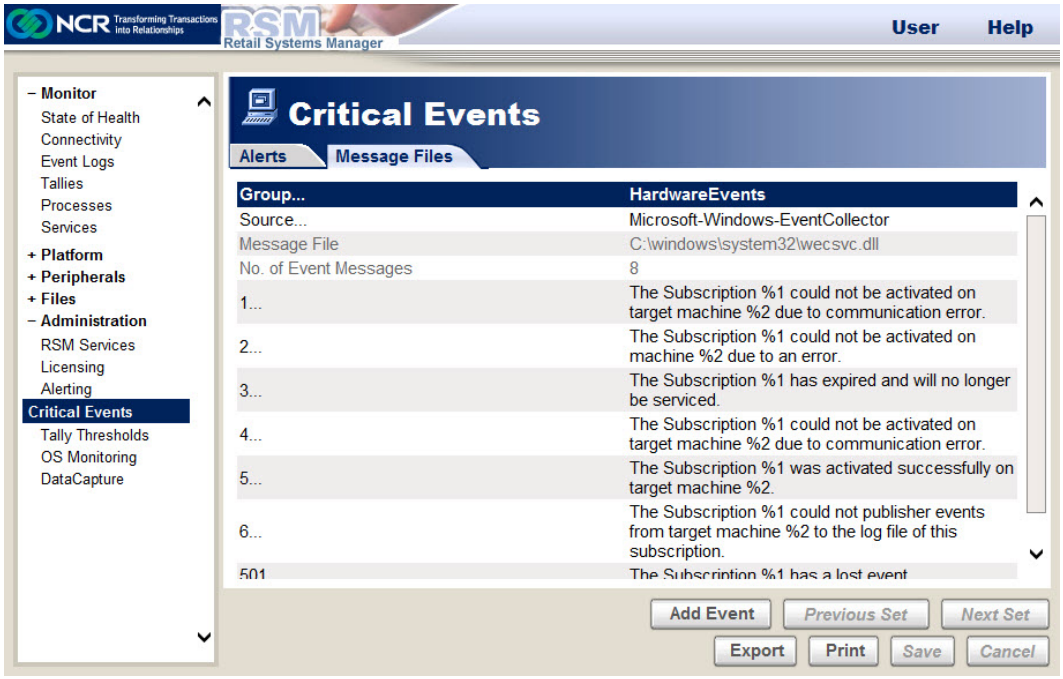


Viewing Event Messages in Message Files

If licensed, an additional Message Files tab displays on the Critical Events section. The message files tab permits users to view the messages in the event message files registered for any event source. The tab determines what the critical events mean and which events the user wants to configure.

To view the event messages in a message file, follow these steps:

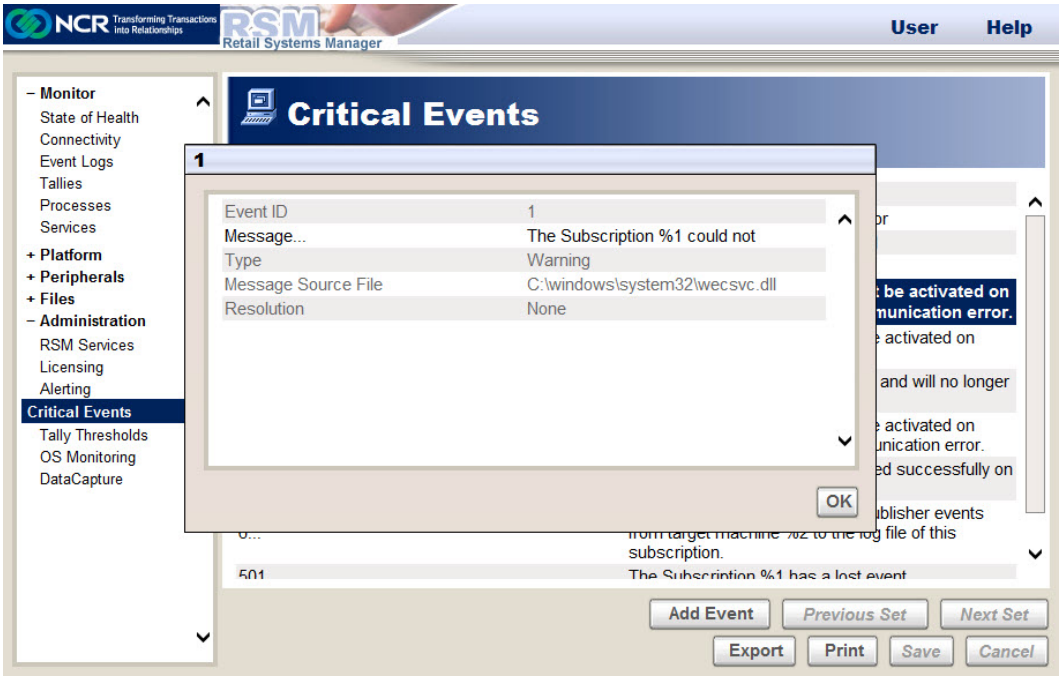
1. Select the **Message Files** tab in the Critical Events section, and then select the **Group** and **Source**.



The system displays the following information:

- Group—refers to the event log registered on the system that you have selected.
- Source—refers to the source of the event that you have selected.
- Message File—refers to the path of the message file.
- No. of Event Messages—refers to the number of event messages in the message file.
- Event Messages Set—displays the message set for sources with many messages. Use the **Next Set** or **Previous Set** to access other sets for the source.

2. Select the **Event Message** that you want to view. The system displays this window.



The window displays the following information:

- Event ID—refers to the unique identifier of the event.
- Message—refers to the message description. You can select the message to view the entire message.
- Type—refers to the type of message.

  Example: Warning

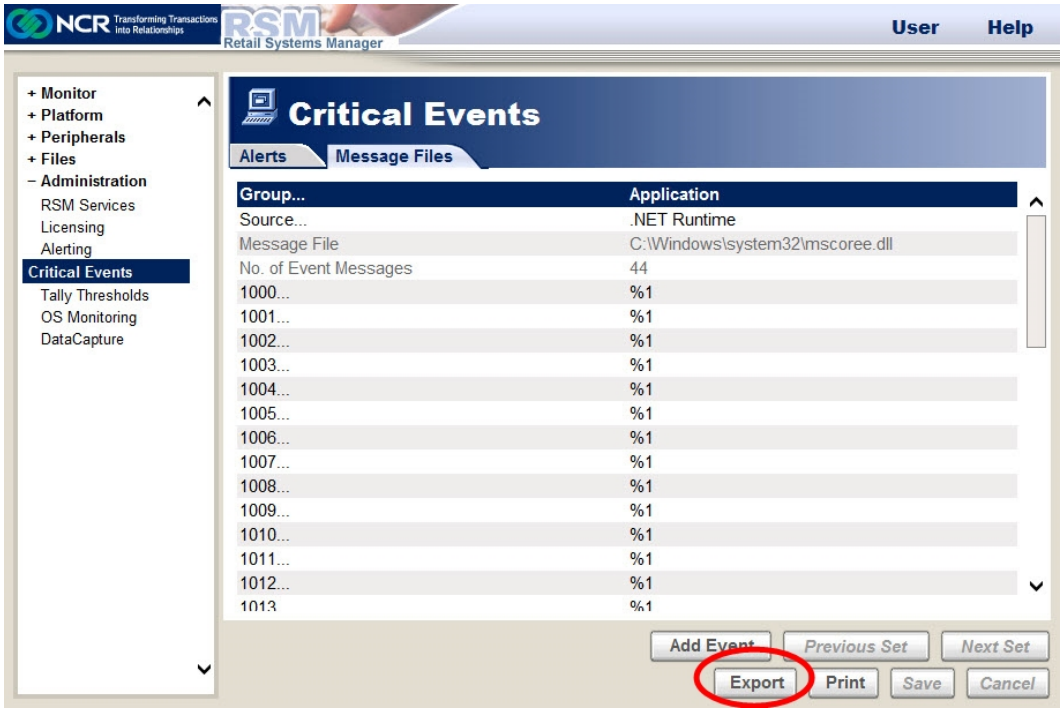
- Message Source File—refers to the location of the file that contains the message.
- Resolution—contains additional details about the meaning of the event and the recommended actions to take to resolve the problem, if defined for this event. This information is available only in RSM, not in Windows Event Viewer. It is available only if the resolution information feature is licensed.

3. Select **OK** to close the window.

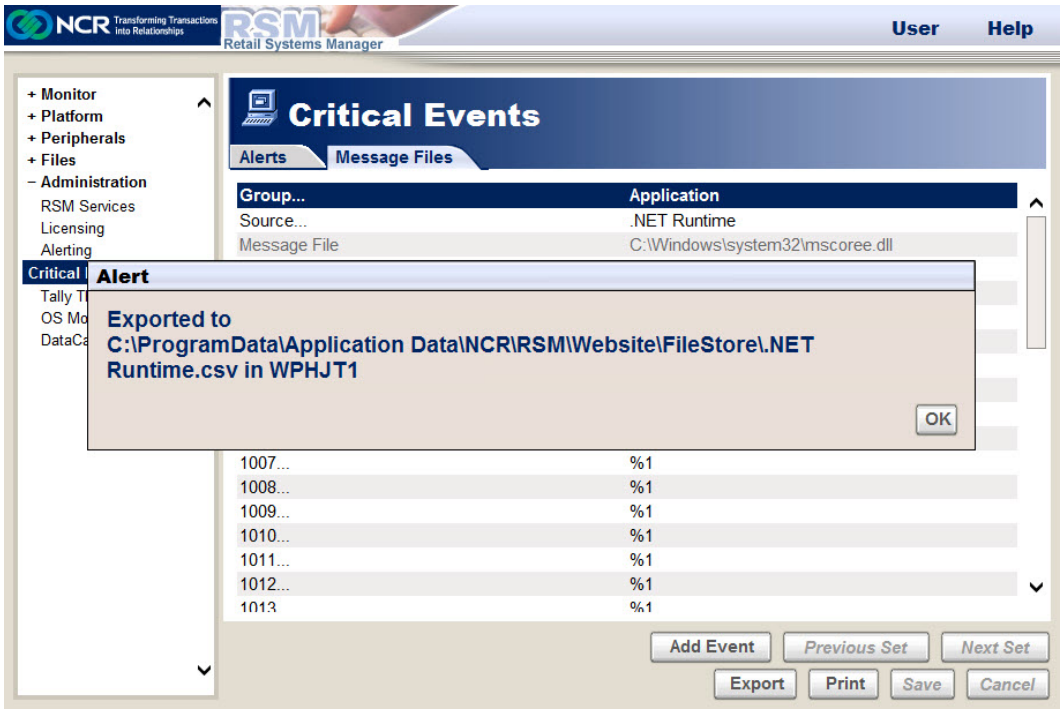
Exporting and Printing the Event Messages Set

To export and print the Event Messages Set, follow these steps:

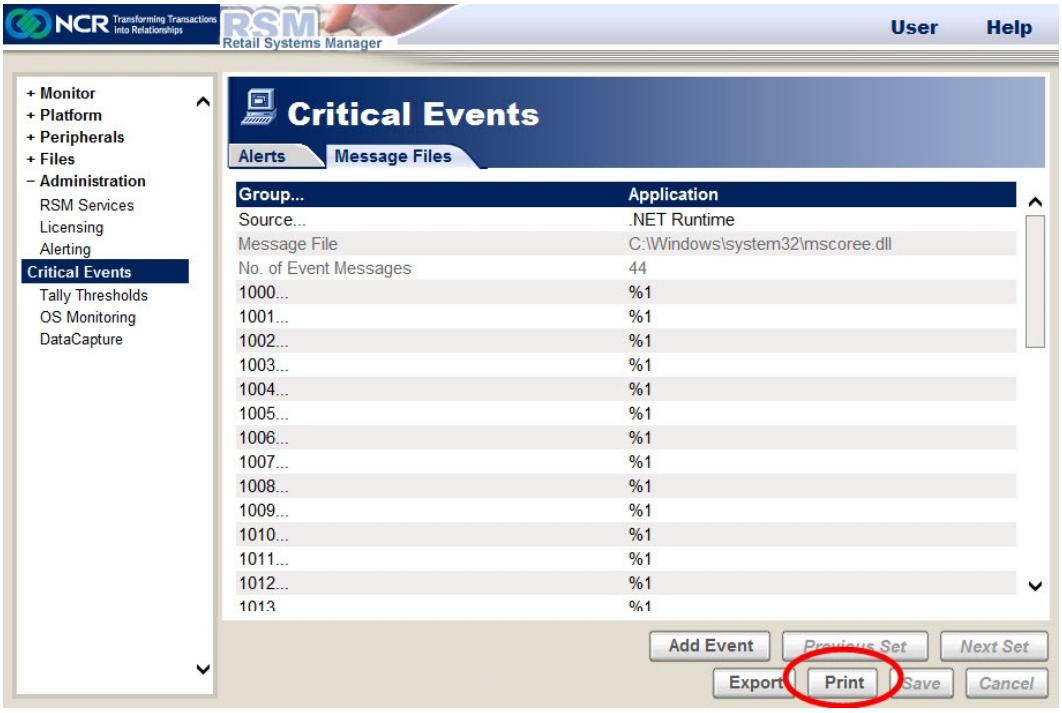
1. From the Message Files tab in the Critical Events section, select **Export**.



