Radia Client Automation Enterprise Out of Band Management

For the Windows® operating systems

Software Version: 9.00

User Guide

Document Release Date: April 2013

Software Release Date: June 2013

Legal Notices

Warranty

The only warranties for products and services are set forth in the express license or service agreements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Persistent Systems shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Persistent Systems or its licensors required for possession, use or copying. No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Persistent Systems.

Copyright Notice

Trademark Notices

Acknowledgements

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software written by Daniel Stenberg (daniel@haxx.se).

This product includes OVAL language maintained by The MITRE Corporation (oval@mitre.org).

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://support.persistentsys.com/

This site requires that you register for a Persistent Passport and sign in. Register online at the above address.

For more details, contact your Persistent sales representative.

Support

Persistent Software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by being able to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Submit enhancement requests online
- Download software patches
- Look up Persistent support contacts
- Enter into discussions with other software customers
- Research and register for software training

To access the Self-solve knowledge base, visit the Persistent Support home page.

Note: Most of the support areas require that you register as a Persistent Support user and sign in. Many also require an active support contract. More information about support access levels can be found on the Persistent Support site.

To register for a Persistent Support ID, go to: Persistent Support Registration.

Contents

Chapter 1

Introduction

Radia Client Automation (RCA) server enables you to use Out of Band Management (OOBM) features to perform out of band operations regardless of system power or operating system.

In band management refers to operations performed when a computer is powered on with a running operating system.

Out of band management refers to operations performed when a computer is in one of the following states:

- The computer is plugged in but not actively running (off, standby, hibernating).
- The operating system is not loaded (software or boot failure).
- The software-based management agent is not available.

Overview

The RCA server supports Out of Band Management of Intel vPro devices and DASH-enabled devices.

Intel vPro devices can be discovered and managed even when powered off because the Intel Active Management Technology (AMT) firmware stores information about them in non-volatile memory and provides a set of management operations that can be invoked by a remote management console. DASH is one of several Distributed Management Task Force (DMTF) Management Initiatives, providing a comprehensive framework for syntax and semantics necessary to manage computer systems, independent of machine state, operating platform, or vendor.

Both technologies provide remote diagnostics and repair capabilities, that include hardware-based remote-boot and text console-redirection.

For more information on Intel vPro and DASH devices, see "Setting Up vPro and DASH Devices" on page 20.

OOBM features enable you to use processes such as Discover, Heal, and Protect for devices in your RCA environment.

- **Discover**
  OOBM enables you to identify hardware and software assets in your environment. This helps you determine specifications for the hardware on devices, identify applications on devices, compatibility issues, and so on.
- **Heal**
  OOBM makes use of operations such as Remote Operations and Event Management to help you identify, diagnose, and repair any software, operating system, and hardware failures. Event Management is relevant only for vPro devices.
- **Protect**
  OOBM helps you protect only vPro devices from malicious software and worm proliferation. It

monitors the agents running on the devices and this enables it to quarantine worm infected devices in the network.

For more information on Discover, Heal, and Protect, see "OOBM Features" on page 144.

Abbreviations and Variables

Abbreviations Used in this Guide

Abbreviation	Definition
RCA	Radia Client Automation
Core and Satellite	RCA Enterprise environment consisting of one Core server and one or more Satellite servers.
CSDB	Configuration Server Database

Variables Used in this Guide

Variable	Description	Default Values
`InstallDir`	Location where the RCA server is installed	For a 32-bit OS: `C:\Program Files\Hewlett-Packard\HPCA` For a 64-bit OS: `C:\Program Files(x86)\Hewlett-Packard\HPCA`
`SystemDrive`	Drive label for the drive where the RCA server is installed	C:

OOBM Workflow

This section describes the steps you need to follow to successfully implement OOBM in the RCA environment.

1. **Identify and set up devices**
   This is a prerequisite for using OOBM. You need to identify and set up Intel vPro and DASH-enabled devices before you start working with OOBM. Additionally, you need to configure the SCS server to communicate with the vPro devices. For more information on setting up and configuring of SCS server, Intel vPro devices, and DASH-enabled devices, see *"Setting Up vPro and DASH Devices" on page 20*.

2. **Enable OOBM in RCA environment**
   This is performed using RCA server. Enable OOBM in RCA server to manage Intel vPro and DASH-enabled devices. For more information, see "Administrative Tasks" on page 52.

3. **Configure OOBM (Optional)**
   This is an optional task. Use the configuration parameters to configure OOBM in RCA environment if you want to change the default settings in OOBM. For more information on configuring OOBM, see *"OOBM Configuration" on page 38*.

4. **Perform Administrative Tasks**
   After enabling OOBM, you can perform tasks such as Device Type Selection, vPro System

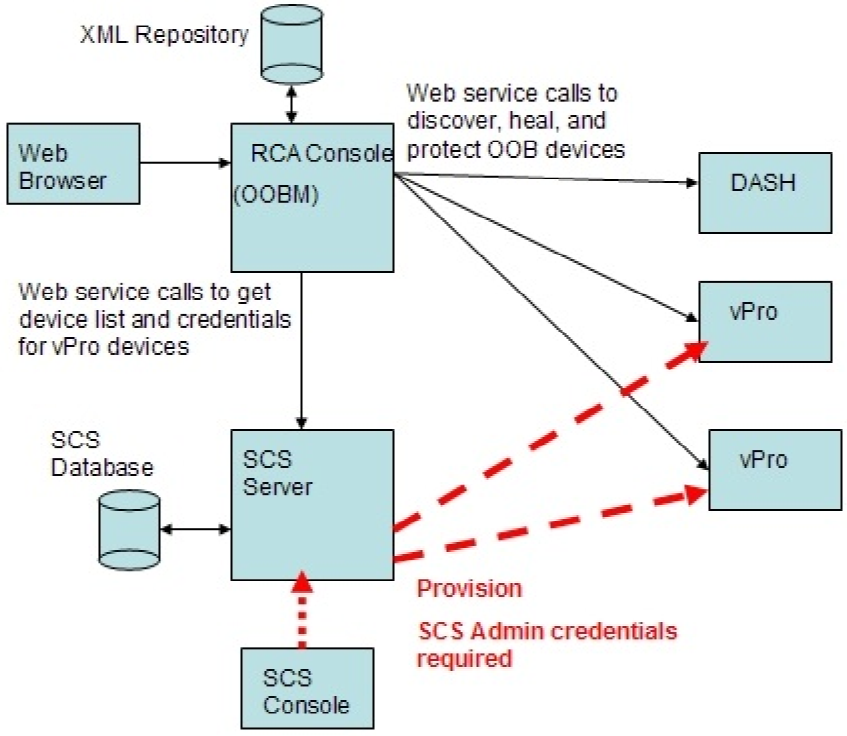
Defense Settings, Provisioning vPro Devices, and other administrative tasks. For more information, see "Administrative Tasks" on page 52.

5. **Manage devices**
   You can start managing devices by performing the following tasks on the Operations tab of the RCA server either as an administrator or operator:
   - **Managing Devices**: The Device Management option enables you to manage multiple and individual OOB devices. These tasks include refreshing data, reloading device information, discover Devices, Power on and off and reboot devices, subscribe/unsubscribe to vPro alerts, manage common utilities on vPro devices, and so on. For more information, see "Device Management" on page 76.
   - **Managing Groups**: The Group Management option enables you to manage groups of vPro devices as defined in the Client Automation software. You can perform OOB operations on Client Automation groups that contain vPro devices. You can manage groups of vPro devices to perform various discover, heal, and protect tasks. These include power management, alert subscription, and deployment of System Defense policies, watchdogs, OOBM agent software lists, and heuristics. For more information, see "Group Management" on page 114.
   - **Viewing Alerts**: For vPro devices, you can view the alerts created by provisioned vPro devices if you have an alert subscription to the device. Monitoring alert notifications provides you a good idea of the health of the devices on your network. For more information, see "Alert Notifications" on page 122.

OOBM Structure in RCA

The following figure illustrates the structure and communication interfaces in OOBM.

Out of Band Management Structure


XML Repository
Web Browser
RCA Console (OOBM)
Web service calls to discover, heal, and protect OOB devices
DASH
vPro
vPro
Web service calls to get device list and credentials for vPro devices
SCS Database
SCS Server
Provision
SCS Admin credentials required
SCS Console

OOBM Management Operations

The following table summarizes the management operations that are possible depending on the type of OOB device you want to manage.

Management Operations on Out of Band Devices

Management Operation	vPro	DASH	Where to Find Information
Provisioning Configuration*	X		"Performing Provisioning Tasks" on page 72
Device Discovery**	X	X	"Device Discovery" on page 77
Managing Multiple Devices	X	X	"Managing Multiple Devices" on page 76
General Asset Discovery	X		"Viewing vPro General Asset Information" on page 91
Hardware Asset Discovery	X	X	"Viewing Hardware Assets" on page 91
Software Asset Discovery***	X	X	"Viewing Software Assets" on page 92

Management Operation	vPro	DASH	Where to Find Information
Power Management****	X	X	"Changing Power State" on page 93
Rebooting****	X	X	"Rebooting the System" on page 97
Rebooting with IDE-R****	X		"Rebooting vPro System with IDE-R" on page 99
Rebooting to BIOS****	X		"Rebooting vPro System to BIOS Settings" on page 99
Rebooting to LAN (PXE)****	X	X	"Rebooting System to Preboot Execution Environment" on page 100
Rebooting or powering to more discrete sleep states****		X	"Booting to DASH-only Supported Power States" on page 101
Text Console Redirection	X	X	"Remote Operations" on page 145
Device Group Management	X		"Group Management" on page 114
Event Management	X		"Viewing vPro Event Log" on page 89, "Viewing vPro Event Filters" on page 90, "Alert Notifications" on page 122
System Defense	X		"Managing System Defense Filters" on page 55, "Managing System Defense Policies" on page 59
Agent Presence	X		"Managing Watchdogs" on page 67
Heuristics Worm Containment	X		"Managing Heuristics Information" on page 63
Front Panel Settings Configuration	X		"Configuring Front Panel Settings on the vPro Device" on page 109
Flash Limit Reset	X		"Resetting Flash Limit on the vPro Device" on page 110
Boot Settings Configuration		X	"Configuring the Boot Settings on the DASH Device" on page 111
Delete Devices	X	X	"Deleting Devices " on page 84

* Provisioning Configuration: There are multiple ways to provision vPro devices. The RCA server represents only one of the ways to do it through delayed remote configuration. DASH devices are assumed to be provisioned already as per machine documentation.

** Device Discovery: vPro devices are discovered by using the SCS device repository. DASH devices are discovered by specifying an IP address or through Active Directory (AD)

*** Software Asset Discovery: The software assets on a vPro device are discovered by using the information located in the third party data store. On DASH devices, they are discovered by using the information located in the network controller’s NVRAM.

**** Power and Reboot Operations: For more information, see "Viewing Power State" on page 85.

Advantages of OOBM

OOBM in RCA server offers several advantages. These are listed below:

- Takes advantage of hardware-based management capabilities in PCs with vPro technology or ones with an implementation of the DASH standard making these PCs accessible even when they are powered off, their operating systems are not working, or their management agents are missing.
- Improves the accuracy and thoroughness of hardware and software inventories from initial deployment to end-of-lease agreements.
- Reduces the need for desk-side visits because PCs can be remotely powered on, restarted, and reimaged.
- Provides System Defense capabilities for vPro devices that permit selective network isolation of Ethernet and IP protocol packet flows based on policies and filters created through the RCA server.
- Provides Agent Presence capabilities that permit the monitoring of OOBM agents running on vPro systems by watchdogs that are created through the RCA server. If a monitored agent stops running, an Agent Presence policy is enabled and/or an event is logged.
- Provides an operating system-independent and tamper-resistant worm-containment system for vPro devices. When a worm is detected, the host is quarantined and a notification is sent to the RCA server.
- Provides a secure, always available communication channel through HTTP authentication and Transport Layer Security (TLS) that runs below the operating system layer of the managed vPro device.