The system creates a CSV file and uses the Message File Source as the file name. It then displays an Alert window showing the path to where the file is saved.



2. To print the Event Messages Set, select **Print**.



The system then displays the Print window.

3. Configure the print settings, and then select **Print** from the Print window.

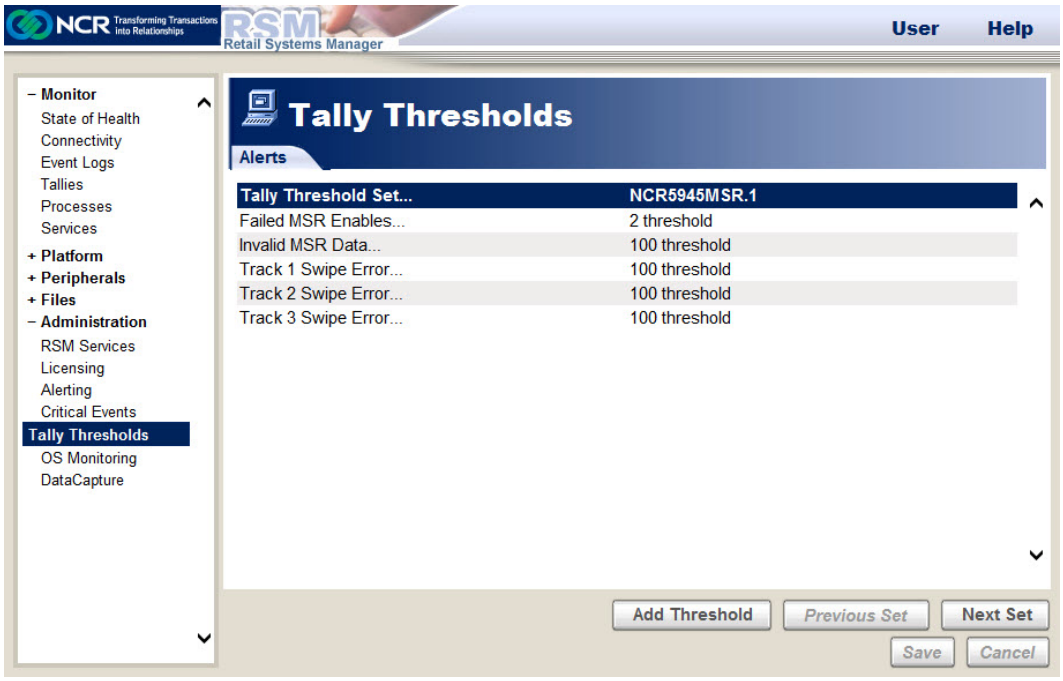
Tally Thresholds

Tallies are counts of the number of times a certain operation is performed. For example, the number of track 1 reads on the Magnetic Stripe Reader. A tally threshold is the number of tallies recorded for a device when you wish to be notified.

There are multiple ways to set tally thresholds, and these include the following:

- Default tally thresholds are installed with RPSW. The default tally thresholds are based on the default profiles. If the default profiles are not used, the default tally thresholds should be replaced with tally thresholds for the peripheral profiles used.
- An alternate set of tally thresholds can be installed with RPSW using a command line parameter to specify a `.reg` file containing tally thresholds.
- Add a tally threshold for a system or a group using the Tally Threshold menu in the RSM user interface where all the tally thresholds are listed.
- You can enable a tally threshold from the tallies page by selecting **Monitor→Tallies** in the RSM user interface. You can add a tally threshold for a system only (not groups) by using the tally page for a device and selecting the tally.

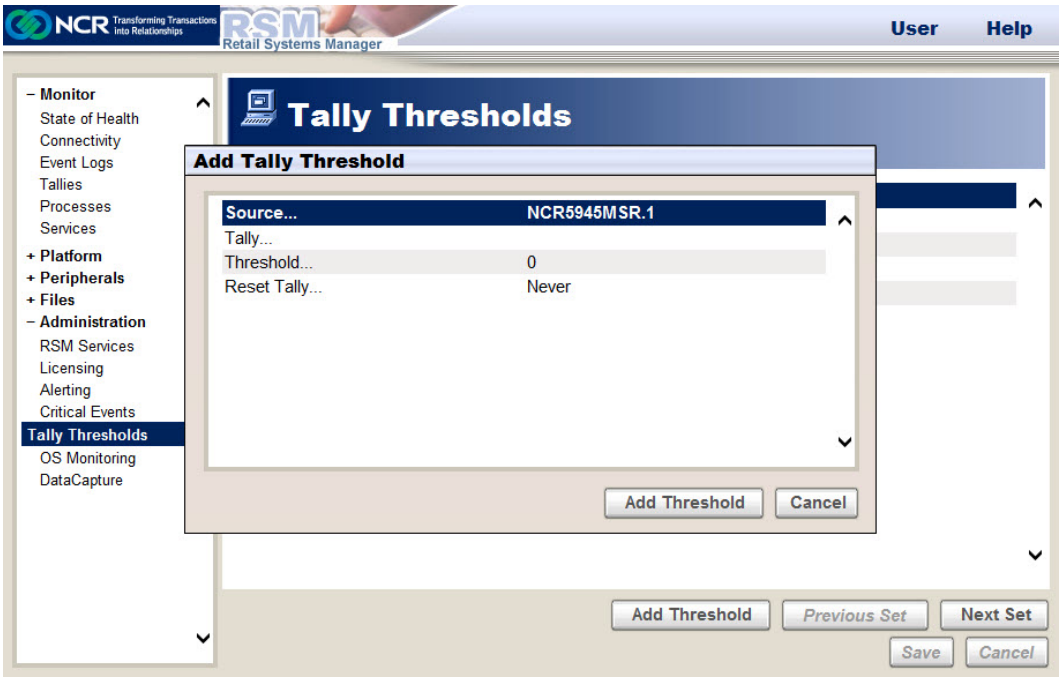
To display the Tally Thresholds menu, select **Administration→Tally Thresholds**.



Setting Tally Thresholds in the Tallies Threshold Menu

To set tally thresholds in the Tallies Threshold menu, follow these steps:

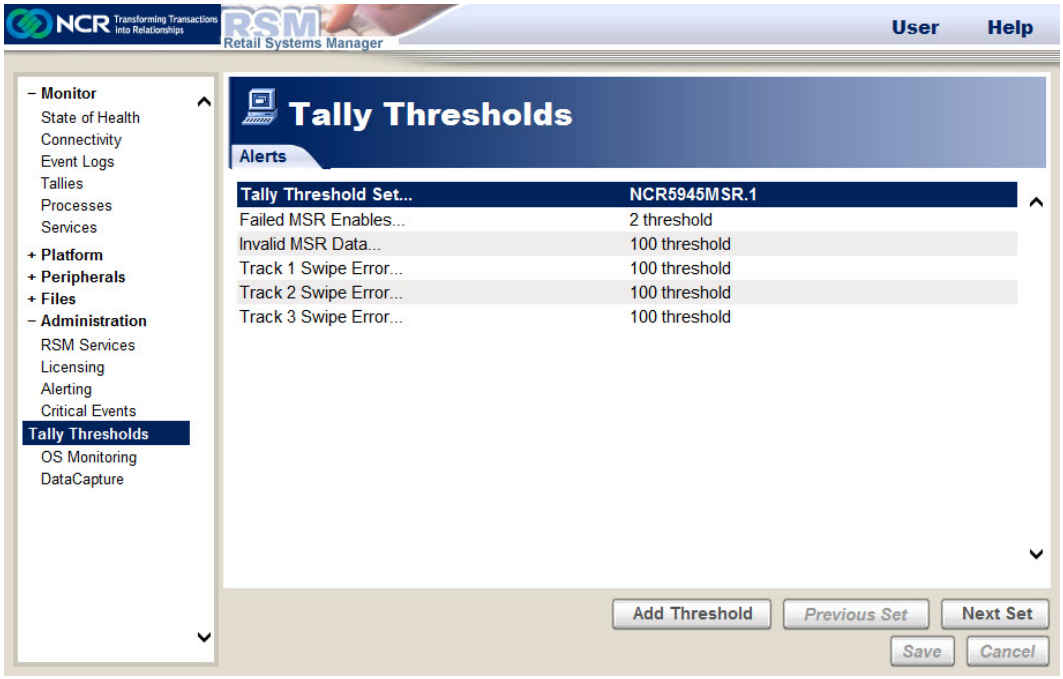
1. Select **Administration→Tally Thresholds→Add Threshold**. The system displays the Add Tally Threshold window.



2. Enter the following information:
   - **Source**—refers to the device that the tally is defined for.
   - **Tally**—refers to the description for the tally.
   - **Threshold**—refers to the number of times that the tally can occur before you are notified that the tally limit has been reached.
   - **Reset Tally**—refers to the reset option, whether to reset tally "When Threshold Occurs" or "Never".
3. Select **Add Threshold**. The tally threshold is added. The system then displays it in the Tally Threshold menu.

After a tally threshold is set up, you can remove it by selecting the tally threshold, and then selecting the **Remove Tally** button.

In the Tally Thresholds menu, you can go through the device tallies by selecting **Next Set** or **Previous Set**.



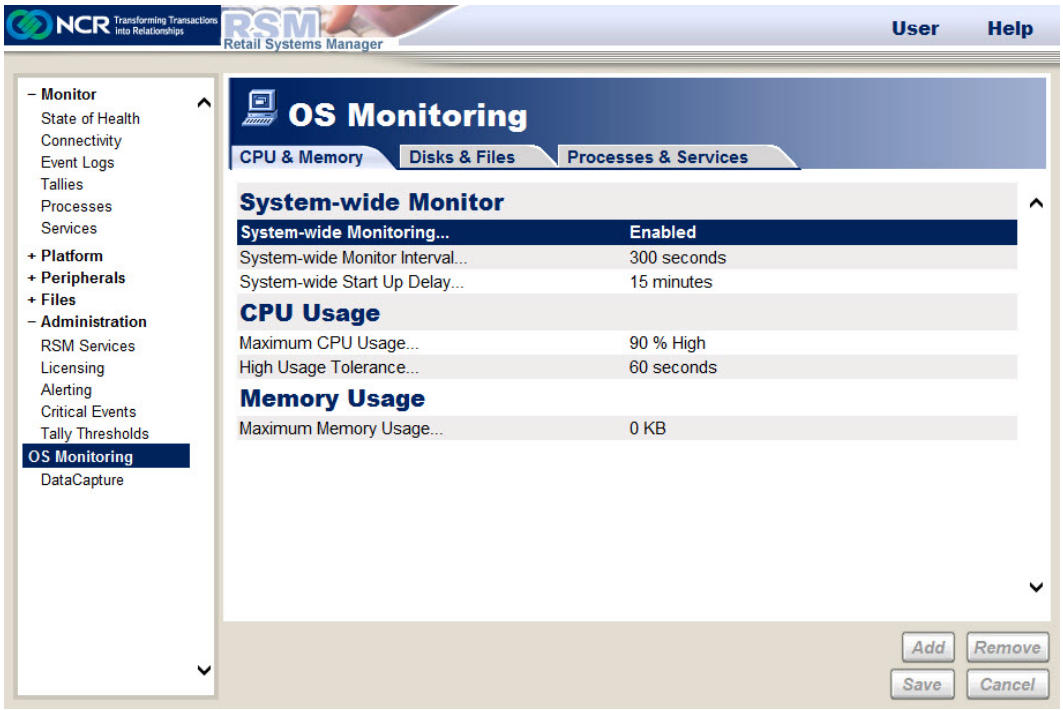
OS Monitoring

If licensed, Operating System (OS) Monitoring provides a display of various features that can be measured by the operating system. The OS Monitoring feature tracks and reports information about system performances, disks, SMART disks, files, processes, and services. OS Monitoring is performed periodically. If an error condition is found, an event is logged, and a State of Health (SOH) transition occurs. On subsequent checks, if the same error condition is still present, no error is logged because the previous error condition is remembered. If the error condition is no longer present on subsequent checks, a healthy or informational event is logged and SOH transitions to healthy.

Healthy or informational events are logged only after an error condition is resolved; they are not logged when the initial state is healthy.

If Command Center is used, OS Monitoring is licensed even if an RSM license is not present. OS Monitoring can be configured locally through RSM LE or remotely through Command Center.

To access the OS Monitoring parameters, select **Administration→OS Monitoring**.



For each type of OS Monitoring (overall system performance, disk, SMART disk, file, process, and services), two configuration settings determine when the monitoring is performed: Start Up Delay and Monitoring Interval.

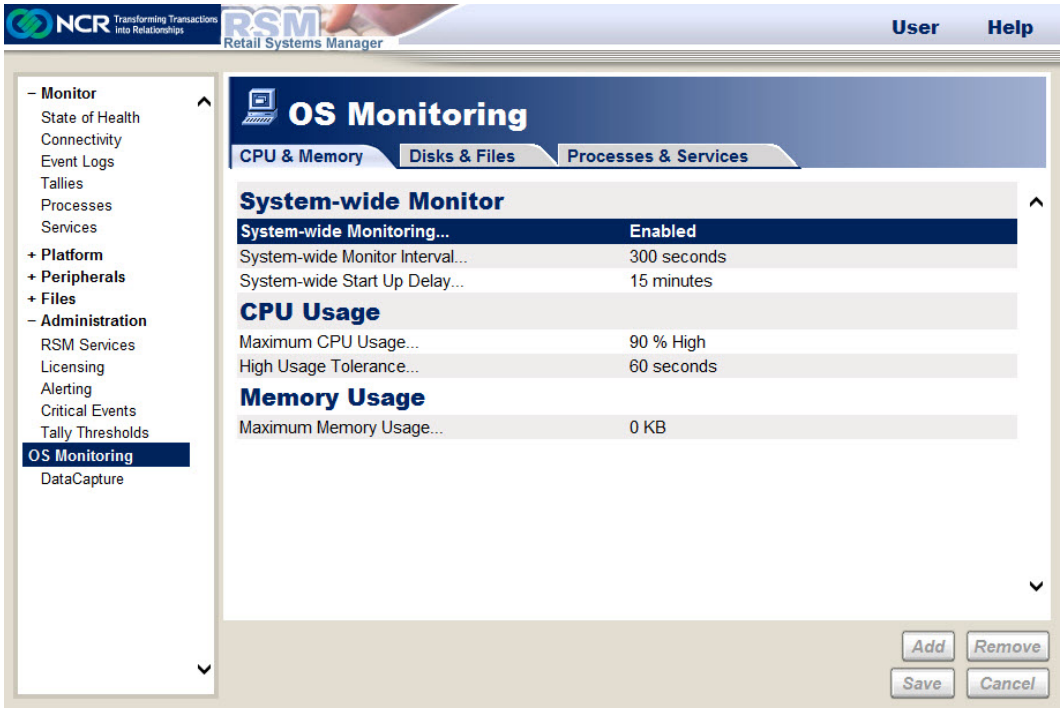
Configuration Settings	Description
Start UP Delay	The Start Up Delay setting determines how long RSM waits after start up before it begins monitoring. The default values are selected to provide the system time to fully start up before monitoring begins and to not start all monitoring at the same time. If the Start Up Delay is changed, the change takes effect on the next start up.
Monitoring Interval	The Monitoring Interval setting determines how often periodic checks occur after monitoring begins. If the Monitoring Interval is changed, the change takes effect immediately and the interval starts over. If the Monitoring Interval is set to zero, that particular OS Monitoring occurs once on start up (after the Start Up Delay period) and then ends. Any error that occurs when the checks occur on start up results in SOH transitions to an error state. These SOH errors cannot be cleared until the next time the monitoring is done and the condition that caused the error has cleared up, either on the next start up or if the monitor interval is changed to some periodic value. If you intend to use Monitor Interval of zero, you may want to consider changing the configuration of your system to use Critical Events instead of SOH for the related error conditions. If the Monitoring Interval is set to zero, the related monitoring thread ends after the check is done, to conserve system resources. If you change the monitoring interval later so that periodic checks occur, the thread is started up again as at start up. The Startup Delay period is used first as on start up, and then the periodic Monitoring Interval is used after that. If an error was logged for a condition on start up and the condition is still present after the monitoring restarts, it does not remember that it already logged an event for that error condition on the initial start up and it logs it again.

The following are the three sections defined for OS Monitoring:

- CPU & Memory
- Disks & Files
- Processes & Services

CPU and Memory

The CPU & Memory tab displays the monitoring information for CPU and memory usage of the overall system.



System–wide Monitor

The System–wide Monitor displays the following monitoring settings for CPU and memory usage:

Information	Definition
System–wide Monitoring	Refers to the option to enable or disable the monitoring of CPU and memory usage.
System–wide Monitor Interval	Refers to the time (in seconds) that determines how often the RSM application checks the CPU and memory usage. If you set the monitor interval to zero, the monitoring of CPU and memory usage occurs only at the start up of the NCRLoader.
System–wide Start Up Delay	Refers refers to the time (in minutes) before monitoring of CPU and memory usage starts at the start up of the NCRLoader. You can set this setting to provide time for the system start up to complete before monitoring begins because high activity during start up may be normal. Changes to this setting take effect on the next start up.

CPU Usage

CPU Usage displays monitoring settings for the following information:

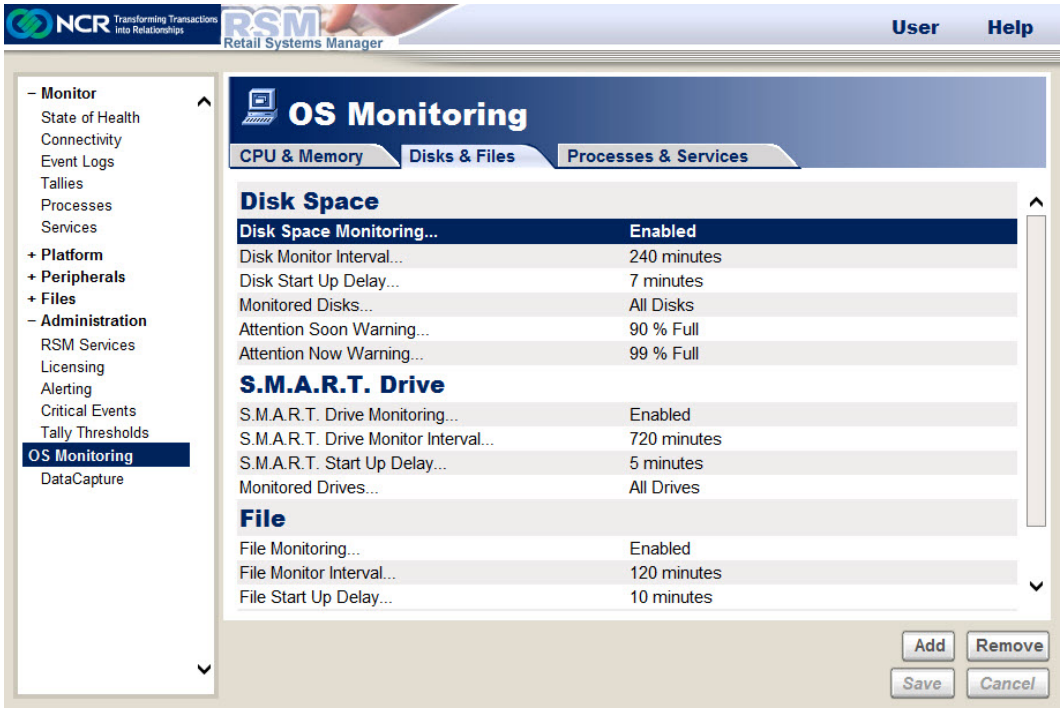
Information	Definition
Maximum CPU Usage	Refers to the maximum allocation that is permitted for CPU usage.
High Usage Tolerance	Refers to the time (in seconds) that is permitted for high CPU usage.

Memory Usage

Memory Usage displays the monitoring settings for the Maximum Memory Usage, which is the maximum allocation permitted for memory usage. If set to zero, monitoring of memory usage is disabled.

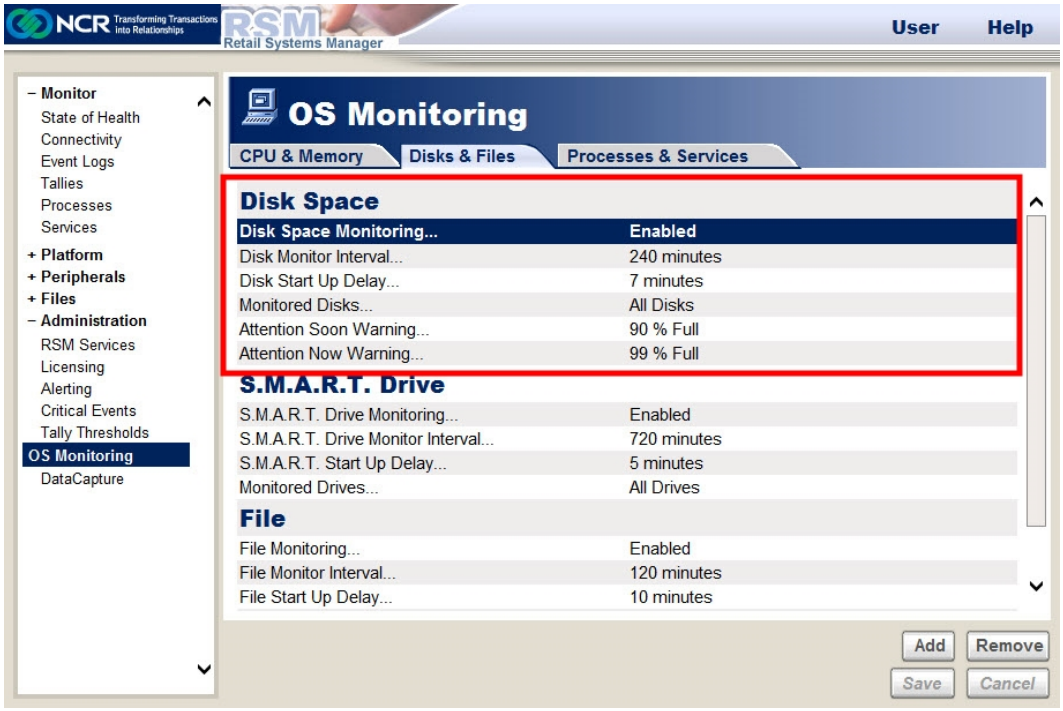
Disk and Files

The Disk and Files tab displays the monitoring information for the standard disk drives, SMART drives, and files.



Disk Space

RSM can monitor the amount of disk space used. Alerts and State–of–Health status indicate when disk usage is higher than the configured thresholds. The Disk Space section displays the following options for monitoring the disk space:



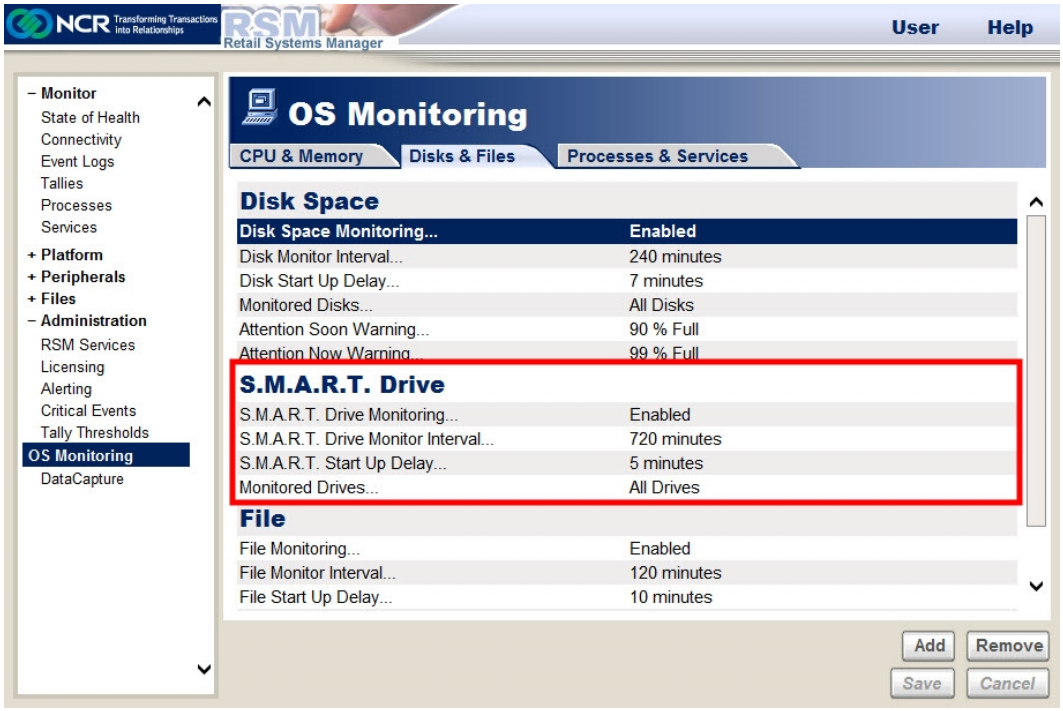
Refer to the following table for more information on the Disk Space options.