Chapter 2

Setting Up vPro and DASH Devices

Intel vPro devices are enabled by Intel Active Management Technology (AMT). AMT is just one part of vPro technology. The Intel chipset and the Intel Network Interface Card (NIC) are also part of the vPro technology solution. Intel vPro devices can be discovered and managed even when powered off because the Intel AMT firmware stores information about them in non-volatile memory and provides a set of management operations that can be invoked by a remote management console.

Similarly, DASH-enabled devices can take advantage of out of band management. DASH is designed to provide the next generation of standards for secure out of band and remote management of desktop and mobile systems. DASH is one of several Distributed Management Task Force (DMTF) Management Initiatives, providing a comprehensive framework for syntax and semantics necessary to manage computer systems, independent of machine state, operating platform, or vendor.

Both technologies provide remote diagnostics and repair capabilities, which include hardware-based remote-boot and text console-redirection. On vPro devices, remote boot is provided through integrated drive electronics redirect (IDE-R), and text console redirection is available through serial over LAN (SOL) technology.

Intel vPro technology also enables you to automatically provision remote vPro devices. In addition, it provides System Defense and Agent Presence capabilities, which serve to protect vPro devices from malware attacks and the removal of OOBM agents that secure the system. In addition, it provides Network Outbreak Containment (NOC) heuristics, which is a mechanism for measuring, analyzing, and reacting to traffic to detect and impede the proliferation of worms.

All vPro OOBM capabilities can be secured through Transport Layer Security (TLS) and Digest authentication. Currently, for Dash-enabled device, the only supported mechanism is through Digest authentication.

Note: The RCA server does not support Kerberos authentication.

Note: The only conditions for discovery and management of the OOB devices are that they are physically connected to the network and that they are plugged into a power source.

Setting up vPro Device

To make a vPro device operational, the SCS server (also referred to as the Setup and Configuration Server) performs all the necessary steps. The SCS server is the system that runs the Intel Setup and Configuration Service (SCS) and is relevant to vPro devices only.

For the SCS server and the vPro device to communicate with each other, several setup and configuration steps must be performed on both sides as described in the following sections.

> **Note:** Be sure to use the version of the SCS software that is bundled with the RCA Core distribution media located in the `Media\OOBM\win32\AMT Config Server` directory. Also, if you are migrating from an earlier release, ensure that you migrate the SCS software as well to the one included on the distribution media for the current release. Otherwise, you may experience erroneous behavior.

SCS Provisioning of vPro Devices

The SCS server and the vPro device communicate securely. The SCS server creates and sends the vPro device initial parameter values and security-related configuration information. Set up and configuration include setting parameters that are either included in profiles or created automatically.

For more information on vPro security-related configuration information, see the *Introduction to Intel SCS* section in the *Intel Setup and Configuration Service Console User Guide Version 5.4* located in the `Media\oobm\win32\AMT Config Server` directory on the RCA Core distribution media.

For more information on the Setup and configuration parameters, see the *Setup and Configuration Operational Overview* section in the *Intel Setup and Configuration Service Console User Guide Version 5.4*.

RCA and SCS on Different Systems

You may want to install the SCS software and RCA software on separate systems since the supported operating system platforms for SCS and RCA may be different.

Setting Up TLS Mode

If you do not require TLS, skip to "Setting up SCS Server" on page 27.

Security is important for many vPro features, especially for redirection. The usage model of serial over LAN (SOL) and drive electronics redirect (IDE-R) includes remote troubleshooting that enables remote diagnostics, boot, and OS installation. These procedures usually involve authentication steps, which require usernames and passwords to be sent over the LAN as part of the redirection session. If the vPro device supports TLS, the RCA server will establish a TLS session with it before opening SOL or IDE-R sessions, thus ensuring that all relevant network communications are secure.

You must use Mutual Authentication for vPro devices and Server Authentication for SCS server.

> **Note:** If you set up TLS authentication on the RCA server, it manages only those vPro devices that are configured to use TLS. Conversely, if you have not set up TLS authentication on the RCA server, it manages only those vPro devices that are not configured to use TLS.

Perform the following tasks to set up TLS mode:

Task 1: Installing Microsoft Certification Authority

The Microsoft Certification Authority enables you to create the client certificate and to export the client certificate and the trusted root certificate so that they can be used for TLS authentication.

To install the Microsoft CA on Windows Server 2003, follow these steps:

> **Note:** The steps to install Microsoft CA may vary based on the platform.

1. Click the Windows **Start** button and select the **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. From the left panel, click **Add/Remove Windows Components**.
4. Select the **Certificate Services** checkbox. A warning message is displayed indicating that the machine name or the domain membership of the machine cannot be changed while it acts as a certificate server. Click **Yes** to close the message window.
5. Click **Details**.
6. Select both the **Certificate Services CA** checkbox and the **Certificate Services Web Enrollment Support** checkbox to specify the subcomponents of Certificate Services. Click **OK**.
7. On the Windows Components window, click **Next**. The CA Type window opens.
8. Select **Enterprise root CA** as the type of certificate you want to setup. Click **Next**. The CA Identifying Information dialog opens.
9. In the CA Identifying Information dialog, specify the following:
   - **Common Name for this CA**: The Common Name for the Microsoft CA must be the same as the Computer Name on which you are installing the Microsoft CA.
   - **Distinguished name suffix**: An example is `DC=AMT,DC=HP,DC=COM`
10. Complete the remaining steps in the Windows Components Settings Wizard. Click Finish when done.

This installs the Microsoft CA software. The Microsoft CA enables you to create the client certificate as described in the next sections, as well as export trusted root certificates that are used for signing in the authentication process. The export procedure is described in "Task 7: Exporting the Root Certificate" on page 25.

Task 2: Creating Internet Information Services Server Certificate on SCS Server

A server certificate is required to provide secure communication between the SCS server and the SCS console.

For detailed steps, see the *Securing the Connection to IIS Using SSL* section under the *Installing Microsoft's Certification Authority* chapter in the *Intel Setup and Configuration Service Installation Guide Version 5.4* located in the `Media\oobm\win32\AMT Config Server` directory on the RCA Core distribution media.