Information	Definition
Disk Space Monitoring	Refers to the option to enable or disable the monitoring of standard disk space.
Disk Monitor Interval	Refers to the time (in minutes) that determines how often the RSM application checks the standard disk drives. If you set the monitor interval to zero, the monitoring of standard disk drives occurs only at the start up of the NCRLoader.
Disk Start Up Delay	Refers to the time (in minutes) before monitoring of standard disk drives starts at the start up of the NCRLoader. You can set this setting to provide time for system start up to complete before monitoring begins because high activity during start up may be normal. Changes to this setting take effect on the next start up.
Monitored Disks	Refers to the standard disk drives that the RSM application monitors.

Information	Definition
Attention Soon Warning	Refers to the percentage of used disk space that triggers a warning that implies the disk is almost full.
Attention Now Warning	Refers to the percentage of used disk space that triggers a more severe warning that implies the disk is almost full.

SMART Drive

The RSM application monitors SMART drives at the monitor interval that you provided, and if problems exist, the application generates an alert. The SMART Drive section displays the following options for monitoring SMART drives:



Refer to the following table for more information on the SMART drive options.

Information	Definition
SMART Drive Monitoring	Refers to the option to enable or disable the SMART drives monitoring.
SMART Drive Monitor Interval	Refers to the time (in minutes) that determines how often the RSM application checks the SMART drives. If you set the monitor interval to zero, the SMART drives monitoring occurs only at the start up of the NCRLoader.
SMART Start Up Delay	Refers to the time (in minutes) before SMART drives monitoring starts at the start up of the NCRLoader. You can set this setting to provide time for system start up to complete before monitoring begins because high activity during start up may be normal. Changes to this setting take effect on the next start up.
Monitored Drives	Refers to the SMART drives that the RSM application monitors.

File

The RSM application monitors files in the system, and alerts you if a monitored file is either present or not. It can also monitor file sizes and versions. The File section displays the following options for monitoring files:

Refer to the following table for more information about the File options.

Information	Definition
File Monitoring	Refers to the option to enable or disable the monitoring of files.
Monitor Interval	Refers to the time (in minutes) that determines how often the files are checked. If you set the monitor interval to zero, the file monitoring occurs only at the start–up of the NCRLoader.
File Start Up Delay	Refers to the time (in minutes) before files monitoring starts at the start–up of the NCRLoader. You can set this setting to provide time for system start–up to complete before monitoring begins because high activity during start–up may be normal. The default values are selected so that all OS monitoring does not start at the same time. Changes to this setting take effect on the next start–up.

Files Monitored

RSM permits monitoring for file presence, size, and version. File monitoring generates State–of–Health status and alerts. The Files Monitored section is displayed only if files are being monitored.

Monitoring Files

To monitor a file, follow these steps:

1. On the OS Monitoring section, select **Add**. The Add window is displayed.

2. Select **File**, and then select **OK**. The system displays the Add File window.

3. Enter the following parameters:

Parameter	Definition
File Name	Refers to the name of the file that you want to monitor.
Path	Refers to the directory path of the file that you want to monitor.
Presence	Refers to the type of monitoring that you want, which can be any of the following: • Not Monitored—indicates that the presence of the file is not monitored. • Present—indicates that you want to make sure the file is present. • Not Present—indicates that you want to make sure the file is not present.
Maximum File Size	Refers to the maximum file size for the file before an event is triggered. Zero disables maximum file size monitoring.
Version	Monitors the version of the file to verify that the correct version is present. Leaving it blank disables version monitoring.

4. Select **Add**. The Files Monitored section indicates that the file is added for monitoring.

To stop the monitoring for a file, select the line containing the name of the file, and then select **Remove**. Confirm the removal by selecting **OK**.

Processes and Services

The Processes & Services tab displays monitoring information of the processes and services in the system.

Processes

RSM permits monitoring processes that are running and their running usage. Process monitoring generates State–of–Health status and alerts. The Processes section displays the following options for monitoring processes:

Information	Definition
Process Monitoring	Refers to the option to enable or disable the monitoring of processes.
Process Monitor Interval	Refers to the time (in minutes) that determines how often the RSM application checks the processes. If you set the monitor interval to zero, the process monitoring occurs only at the start–up of the NCRLoader.
Process Start Up Delay	Refers to the time (in minutes) before process monitoring starts at the start–up of the NCRLoader. You can set this setting to provide time for system start–up to complete before monitoring begins because high activity during start–up may be normal. Changes to this setting take effect on the next start–up.

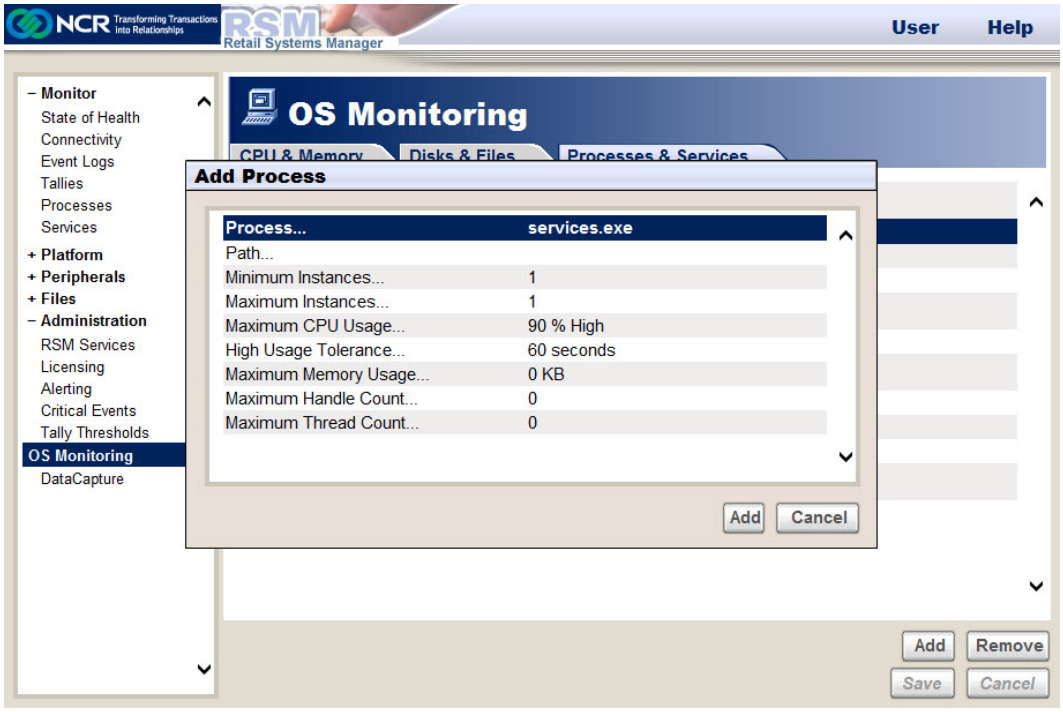
Monitoring Processes

To monitor a process, follow these steps:

1. On the OS Monitoring section, select **Add→Process**, and then select **OK**.

The system displays the Monitored Process window.

2. Select a process from the drop–down menu, and then select **OK**. The system displays the Add Process window.



3. Enter the following parameters:

Parameter	Definition
Process	Refers to the process you want to monitor. When configuring the process to be monitored, a drop–down box permits selection of one of the processes currently running. If you select *Unlisted Process*, you can enter another process name. If a list of currently running processes is not available, the system does not display the drop–down box. You must then enter the process name.
Path	Refers to the directory path of the process. The path is optional. If you do not specify a path, the RSM application monitors any process matching the process name. If you specify a path, ensure that both the process name and path match a running process.
Minimum Instances	Refers to the minimum number of copies of the process that can run at the same time. A zero input means that the minimum number of instances of the process is not monitored.
Maximum Instances	Refers to the maximum number of copies of the process that can run at the same time. A zero input means that the maximum number of instances of the process is not monitored.
Maximum CPU Usage	Refers to the maximum percentage of CPU usage that the process can use without generating an alert. Alerts are generated only if the CPU usage exceeds the threshold for High Usage Tolerance rather than generating alerts for brief spikes in CPU usage. A zero input means that the maximum percentage of CPU usage of the process is not monitored.
High Usage Tolerance	Refers to the time (in seconds) that determines how long the Maximum CPU Usage can last until an alert is generated. A zero input means that the high usage tolerance of the process is not monitored.
Maximum Memory Usage	Refers to the maximum memory usage (in MB) that the process can use without generating an alert. A zero input means that the maximum memory usage of the process is not monitored.

Parameter	Definition
Maximum Handle Count	Refers to the maximum number of handles the process can use without generating an alert. A zero input means that the maximum number of the handles of the process is not monitored.
Maximum Thread Count	Refers to the maximum number of threads the process can use without generating an alert. A zero input means that the maximum number of the threads of the process is not monitored.

4. Select **Add**. The system displays the process in the Processes Monitored section.

To stop monitoring a Process, select the line containing the name of the Process, and then select **Remove**. Confirm the removal by selecting **OK**.

Services

RSM permits monitoring of services with Started or Stopped states and their start–up type. Service monitoring generates State–of–Health status and alerts. The Services section displays the options for monitoring services:

Information	Definition
Service Monitoring	Refers to the option to enable or disable the monitoring of services.
Service Monitor Interval	Refers to the time (in minutes) that determines how often the RSM application checks the services. If you set the monitor interval to zero, the service monitoring occurs only at the start–up of the NCRLoader.
Service Start Up Delay	Refers to the time (in minutes) before service monitoring starts at the start–up of the NCRLoader. You can set this setting to provide time for system start–up to complete before monitoring begins because it takes a little time for services to start up and get to their normal state after start–up. Changes to this setting take effect on the next start–up.

Monitoring a Service

To monitor a service, follow these steps:

1. On the OS Monitoring section, select **Add→Service**, and then select **OK**.

The system dispalys the Monitored Service window.

2. Select a service from the drop–down menu, and then select **OK**. The system displays the Add Service window.

3. Enter the following parameters:

Parameter	Definition
Service	Refers to the service that you want to monitor. When configuring a service to be monitored, a drop–down box permits selection of one of the services currently registered. If you select *Unlisted Service*, you can enter another service name. If a list of currently registered services is not available, the system does not display the drop–down box. You must then enter the service name.
Expected Startup Type	Specifies whether to monitor the Startup Type of the service, and if monitored, what Startup Type is expected. If the actual Startup Type is not the same as this setting, the RSM application logs an event and generates an alert. The following options are available: • Automatic (Delayed Start) • Automatic • Manual • Disable • Not Monitored **Note:** The Automatic (Delayed Start) option displays only on systems running on Windows 7 operating system.
Expected Status	Specifies whether to monitor the Status of the service, and if monitored, what Status is expected. If the actual Status is not the same as this setting, the RSM application logs an event and generates an alert. The following options are available: • Started • Stopped • Not Monitored

4. Select **Add**. The system displays the service in the Services Monitored section.

To stop monitoring a Service, select the line containing the name of the Service, and then select **Remove**. Confirm the removal by selecting **OK**.

Data Capture

Data Capture is for use by NCR developers when a problem arises with NCR software. The NCR developer provides the information for the Trace Mask and the Level Mask, based on the problem to be solved.