Task 3: Creating Client Certificate Template

You must create a client certificate for TLS mutual authentication that will be installed on the RCA server.

To create the client certificate template, follow these steps:

1. Click the Windows **Start** button and select **Run**.
2. Enter **MMC** and click **OK**. The Microsoft Management Console opens.

3. From the File menu, select **Add/Remove Snap-in**.
4. Click **Add**. The Add Standalone Snap-in dialog box opens.
5. Select **Certificate Templates** and click **Add** and then click **Close**.
6. Click **OK** in the Add/Remove Snap-in window.
7. Click **Certificates Templates** in the left pane. All existing templates display to the right pane of the console.
8. Right-click the Web Server Template and select **duplicate template**.
9. On the **General** tab, specify the following:
   - **Template display name**: The name you want to appear when the template is displayed. For example, it can be `ClientAuthTmpl`.
   - **Template name**: The name of the template. It can be the same as the display name.
   - Select the **Publish certificate in Active Directory** checkbox.
10. On the **Request Handling** tab, select the **Allows private keys to be exported** checkbox.
11. On the **Extensions** tab, select **Application Policies** and click **Edit**. The Edit Application Policies Extension window opens. The Server Authentication policy is displayed by default.
12. Select **Server Authentication policy** and click **Remove**. Now the Application policies list is empty.
13. Click **Add**. The Add Application Policy window opens.
14. In the Add Application Policy window, select **Client Authentication Policy** and click **OK**. The Add Application Policy window closes and the Edit Application Policies Extension window opens. The Client Authentication Policy is displayed in the list.
15. In the Edit Application Policies Extension window, click **Add**. The Add Application window opens.
16. Click **New**. The New Application Policy window opens.
17. Enter the Name, for example, `AMTRemote`, and Object identifier, `2.16.840.1.113741.1.2.1` for the policy. This policy enables the private key for the server certificate to be exported.
18. Click **OK** three times. After adding the application policies, the Client Authentication policy and the `AMTRemote` policy are displayed in the Description of Application Policies list.
19. Edit Issuance Policies and click **Add**. Select the **All Issuance Policies** option and click **OK** twice. Now the all issuance policies option is displayed in the Description of Issuance Policies list.
20. On the **Security** Tab, select **Domain Admins** and set Read, Write, Enroll and Autoenroll permission. Select **Enterprise Admins** and set Read, Write, Enroll and Autoenroll permission. Select **Authenticated users** and set Read permission.
21. The other tabs (Issuance Requirements, Superseded Templates, and Subject Name) do not require any changes.
22. Click **Apply** and then **OK**. The new Template for Client Authentication is displayed in the right pane of Certificate Template.

Task 4: Issuing Client Certificate Template

Before you install the certificate, you must issue the certificate template that enables the template to become a certificate.

To issue the client certificate template, follow these steps:

1. Click the Windows **Start** button and select **Administrative Tools** > **Certificate Authority**.
2. Expand the installed Microsoft CA. Right-click Certificate Templates and select **New** > **Certificate Templates to Issue**. The Enable Certificate Templates window opens.
3. Select the client authentication template you created in "Task 3: Creating Client Certificate Template" on page 22. In our example, it is the **ClientAuthTmpl** template.
4. Click **OK**. The issued certificate template is displayed in the right pane of the Certificate Templates window.

Task 5: Installing Client Certificate

1. You must install the client certificate on the SCS server as well as on the system where you installed the RCA server .
   - To install client certificate on SCS server or RCA server, use the following URL:
     `http://`*<FQDN_CAServer>*`/certsrv`
     where <*FQDN_CAServer*> is the Fully Qualified Domain Name of the Certification Authority Server.

   You can find the fully qualified domain name (FQDN) of a machine from the Windows desktop on that machine.

   a. Right-click **My Computer**, select **Properties**. The System Properties window opens.

   b. Select the **Computer Name** tab. The FQDN of the machine is displayed in this window.

   Make sure that this URL is added to the browser’s trusted sites list. To add this site, do the following:

   a. In your browser, go to **Tools** > **Internet Options** > **Security** and select **Trusted Sites**.

   b. Click **Sites**. The Trusted sites window opens.

   c. Enter the URL in the **Add this Web site to the zone** field.

   d. Clear the **Require Server Verification (https :) for all sites in this zone** check box.

   e. Click **Add**.

   f. Click **Close**.
2. Click **Request a certificate** > **Advanced certificate request** > **Create and submit a request to this CA**.
3. Select the client certificate template from the **Certificate Template** pull down list. In our example, it is `ClientAuthTmpl`.
4. In the **Identifying Information For Offline Template**, the **Name**: field must be the fully qualified name of the machine where client certificate will be installed.
5. Select the **Mark keys as exportable** check box.
6. Click **Submit**. Select **Yes** in the subsequent window and install the certificate.

Task 6: Exporting the Client Certificate

You *must* export the client certificate for both, RCA server and SCS server.

To export the client certificate, follow these steps:

1. On the server, click the Windows **Start** button and select **Run**.
2. Enter **MMC** and click **OK**. The Microsoft Management Console opens.
3. From the File menu, select **Add/Remove Snap-in**.
4. Click **Add**.
5. Select **Certificates** and click **Add**.
6. Select **My user account** and click **Finish**.
7. Click **Close** and then **OK**.
8. From the left panel of the Microsoft Management Console, expand the Certificates-Current User branch.
9. Expand the Personal branch.
10. Select **Certificates**.
11. In the right panel, right click the client certificate. A popup menu opens. You can find the client certificate on the **Intended Purposes** tab.
12. Select **Open**. The Certificate Information Window opens.
13. Select the **Details** tab.
14. Click **Copy to File**. The Welcome window of the Certificate Export Wizard opens.
15. Click **Next**. The Export Private Key window opens.
16. Select **Yes** > **export the private key** > **Next**. The Export File Format window opens. Click **Next**.
17. Enter and confirm the password that protects the private key. You will need this password when you import the certificate. Click **Next**.
18. Enter the complete path and name for the file to Export. The suffix for the file indicating its file type (`.pfx`) is automatically created. Make note of the location since you will have to access it in subsequent procedures.
19. Click **Next** and then **Finish**.
20. Click **OK** to close the Certificate Information window.

Task 7: Exporting the Root Certificate

The root certificate is required on both the vPro device and the RCA server to verify the digital signature on the server and client certificates.

- On the vPro device, the SCS server provisions the vPro device with the root certificate when it configures the profile for the device. The root certificate is used on the vPro device to authenticate the identity of the RCA server client when the RCA server sends the vPro device its client certificate.
- On the RCA server, the root certificate is used to authenticate the identity of the vPro device when the device sends its certificate to the RCA server. The root certificate is used for signing with vPro device to authenticate hardware and software queries and remote control capabilities.

To export the root certificate to the Microsoft CA server, follow these steps:

1. Click the Windows **Start** button and select **Administrative Tools** > **Certificate Authority**. The Certification Authority Management Console opens.
2. In the left window, right-click the installed Microsoft CA. From the shorcut menu, click **Properties**. The CA Properties window opens.
3. Select the **General** tab.
4. Select the certificate and click **View Certificate**.
5. Select the **Details** tab.
6. Click **Copy to file**. The Certificate Export Wizard opens.
7. Click **Next**.
8. Select the Export File Format as **DER encoded binary X.509 (.CER)** (default selection).
9. Click **Next**.
10. Enter the complete path and name for the file to Export. The suffix for the file indicating its file type (`.cer`) is automatically created. Make note of the location since you will have to access it in subsequent procedures.
11. Click **Next** and review the settings. To proceed, click **Finish**. A message displays indicating that the export was successful.
12. Click **OK**. You are returned to the **Details** tab on the Certificate window.
13. Click **OK** to close the Certificate window.
14. Click **OK** to return to the Certification Authority Management Console. Close the console.
15. Copy the certificate file to a location on the SCS server and RCA server.

Task 8: Converting and Importing Certificates

The root certificate on the RCA server is converted to PEM format so that it can be used to secure IDE-R/SOL operations when TLS mutual authentication is turned on. This conversion is described in "Converting Certificates to PEM Format" on page 51.

The client certificate is installed on the RCA server where it is converted to PEM format so that it can be used to secure IDE-R/SOL operations when TLS mutual authentication is turned on. The conversion is described in "Converting Certificates to PEM Format" on page 51.

On the RCA server, the root certificate is added to the Java key store so that it can be used to authenticate the identity of the vPro device server when the device sends the RCA server its server certificate. This conversion is described in "To Import the Root Certificate into the Java Key Store" on page 50.

Task 9: Configuring Security Parameters and Restarting Tomcat Service

You must specify the password for the PEM and PFX client certificate and set the configuration parameters for TLS authentication as described in "Configuring Security Parameters " on page 40.

Finally, restart the **HPCA Tomcat Server** service.

Setting up SCS Server

The Setup and Configuration Service must be configured so that all communications with the vPro device are secure. This software is installed on the SCS server.

Install Setup and Configuration Service

To install the components of the Setup and Configuration Service, see the *Installation* chapter in the *Intel Setup and Configuration Service Installation Guide Version 5.4*.

Logging in to the SCS Console

To log in to the SCS console:

1. On the SCS server, click the Windows **Start** button and select **Intel AMT Configuration** > **Intel AMT SCS Console**. The log in window opens.
2. In the Service Name field, enter the URL path, including the virtual directory, for the SCS Web Services. The format is `<http|https>://`*<FQDN of Provision Server>*`/`*<SCS Web Services Virtual_Directory>.*
   The SCS Console opens.

Configuring SCS Service Settings

You must select **None** for Active Directory Integration, in the SCS Service Settings windows.

For more information on configuring SCS Service settings, see the *Viewing and Configuring SCS Services* chapter in the *Intel Setup and Configuration Service Console User Guide Version 5.4*.

Creating and Configuring the Profile

This profile is associated with a vPro device as described in "Task 3: Adding the new vPro system" on page 29. The profile provides initial values to the vPro device during the provisioning process.

To configure the profile:

In the Optional Settings window, enable the following options:

- **ACL**
- **Use TLS secure communication for operations on the platform** (Required only if you plan to use TLS communication.)
- **Allow connection to WiFi network** (Required only if you want to manage using wireless NIC.)

In the ACL Details window, specify the following:

- User Type: Select **Digest User**.
- User/Group name: Enter the user name for this type of account.
- Password: Enter the password for the account and enable **Mask**.
- Access Type: Select **Both** from the list.

- Realms: Select the required realms in the list. Realms determine the type of operations the user account can perform when managing a vPro device with the RCA Console. It is recommended that you select all realms except the Security Audit Log Realm for the first account that you create.

In the TLS window, specify the following (Required only if you plan to use TLS communication):

- Under Basic TLS Configuration: For TLS Server Certification Authority, select a **Certificate Authority** from the list. For Server Certificate Template, select **WebServer** from the list.
- Under Advanced TLS Configuration: Select **Use mutual authentication** check box. Select the desired TLS trusted root certificates in the list.
- Click **Add**. The Add Trusted Root Certificate window opens. In this window, select **From File** radio button and browse to the root certificate exported. You can view the certificate. Click **OK** to complete the task.

If you plan to configure the WPA-TKIP profile through the Wireless Access Point of your router, you must make the following selections in the WiFi Profile window:

- Profile Name: Enter a unique name for the profile that is different from the general profile name, for example, PSGWirelessProfile.
- SSID: Enter the SSID value that you used when you set up the WPA-TKIP profile in the router Wireless Access Point. See the wireless router documentation.
- Key Management Protocol: Select **WiFi Protected Access (WPA)** from the list.
- Encryption Algorithm: Select **Temporal Key Integrity Protocol (TKIP)** from the list.
- Passphrase: Select the **Passphrase** radio button. Enter the pass phrase value that you used when you set up the WPA-TKIP profile in the router Wireless Access Point. See the wireless router documentation.

> **Note:** If you are configuring a profile for a vPro device with a wireless interface, you must first configure the WPA-TKIP profile in the Wireless Access Point of your wireless router. You need to see the documentation that comes with your wireless router.