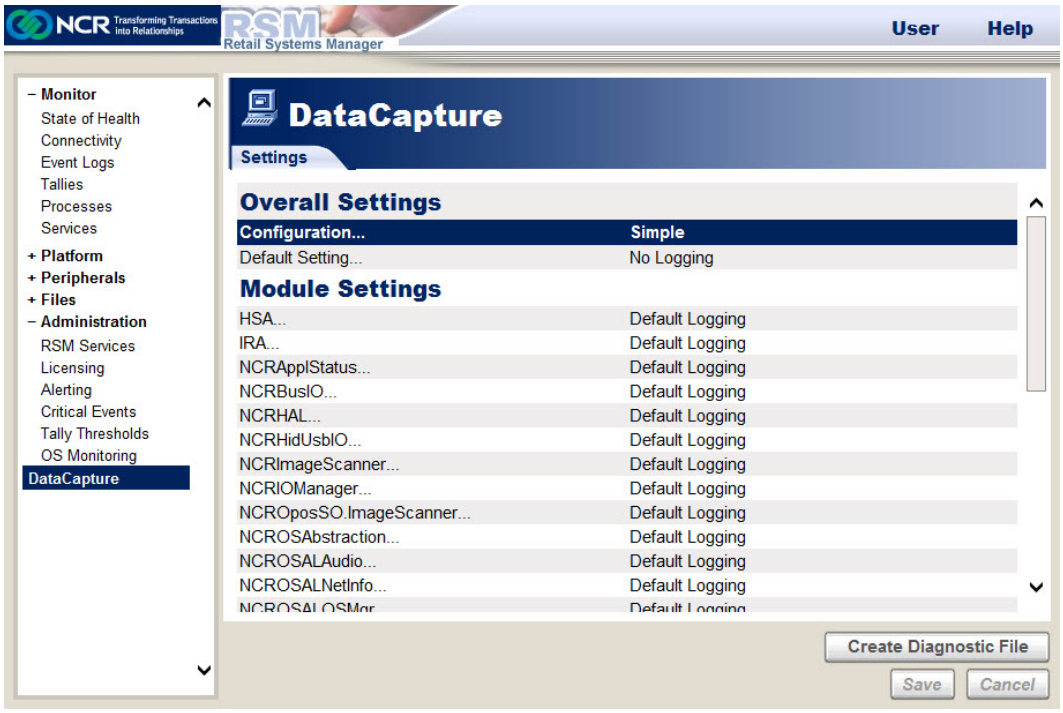
Data Capture Versions

There are two versions of Data Capture:

- The version used with OPOS 2.x, the NCRFSM, and RSM SNMP have different mask settings than displayed in the previous screens. When you change the masks for this version of Data Capture, the software that is writing to data capture must be restarted. For example, in the case of OPOS, you may have to restart the retail application if that is what has loaded the OPOS controls. For NCRFSM data capture, you must restart NCRFSM by restarting the NCRLoader service. You can restart RSM SNMP by restarting the SNMP service.
- The version used by Retail Controls 3.x, RSM, and the Base Platform modules is the version with the settings displayed in the previous screens. In RPSW 2.3 and later and RSM 2.1 and later, the settings take effect immediately after they are saved through the RSM user interface. In older releases, these data capture settings do not take effect until the NCRLoader service is restarted.

For Retail Controls, data capture settings are also listed with the profile settings. OPOS 2.x data capture settings are set only with the profile settings and are per profile. Retail Controls 3.x data capture settings may be set on the data capture page or with the profile settings. The Retail Controls 3.x data capture settings are per module, not per profile.

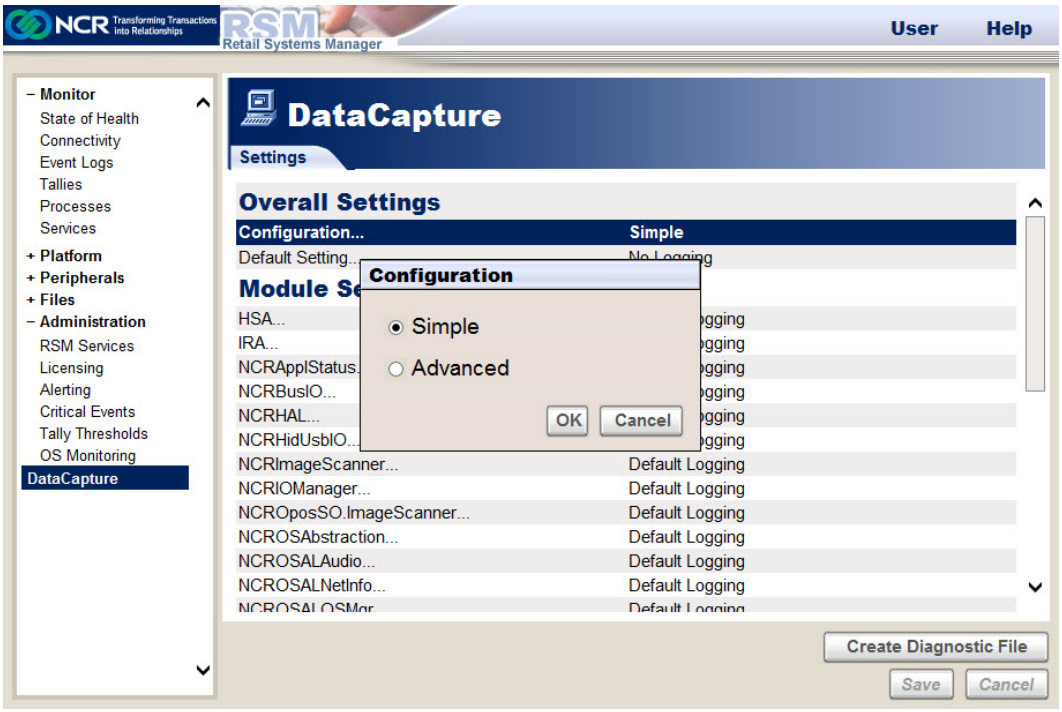
Data Capture information is accessed by selecting **Administration→DataCapture**.



Configuring the Data Capture Settings

Configuring data capture affects the menu options for the other settings. To configure the data capture settings, follow these steps:

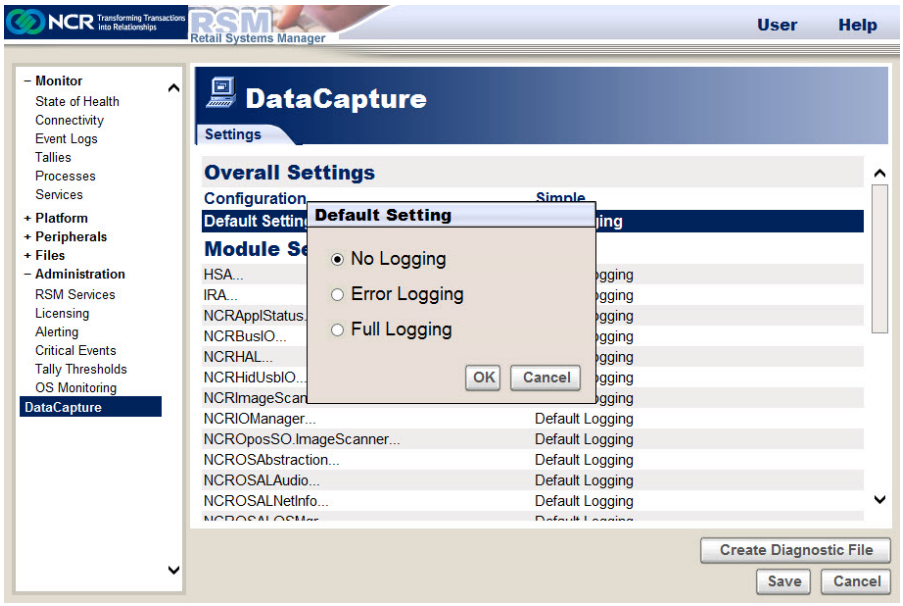
1. On the Overall Settings section of the DataCapture window, select **Configuration**. The system displays the Configuration window.



2. Select the configuration setting:
   - Simple—permits easily selecting the most commonly used data capture settings.
   - Advanced—provides you the functionality to select the specific tracing masks for data capture.

   In most cases, Simple configuration provides the necessary options and is easier to use.

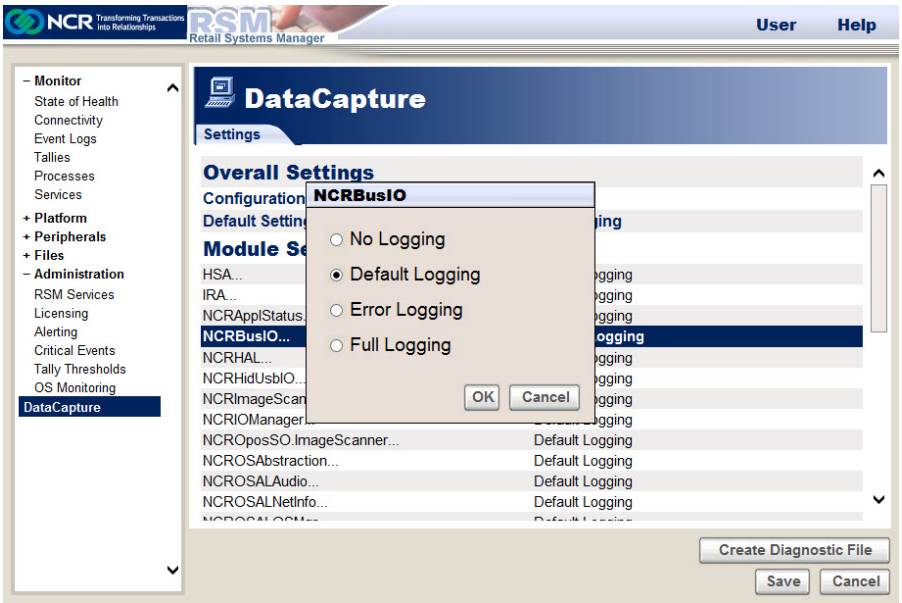
3. If you selected the **Simple** configuration, select **Default Setting**. The system displays the Default Setting window.



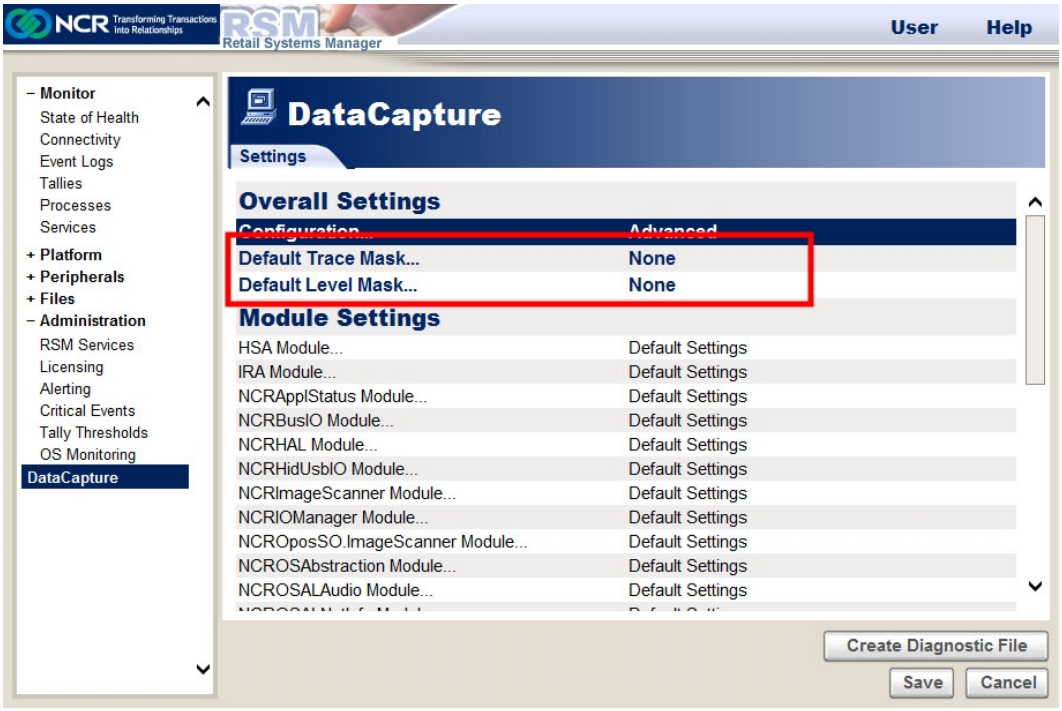
The Default Setting is the data capture mask used for all modules listed under Module Settings. These modules are configured for Default Logging.

a. Select the default setting, and then select **OK**.