For more information on Creating and Configuring the Profile, see the *Creating and Changing Profiles* chapter in the *Intel Setup and Configuration Service Console User Guide Version 5.4*.

Provisioning vPro Devices

Intel vPro devices are by default delivered in an unconfigured state (Factory mode). Before a management application can access the vPro device, the device must be populated with configuration settings that include username, password, network parameters, TLS certificates, and PID-PPS key necessary for secure communication.

You can configure vPro devices by entering the Management Engine BIOS Extension (MEBx) of each device and entering the required information manually. Provisioning devices manually uses the Pre-shared Key (PSK) mode to secure communication between the SCS server and the vPro device. For more information, see "Configuring the vPro Device Using MEBx" on next page.

Alternatively, you can configure the devices by taking advantage of the Intel Remote Configuration process, which provisions devices automatically. Provisioning devices automatically uses the

Public Key Infrastructure (PKI) to secure communication. For more information, see "Configuring the vPro Device Using Remote Configuration" below.

Configuring the vPro Device Using MEBx

Task 1: Configuring security keys

For information on how to configuring security keys, see the *Configuring Pre-Setup and Configuration Security Keys* section under the *Using USB Drives for TLS-PSK Keys* chapter in the *Intel Setup and Configuration Service Console User Guide Version 5.4*.

> **Note:** It is recommended that you select **Fixed Password** in the Create TLS-PSK Keys window and supply the new password.

Task 2: Configuring the vPro Device through the MEBx.

See the vendor documentation for the device for definitive steps. You must set up the following parameters to configure the vPro Device through MEBx:

- Enter the hostname of the vPro device.
- Enable TCP/IP.
- Enable DHCP.
- Select **Provisioning Server**. Enter the IP address of the machine you are using to run Intel SCS.
- Set the listening port to 9971.
- Set the PID and PPS to the values specified when configuring security keys.

Task 3: Adding the new vPro system

For information on Adding the new vPro system, see the *Adding a Platform Definition* section under the *Preparing and Managing Platforms* chapter in the *Intel Setup and Configuration Service Console User Guide Version 5.4*.

Configuring the vPro Device Using Remote Configuration

Remote Configuration is a vPro mechanism that eliminates the need to manually install a PID/PPS pair on each device to enable setup. To take advantage of Remote Configuration, you must do the following:

Task 1: Purchase a security certificate from a trusted Certification Authority (CA).

The CA vendor must match one of the vendors whose root certificate hashes are built into the vPro firmware. Go to the vendor’s website of choice to purchase an SSL certificate. Each site documents the step required to request, enroll, install, and move an SSL certificate. You must install the certificate in the System Certificate Store on the system where the SCS server is installed. For more information, see the *Remote Configuration Flow* section in the Remote *Configuration* appendix in the *Intel Setup and Configuration Service Console User Guide Version 5.4*.

Task 2: Remote Configuration of the vPro Device

There are two ways a vPro device can be provisioned through Remote configuration. They are the following:

- Bare Metal Remote Configuration of the vPro Device as descibed in "Bare Metal Remote Configuration of the vPro Device" below.
- Delayed Remote Configuration Provisioning through OOBM Agent as described in "Delayed Remote Configuration Provisioning of the vPro Device" below.

Bare Metal Remote Configuration of the vPro Device

Typically, immediate setup of the vPro device occurs (if you have performed theRemote Configuration Requirements correctly) when you connect the device to the network. This is referred to as *bare metal configuration*. The device starts sending out “Hello” messages to the SCS server indicating that it has transitioned to setup mode. If the device is successfully provisioned in the Limited Network Access time interval that the network interface opens for that device, no further provisioning tasks need to be performed.

> **Note:** For HP desktops, Limited Network Access time interval is 255 hours. After the time interval has elapsed, the interface will close if the setup and configuration time was not extended by a network command from the SCS.

To perform a bare metal configuration of the vPro device:

1. Connect the vPro device to the network with the SCS server. The vPro device must be connected in the same domain where SCS has been installed.
2. Turn on the vPro device.
   The vPro device automatically sends out “Hello” packets. After the vPro device receives a message from the SCS server, the provisioning process is started where the SCS server loads all of the settings and data needed to enable the vPro device.
3. After the vPro device is configured, install an operating system. You can install an IT-specified operating system from the network onto the vPro device providing a complete “no touch” configuration of the vPro system.

Bare Metal Remote Configuration Failure

Although the bare metal provisioning process starts as soon as the vPro device is connected to the network and AC power, the device may not be successfully provisioned within its limited network access window. Reasons for failure include the following:

- OTP has been enabled on the SCS server
- Excessive network traffic
- Certificate mismatch with root hashes on the vPro device

Delayed Remote Configuration Provisioning of the vPro Device

If bare metal configuration fails, you can provision the device by using Delayed Remote Configuration. To understand what occurs during the transition to Setup mode and the provisioning process in Delayed Remote Configuration, see "Delayed Remote Configuration of the vPro Device" on page 156.

It is recommended that you install the OOBM agent at this point in the workflow. If the vPro device could not be successfully provisioned in the limited time window of bare metal configuration, the OOBM agent invokes delayed configuration as part of its installation process on unprovisioned devices.

Installing the OOBM Agent

There are two ways to install the OOBM agent on vPro devices. One way is to install the OOBM agent manually on each vPro device. Alternatively, you can install the OOBM agent automatically to multiple vPro devices through the RCA Core Console.

Both methods are described in the following sections.

Configuration Client Role

To be able to provision vPro devices through the OOBM agent, you must do the following regardless of the installation method you choose:

- A user with the role of configuration client must be created and added in the SCS console. For example, the user created and added in the SCS console can be named **SCSUser**.
- This user must be created in domain **VLAN1**, for example, **SCSUser@vlan1.hp.com**.

The credentials for the user with the configuration client role need to be provided during OOBM agent installation. The user credentials of the SCS configuration client must be provided correctly, otherwise the OOBM agent will not start the provisioning of the device through delayed setup.