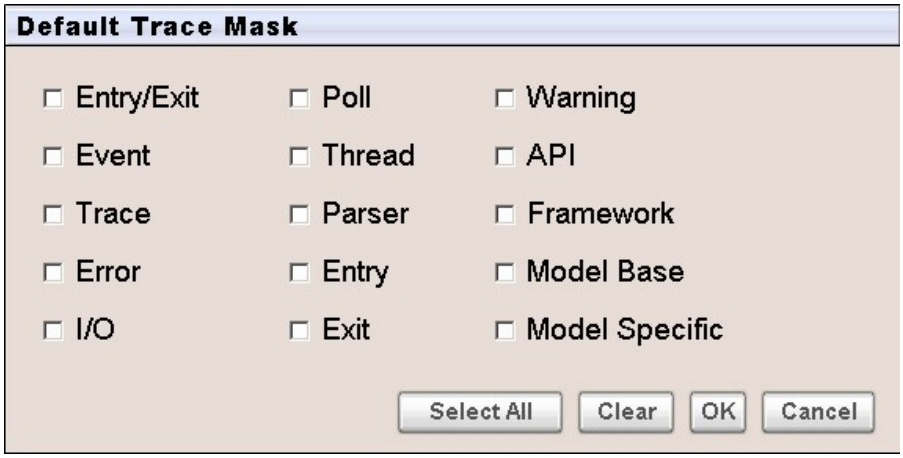
b. If you want to configure a module and set it to a logging that is different from the default setting, select the module and then select any of the following options:



4. If you selected the **Advanced** configuration, the DataCapture section additionally displays the Default Trace Mask and the Default Level Mask settings.



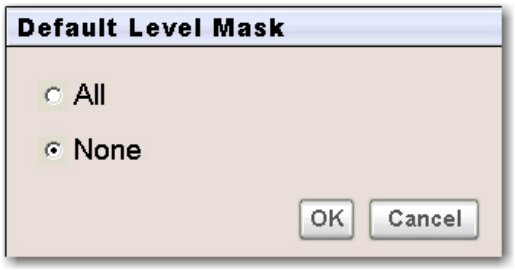
a. Select **Default Trace Mask**, and then select the trace mask settings from the default Trace Mask window.



Note: You can select more than one trace mask.

b. Select **OK**.

c. Select **Default Level Mask**, and then select the level mask setting, whether **All** or **None**.



d. Select **OK**.

e. If you want to configure a module and set it to a setting that is different from the default setting, select the module and then select the desired setting.

5. Select **Save** in the DataCapture section to save the changes.

Creating a Diagnostic File

To simplify retrieval of information for problem resolution, a GDF (Get Diagnostics File) `.zip` file can be created rather than gathering the files individually. The GDF feature is available with RPSW 2.3 or RSM 2.1 and higher. If running an earlier version of RPSW or RSM, the files must be gathered manually.

A GDF file is a zipped file that contains the following:

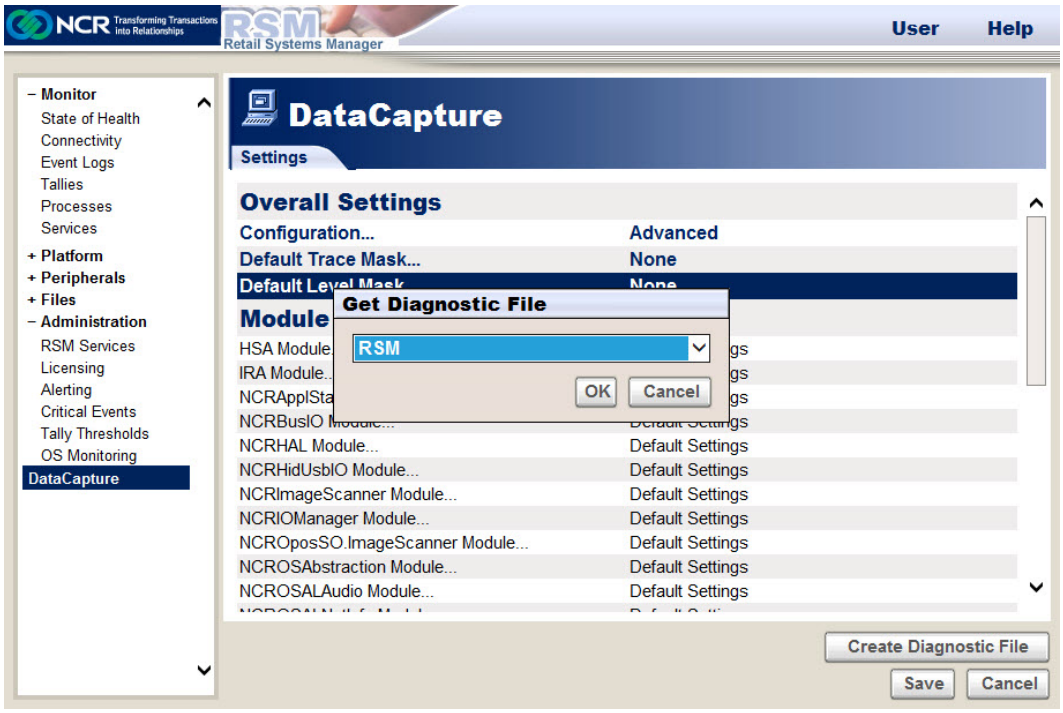
- Windows System and Application Event logs (`*.evt`)
- Dr. Watson log file (`drwtsn32.log`)
- NCR registry key (`HKLM\SOFTWARE\NCR`)
- OLEforRetail key (`HKLM\SOFTWARE\OLEforRetail`)
- NCR configuration files
- NCR log files
- RSM license files (`RSM\Website\XML\*.dat`)
- RSM local databases
- Other files used for investigating problems

Warning: When a problem occurs, the files should be retrieved immediately.

If the NCRLoader service is restarted or the system is rebooted, new log files are created and the old files are renamed to `*.bak` and older `*.bak` files are lost. This problem also occurs when a log file reaches its maximum size. If the log files are not retrieved immediately when the problem occurs, information about the problem may be lost.

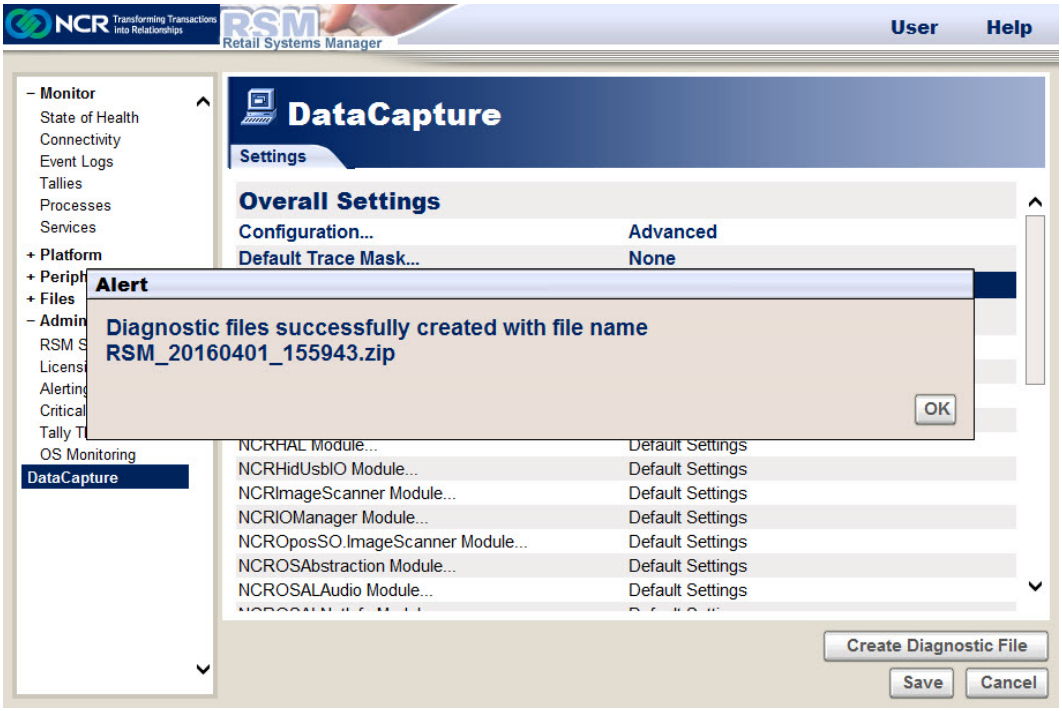
To create a GDF file, follow these steps:

1. Select the system from which the information is to be retrieved (for managed systems).
2. Select **Administration→DataCapture**.
3. Select **Create Diagnostic File**. The system displays the Get Diagnostic File window.



4. Select from the options, and then select **OK**. The system launches a utility to create the GDF file on the system where the information is to be gathered.

An Alert window is displayed after the GDF file is created.



The file name is of the following form so that creating a file does not overwrite the files previously created:

`<product>_<date>_<time>.zip`

Example: `RSM_20060810_133314.zip`

For RPSW 2.x and 3.x releases, the GDF file created is stored in `C:\Program Files\NCR\RSM\Diags` on the system where the information is gathered.

For RPSW 4.0 and up, the path for the diagnostic files is at `%ALLUSERSPROFILE%\Application Data\NCR\RSM\Diags`. The `%ALLUSERSPROFILE%` variable is an environment variable that points to different locations depending on the operating system.

Note: Prior to RSM Release 3.0.3, there was no file retrieval, so to get the file from a remote system using an older version of RSM, you must manually retrieve it. With RSM 3.0.3 and up, you can use the RSM file retrieval feature to move files from RSM LE to RSM SE or RSM EE. For more information, refer to the *NCR Retail Systems Manager Software User's Guide* (B005–0000–1518).

If you cannot use the user interface to create the GDF file, you can create the `.zip` file from a command prompt. The command file for creating the file from a command prompt is `RSMlogs.cmd`.

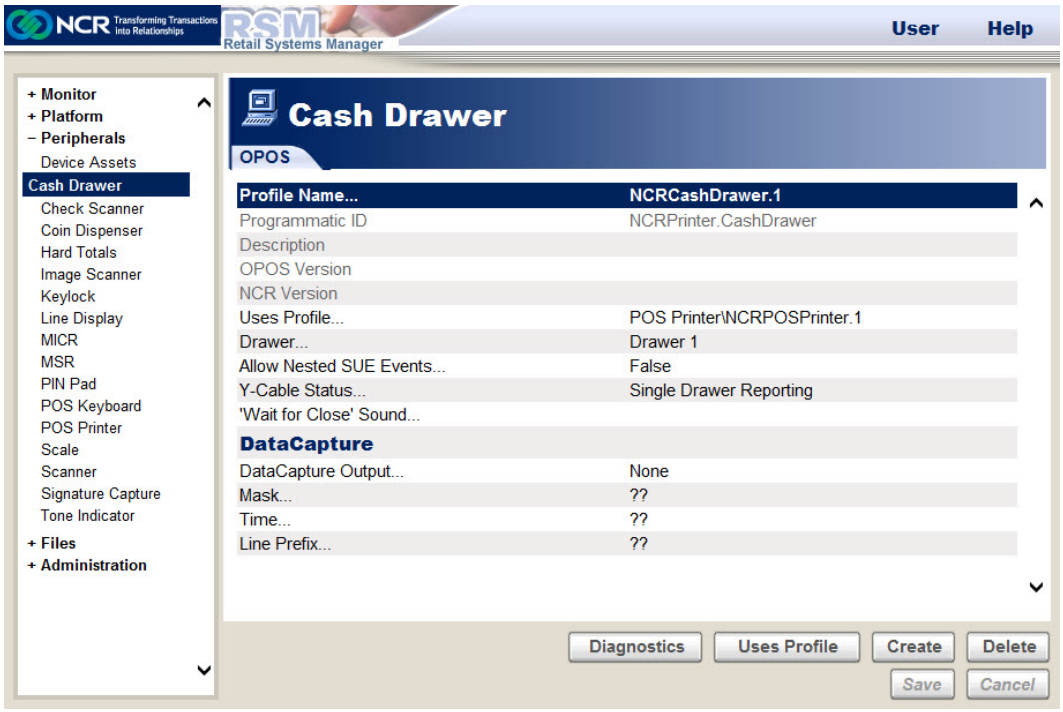
Note: It is best to run `RSMLogs.cmd` as an Administrator. If the current logged in user cannot access the registry or Windows event logs, `RSMLogs.cmd` will not be able to collect some items in the diagnostic file.