> **Note:** When installing the OOBM agent, you must provide a “dummy” user name and password even if you do not intend to provision devices using delayed configuration. If you do not provide a user name and password, the installation fails with error code 1920.

> **Note:** In some cases, you may see an error message in the event log with the error code 1063 as a result of OOBM agent installation or service restart. This message is harmless and can be ignored.

Manually Installing the OOBM Agent on Individual vPro Device

To manually install the OOBM agent on the vPro device:

1. Copy the `oobmclocalagent.msi` file located in the `\Media\client\default\win32\oobm\LocalAgent` directory on the RCA Core distribution media to the vPro device. Double-click the `oobmclocalagent.msi` file. Alternatively, you can also copy the `setup.cmd` file located in the same directory on the distribution media to the vPro device. Double-click the `setup.cmd` file or type `setup.cmd` on the command line. The `setup.cmd` file calls the `oobmclocalagent.msi` file.
2. Click **Next** and accept the license agreement.

3. Click **Next.** The Remote Configuration Parameters window opens. In this window, specify the following:
   - SCS Configuration Client User Name: Enter the user name of the user with the role of configuration client. The format is *SCS_User_Name@Domain_Name*.
   - SCS Configuration Client Password: Enter the password of the user with the role of configuration client.
   - SCS Profile ID: Enter the profile ID for the vPro device. You can find this information in the Profiles area of the SCS Console.
   - SCS Remote Configuration URL: Enter the URL path including the virtual directory for the Intel Setup and Configuration Service (SCS) remote configuration service. An example is https://<*provisionserver.yourenterprise.com*>/amtscs_rcfg, where *provisionserver.yourenterprise.com* is the fully qualified domain name (FQDN) of the IIS host machine and `amtscs_rcfg` is the SCS remote configuration service virtual directory on the host machine.
4. Click **Next**. The User Information window opens, which permits you to enter the vPro digest user credentials for the user defined in the SCS Profile ID (referenced in the previous step). In this window, specify the following:
   - User Name: Enter the vPro username of the digest user defined in the SCS Profile.
   - Password: Enter the vPro password of the digest user defined in the SCS Profile.
   - Select the **TLS Mode** check box if the vPro device is provisioned in TLS mode.
5. Click **Next** and follow the remaining steps in the install wizard.

The RCA Out of Band Management service starts as soon as the OOBM agent is installed.

Automatic Install on Multiple vPro Devices through Client Automation

As indicated, you can automatically install the OOBM agent on multiple devices through the RCA Core Console.

There are two parts to the automatic install procedure. They are the following:

- You must publish the OOBM agent software to the Radia Client Automation Configuration Server database by using the Radia Client Automation Administrator Publisher.
- You must deploy the OOBM agent to the vPro target devices by using the RCA Console.

Publishing the OOBM agent to the Client Automation Database

1. Click **Start** > **Programs** > **Radia Client Automation Administrator** > **Client Automation Administrator Publisher** to invoke the Radia Client Automation Administrator Publisher. The Logon window opens.
2. Log in to the Radia Client Automation Administrator Publisher using the Radia Client Automation user name and password. By default, the user name is `admin` and the password is `secret`. The Publishing Options dialog window opens.
3. Select **Windows Installer** from the list.

4. Click **OK**. The Select wizard opens.
5. Select the OOBM agent installer file (`oobmclocalagent.msi`) in the left navigation menu as the Windows installer file that you want to publish.
6. Click **Next**. The Edit wizard opens.
7. Click the **Properties** link. The properties for the installer file are displayed to the right. Ensure that all the properties that start with **AMT** are set correctly. These properties include the following:
   - AMTUSERNAME: Enter the vPro username of the administrator (Digest username).
   - AMTPASSWORD: Enter the vPro password of the administrator (Digest password for user).
   - AMTTLSMODE: Enter **1** if the vPro device is provisioned in TLS mode, otherwise, enter **0**.
   - AMTPROVSERVERADD: Enter the URL path including the virtual directory for the Intel Setup and Configuration Service (SCS) remote configuration service.
   - AMTPROFILEID: Enter the profile ID for the vPro device. You can find this information in the Profiles area of the SCS Console.
8. Also on the properties page, ensure that the following properties are set correctly:
   - SCSUSERNAME: Enter the user name of the user with the role of configuration client.
   - SCSUSERPASS**:** Enter the password of the user with the role of configuration client.
9. Click **Next**. The Configure wizard opens.
10. In the Configure window, specify the following (fields not listed are optional):
    - Service ID: Enter a text string to identify the service, for example, `Radia_CA_OOB_LOCAL_AGENT`.
    - Description: Enter a description for the software, for example, `Radia CA OOB Local Agent`.
    - Software catalog: Select **User Application** from the list.
    - Limit package to systems with: If you do not select any of the operating systems, the software is deployed to all vPro devices regardless of the operating system.

    > **Note:** The fields may vary depending on the RCA license.

11. Click **Next**. The Publish wizard opens. Summary and Progress information are displayed.
12. Click **Publish**. The OOBM agent application is published to the Radia Client Automation Configuration Server database.
13. Click **Finish**.
14. Click **Yes** in the pop-up window to exit the Radia Client Automation Administrator Publisher.

Automatically Deploying the OOBM Agent to Multiple vPro Devices

For detailed instructions on the following procedures, see the *Radia Client Automation Enterprise User Guide*.

1. Import the vPro devices into RCA.
2. Deploy the OOBM agent to the target vPro devices.
3. Create a static group and add the target vPro devices to the group.
4. Deploy the OOBM agent to the vPro device group.

Checking Version of the OOBM Agent on the vPro Device

1. Go to the installation directory, `<InstallDir>\OOBM Agent` on the vPro device.
2. Right-click the `OOBMCLocalAgent.exe` file and select **Properties** from the context menu.
3. Select the **Version** tab. The version information is displayed in this window.

OOBM Agent on 64-bit Platforms

If you install the OOBM agent on a 64-bit platform, you must ensure that the Intel-specific drivers for both the 32-bit and the 64-bit platforms are installed on the vPro device. You can find these drivers at www.HP.com/support. For desktops, the drivers can be found under the Software – System Management section. The name of the driver is Intel Local Management Service (LMS) and Serial-over-LAN (SOL) Support. For notebooks, the drivers are typically present under the `SWSetup\AppInst` directory of the Windows install directory. If not, these drivers can also be downloaded from the above mentioned HP support site. After the drivers have been installed, you must reboot the system.