Using the Peripherals section

Peripherals consist of OPOS and JavaPOS retail peripherals and the Device Assets.

OPOS and JavaPOS Retail Peripherals

Each of the retail peripherals has a configuration screen and a Diagnostics button to test the functionality of the terminal. If both OPOS and JavaPOS are installed, you can select the desired interface by selecting the OPOS or the JavaPOS tab.

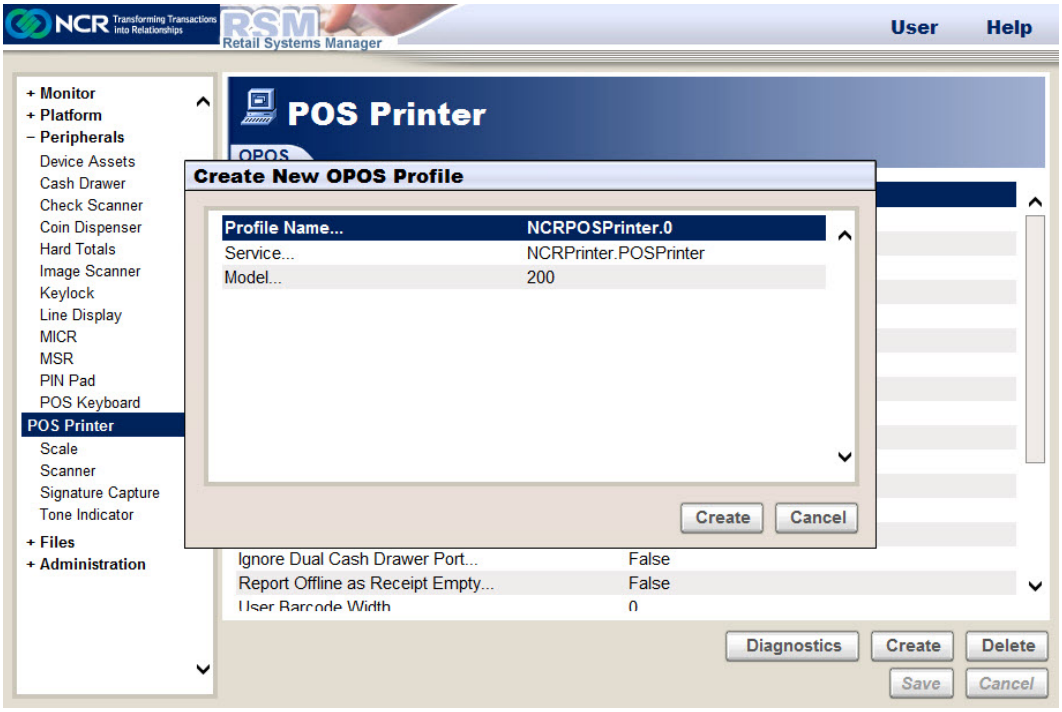


When RPSW is installed, the default profiles for the retail peripherals you chose are installed. These profiles provide some default configurations for the most common uses of the peripherals. You can change a profile's configuration or create new configurations based on your needs.

Creating a New Profile

To create a new profile, follow these steps:

1. Under the Peripherals section, select a device. In this example we are adding a new printer, so the POS Printer Device is selected.
2. Select **Create**. The system displays the Create New OPOS Profile window.

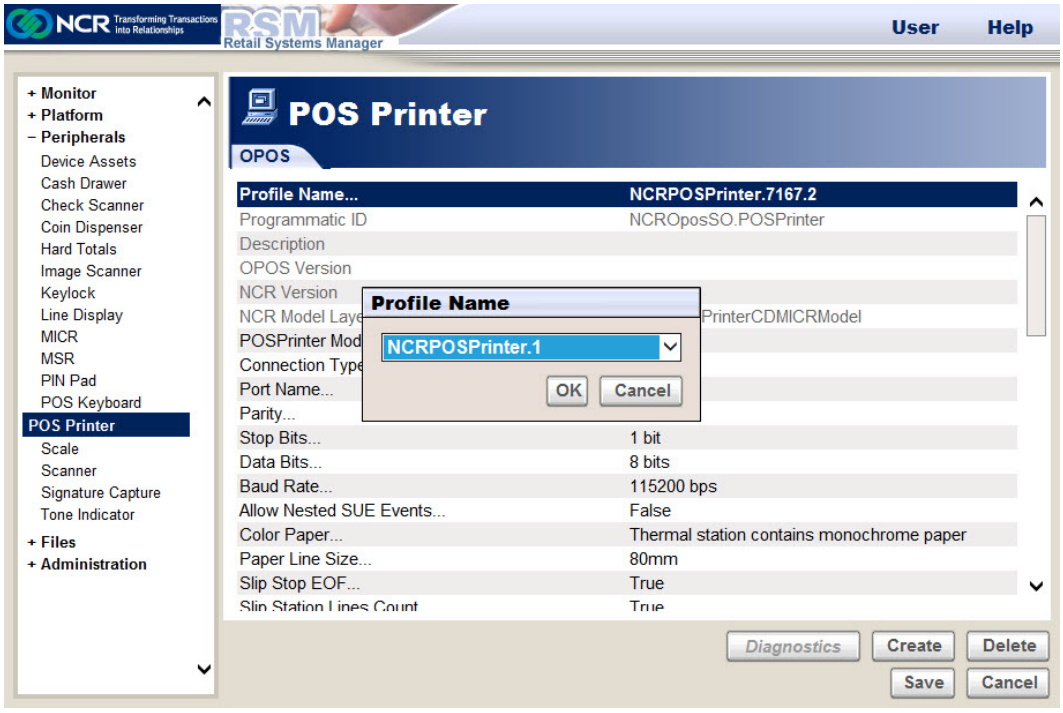


3. Enter the following parameters:
   - **Profile Name**—refers to the name of the profile. If your application uses this profile, you must match the profile name to the name that your application uses for this device.
   - **Service Object**—refers to the Programmatic ID of the device. The Programmatic ID is different depending on whether you are using OPOS 2.x, JavaPOS 2.x, OPOS 3.x, or JavaPOS 3.x. The OPOS 3.x Service Objects always have the format "NCROposSO.xxxxxxx". It is preferable to use the OPOS 3.x objects because of future enhancements that are being planned.
   - **Model**—refers to the profile parameter value. This option displays only when you select a 3.x profile. The Model parameter is available for 2.x profiles after the profile is created.
4. Select **Create** to continue creating the profile.

Changing a Profile

To change a profile, follow these steps:

1. Select **Profile Name**. The system displays the Profile Name window.



2. Select one of the available profiles from the drop–down list, and then select **OK**. The system displays the configuration of the selected profile.

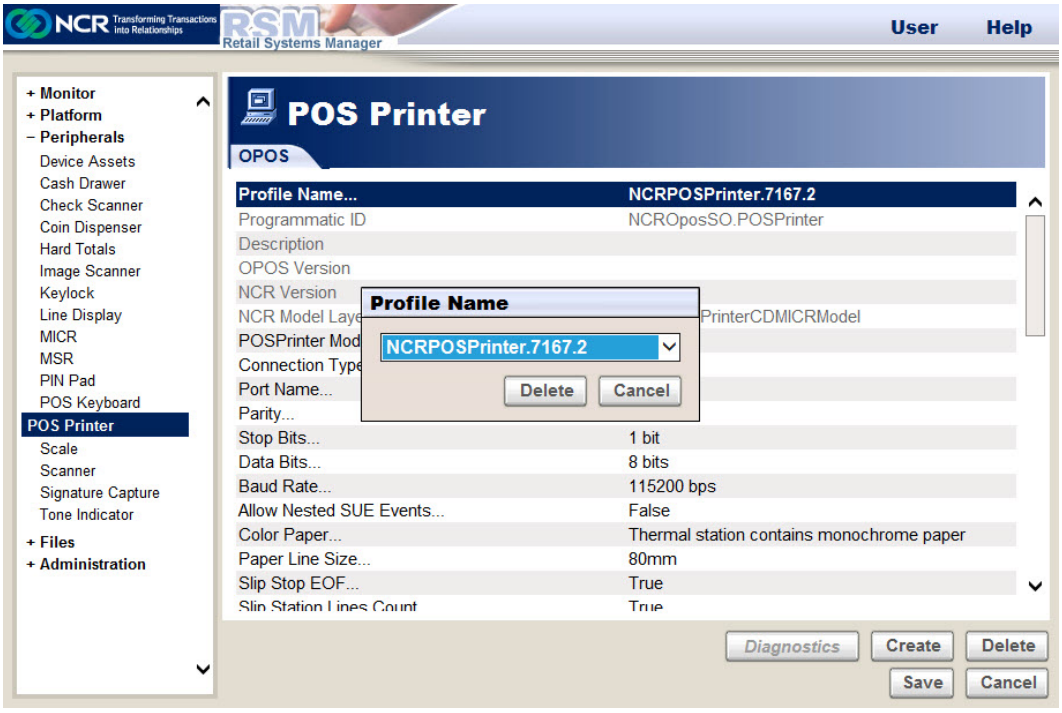
   You can change any parameter that is not grayed out by selecting that parameter and making the changes. Fields in bold font are changes that have not been saved.

3. After making the changes, select **Save**.

Deleting a Profile

To delete a profile, follow these steps:

1. Select the **Delete**, and then select the profile name of the profile you want to delete.



2. Select **Delete** from the Profile Name window.

Performing Diagnostics

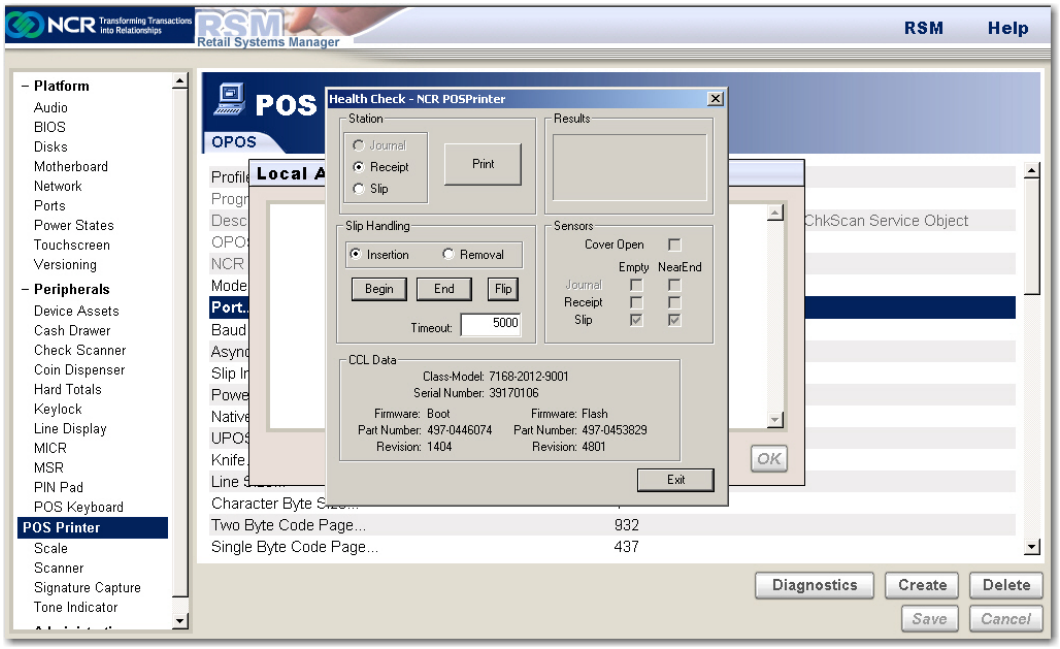
You can perform two different types of diagnostics on the peripherals:

- Interactive Diagnostics—require interaction from the user, such as swiping a card and scanning an item.
- Non–interactive Diagnostics—test the internal software or hardware and do not require user interaction.

To perform diagnostics, follow these steps:

Note: In this example, the desired profile is POS Printer.

1. Select **Peripherals→POS Printer→Diagnostics→Local Attended Diagnostics**. The system displays this window.



The printer test permits you to select a specific print station and other parameters associated with that printer.

2. Select **Print**. The selected printer prints some information.

Using the Platform section

The Platform section displays the platform devices. These are system devices that are not controlled by OPOS or JavaPOS software. The Platform section may provide some configuration information or other information about the device.

Platform Devices

The following are the devices that are not controlled by OPOS or JavaPOS:

- **Audio**
  - Audio volume
  - Diagnostics button tests Stereo, Left, or Right Speaker
- **BIOS**
  - BIOS Information
    - BIOS Version
    - BIOS Release Date
    - BIOS Vendor
    - BIOS ROM Size
    - BIOS OEM String
  - System Information
    - NCR Class & Model

        - NCR Serial Number
        - Manufacturer
        - Motherboard ID
    - **Disks**—provides information for each drive in the system
        - Disk Information
            - Number of Physical Disks
            - Physical Drive 0 Size
            - Number of Logical Disks
            - Logical A Type (for each drive in the system)
            - Logical C Type
            - Logical C Total Size
            - Logical C Free Space
            - Logical D Type
            - SMART drive information where available.
            - Diagnostics button is used to select the drive to display that drive's properties.
    - **Display** (legacy systems, 7610, and 7611 terminals)
        - Panel Type
        - Brightness
        - Contrast
        - Screen Blank Delay
    - **Memory** (if licensed)
        - Physical Memory
        - Available Memory
        - Memory Usage
        - Page File Size
        - Available Page File Size
    - **Motherboard**
        - NCR Class & Model
        - NCR Serial Number
        - Manufacturer
        - Manufacturer ID
        - Processor

- System–wide CPU Usage
- Hardware Monitor Information
  - Processor Temperature
  - System Temperature
  - Processor Fan
  - Various Voltages (based on terminal type)

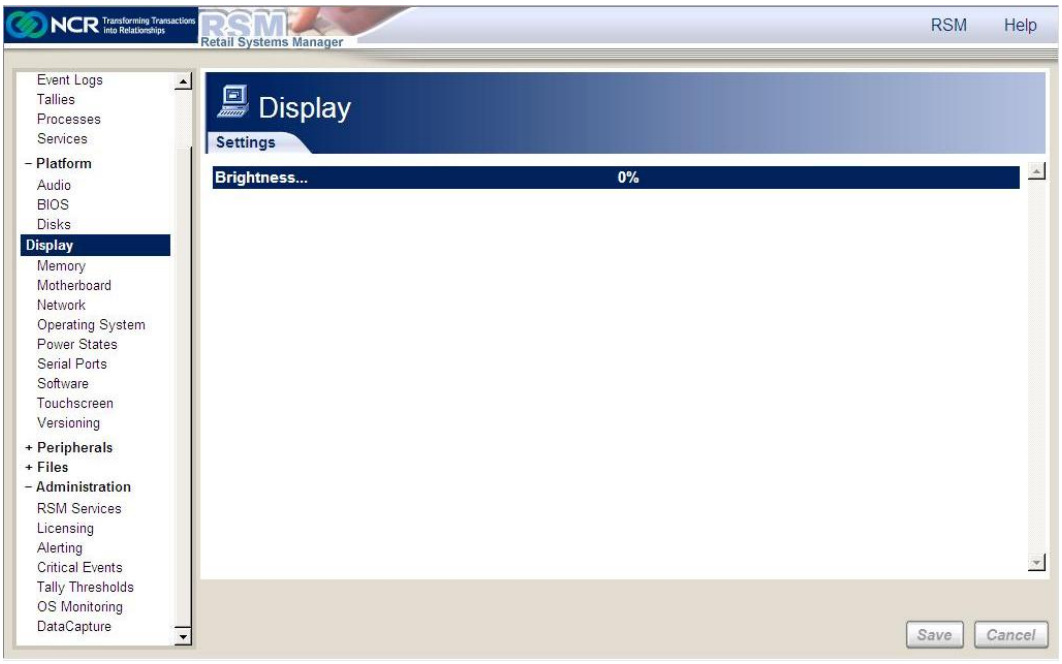
- **Network**
  - Computer Name
  - Number of Adapters
  - Adapter 1 MAC Address (for each adapter)
  - Adapter 1 IP Address (for each adapter)
  - TCP and UDP port usage
  - Diagnostics button is used to test Ethernet or WaveLAN communications. If hardware specific diagnostics are not available for the network adapter, selecting Ethernet brings up the Control Panel so that you can check the Network Connections.
- **Operating System** (if licensed)
  - Version
  - Build
  - Service pack
  - Hot fixes
  - User Name
  - System Drive
  - System Root
  - WinDir
  - Temp
  - OS
  - Path
  - ClassPath
  - OS Image
    - NCR Part Number
    - NCR LPIN
    - NCR Version

- **Power States** (For more information, refer to *Configuring Power States* on page 165.)
- **Serial Ports**—identifies the COM Ports attached to the system.
  - Diagnostics button is used to select a COM port, and then a turnaround test is performed if a turnaround plug is installed on that port.
- **Software** (if licensed)—lists the software installed on the system.
- **Touchscreen**
  - Controller
  - Diagnostics button is used to test a touch screen.
- **UPS** (only if installed with custom install)
- **Versioning**—version numbers for the modules in the following categories:
  - RSM Version
  - Common
    - Common Kernel Drivers
    - Common Libraries
    - Common IO Libraries
    - Common OSAL Libraries
    - Common Utilities
  - Platform
    - Platform Agents
    - Platform HAL
    - Platform Kernel Drivers
    - Platform Libraries
  - Retail Controls
    - JavaPOS Retail Controls
    - Retail Control Models
    - OPOS Retail Controls
  - RSM

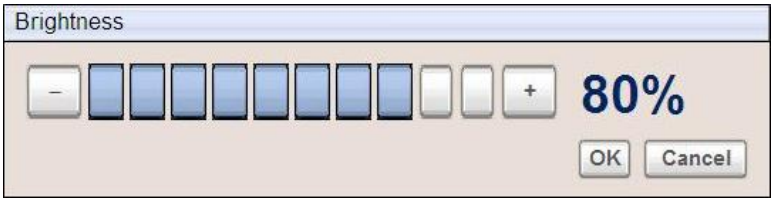
Changing the Display Brightness Settings

You can change the brightness of the display screen on terminals 7610, 7611, and some legacy terminals through the Platform section of the RSM user interface. To change the brightness settings of the display screen, follow these steps:

1. On the RSM window, select **Platform→Display**. The Display section displays the settings available.



2. Select **Brightness**. The system displays the Brightness window.



3. Select the brightness percentage on the slider control. The color blue represents the brightness percentage that is currently set. You can also set the brightness percentage by clicking the plus (+) and minus (-) buttons.
4. Select **OK**, and then select **Save** on the Display section. The display screen of the terminal automatically changes according to the brightness settings you have selected.

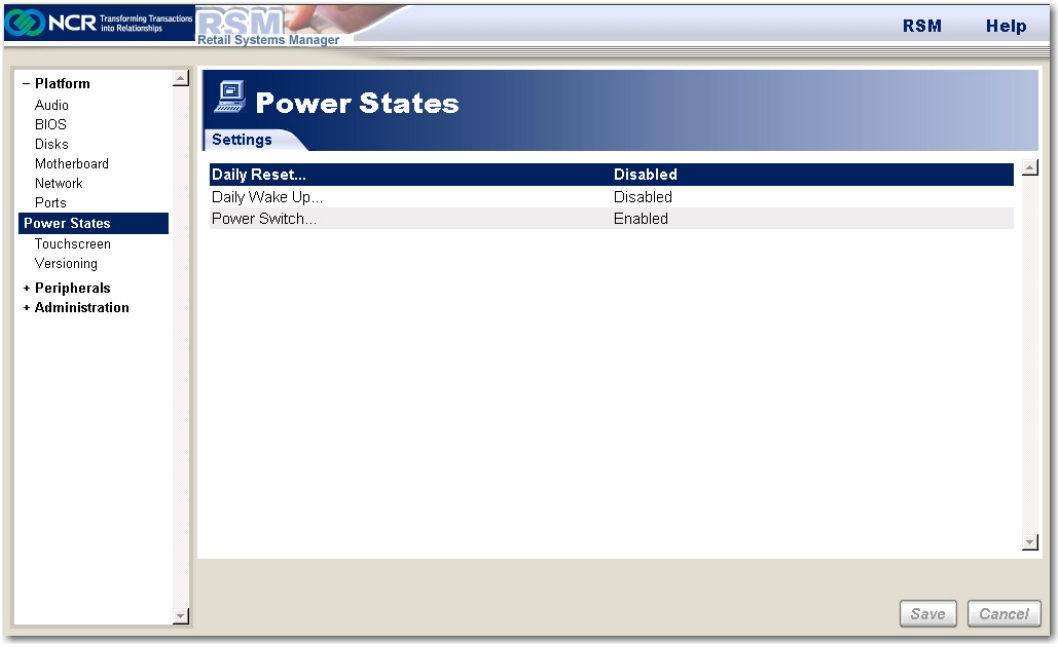
If you modify the brightness settings of a client or terminal through the server, the change reflects automatically even without refreshing the terminal. If you modify the brightness settings on the terminal itself, the change reflects only after selecting Save.

Configuring Power States

The Power States for a System can be controlled in RSM. The following controls are provided:

- Restart (if licensed)
- Shutdown (if licensed)
- Daily Reset
- Daily Wake Up (wake on alarm)
- Power Switch (on terminals that support power switch disable)
- Reboot Type (cold or warm)
- Boot Order (normal or network)

The various models of retail systems support different power states. To access the Power States, select **Platform→Power States**.



Power States Restrictions

Standby is supported only if the system and the operating system support ACPI and standby. Standby is not supported on Windows NT.

Some of the 7402, 7457–4xxx, and 7458–4xxx terminal systems do not wake (Wake–on–LAN or Daily Wake Up) from the off state (depending on the BIOS version). Aside from these terminals, there may be more terminals that do not support this control.

Some systems may require OS, network driver configuration, or BIOS changes to enable Wake–on–LAN.

The Power Switch setting (enable or disabled) is supported only on the following systems:

- 7452
- 7453
- 7456
- 7457–1xxx and 2xxx
- 7458–1xxx and 2xxx

The Reboot Type and Boot Order settings, which affect the corresponding BIOS settings, are supported on the following systems:

- 7402
- 7403
- 7457–4xxx
- 7458–4xxx
- 7459

Active Management Technology (AMT)

AMT support for NCR POS terminals (7459, 7403, and 7409) is a feature requiring RSM Server support. For more information, refer to the *NCR Retail Systems Manager User's Guide* (B005–0000–1518).

Appendix A: Microsoft™ SNMP Service Settings

Overview

There are three settings that need to be set in the Microsoft SNMP Service to load the RSM SNMP agent. Normally, these settings are set by the RPSW installation or by the RSM user interface. However, these settings may need to be checked manually if RSM SNMP is not running as expected or if other software has changed the Microsoft SNMP configuration. These are the following settings:

- Allow Service to interact with Desktop
- NCRLoader service
- RSM SNMP Agent

Allow Service to interact with Desktop

The *Allow Service to interact with the Desktop* setting is set by the RPSW installation or when you enable SNMP from within RSM. Normally, the user should not have to adjust this setting unless other software has changed it.

If this setting for the NCRLoader service and the SNMP service are not set the same way, RSM SNMP starts a separate NCRFSM process instead of using the one started by NCRLoader. State of health and critical events does not work properly if more than one NCRFSM process is running.

NCRLoader Service

The SNMP service is dependent on the NCRLoader service running. In the Microsoft SNMP properties under the Dependencies tab, the NCRLoader service should be listed, which is normally set by the RPSW installation as long as the Microsoft SNMP service was installed prior to installing RPSW.

If you install RPSW before you install the Microsoft SNMP Service, you must manually edit the registry to set this dependency. The install sets the following REG_MULTI_SZ Registry Entry:

```
HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\DependOnService
```

To manually edit the registry, do any of the following:

- On some operating systems, you can just select this value in `regedit` and add the string `NCRLoader` to the list.
- On other operating systems, you may have to export the current setting to a `.reg` file, add NCRLoader to the setting in the `.reg` file, and import the `.reg` file.

Example of `.reg` file entry before NCRLoader is added to the setting:

```
"DependOnService"=hex
(7):45,00,76,00,65,00,6e,00,74,00,4c,00,6f,0067,00,00,00,\00,00
```

After NCRLoader is added, *DependOnService* should look like the following:

```
"DependOnService"=hex
(7):45,00,76,00,65,00,6e,00,74,00,4c,00,6f,0067,00,00,00,\

4e,00,43,00,52,00,4c,00,6f,00,61,00,64,00,65,00,72,00,00,00,00,00
```

Note: This setting may vary from this example if other dependencies are already configured on your system.

RSM SNMP Agent

The Microsoft SNMP Service must be configured to load the RSM SNMP Agent. This setting is set in the RSM LE or RSM SE user interface by selecting **Administration→Alerting→SNMP agent (Enable)**.