Viewing the vPro Device

After provisioning the vPro device, you can view it in the vPro SCS console.

Note: You may have to wait a short period of time before seeing the device in the console.

To View the vPro Device

1. Open the vPro SCS Console.
2. Expand the Platform Collections branch.
3. Double-click **All Platforms** to view the vPro devices. The vPro devices are displayed with their provisioned status.

Changing the Authentication Mode

Note: This section is relevant only if you have set up TLS authentication. If you have not set up TLS, skip to the "OOBM Configuration" on page 38 chapter.

After provisioning the vPro device, it is possible to change the authentication mode of the device by using the vPro SCS console.

To Configure the vPro Device in TLS Server Authentication Mode

1. Open the vPro SCS Console.
2. Expand the Configuration Service Settings branch and select **Profiles**. It lists profiles which are created for different vPro Devices.
3. Select the required profile for the vPro Device and click **Edit**.
4. Select the **Network** tab and select the following options:
   - Use TLS
   - TLS Server Authentication for both the Local and Remote Interface
5. Click **Apply** and then **OK**. You are returned to the Main SCS Console.
6. Expand the Intel AMT Systems branch and select **Global Operations**. The Global Operations window opens.
7. In the Provisioning pane of this window, click **Re-Provision**. It assigns a Request ID to this re-provision request. Make a note of the ID because you can use it when searching for log information in the Action Status log.
8. Click **OK**.
9. Expand the Logs branch and select **Actions Status**. This log displays the status of all requests. You can check if your re-provision request succeeded or not by using the Request ID assigned in the previous step.

To Configure the vPro Device in TCP Mode

1. Open the vPro SCS Console.
2. Expand the Configuration Service Settings branch and select **Profiles**. It lists profiles which are created for different vPro Devices.
3. Select the required profile for the vPro Device and click **Edit**.
4. Select the **Network** tab and clear the **Use TLS** check box.
5. Click **Apply** and then **OK**. You are returned to the Main SCS Console.
6. Expand the Intel AMT Systems branch and select **Global Operations**. The Global Operations window opens.
7. In the Provisioning pane of this window, click **Re-Provision**. It assigns a Request ID to this re-provision request. Make a note of the ID because you can use it when searching for log information in the Action Status log.
8. Click **OK**.
9. Expand the Logs branch and select **Actions Status**. This log displays the status of all requests. You can check if your re-provision request succeeded or not by using the Request ID assigned in the previous step.

Setting Up DASH Device

DASH Configuration

Provision DASH-enabled devices according to the documentation accompanying the device.

For DASH-enabled devices from Hewlett-Packard, DASH configuration information is documented in the "Broadcom NetXtreme Gigabit Ethernet Plus NIC" whitepaper.

To Access this Documentation

1. Go to www.hp.com.
2. Select **Support and Drivers** > **Product Support and Troubleshooting**.
3. Enter a product that supports this NIC, for example, the dc7900.
4. Select one of the dc7900 models.
5. Select **Manuals (guides, supplements, addendums, etc)**.
6. Scroll to the **White papers** section and select **Broadcom NetXtreme Gigabit Ethernet Plus NIC** whitepaper.

DASH Configuration Utilities

The DASH Configuration Utility (BMCC application) is part of the Broadcom NetXtreme Gigabit Ethernet Plus NIC driver softpaq, which is found in the drivers section for each product that supports this NIC.

To Access this Utility

1. Go to www.hp.com.
2. Select **Support and Drivers** > **Drivers and Software**.
3. Enter a product that supports this NIC, for example, the dc7900.
4. Select one of the dc7900 models.
5. Select an operating system.
6. Scroll to the Driver-Network section and select to download the **Broadcom NetXtreme Gigabit Ethernet Plus NIC Drivers**.

Chapter 3

OOBM Configuration

This chapter explains how to configure Out of Band Management (OOBM) after it has been installed through the RCA Installer. For system requirements and installation information, see the *Radia Client Automation Enterprise User Guide* and the *Radia Client Automation 9.00 Support Matrix* available at the following URL: http://support.persistentsys.com/. For more details, contact your Persistent sales representative.

The configuration tasks explained in this chapter are optional. You can perform these tasks if you want to change the default settings in OOBM.

Information about Configuration Parameters

Reconfiguring the SCS Path

If necessary, you can change the SCS path currently configured through the RCA Console. For more information, see "Setting Configuration Parameters" on page 41.

Reconfiguring Client Automation Web Services

If necessary, you can change the gateway URL for the RCA Console. An example URL is `http://`*CAhost*`:3466/ca`, where *CAhost* is the fully qualified name of the Client Automation server and *`ca`* is the Client Automation web services virtual directory on the Client Automation server. For more information, see "Setting Configuration Parameters" on page 41.

Configuring IDE-R Drives

The OOBM software is installed on the server with default settings for the CD and floppy drives when you use integrated drive electronics redirect (IDE-R). These settings are configurable. For more information, see "Setting Configuration Parameters" on page 41. If the default settings do not agree with the drive specifications on your server, you must change the default drive settings to agree with your server. The CD and floppy drive paths must point to real drives or images.

Note: You must have your CD/DVD configuration set correctly (that is, pointing at a real CD/DVD drive) even when you are using the Floppy Drive boot option. The same is true for the Floppy configuration when you are using the CD/DVD Drive boot option. If there is no Floppy drive connected to the RCA server, you can point to any local bootable ISO image instead of the Floppy drive for IDE-R operations.

Note: If you modify the setting for the CD or floppy drive to use an ISO or IMG file, respectively, (as opposed to a physical CD or floppy), the drive path to the ISO or IMG file must be visible to the server running Tomcat. Consequently, copy all necessary ISO and IMG

files to the local drive of the server running Tomcat.
Also, if your ISO or IMG file is a shared network resource, you must use the Universal Naming Convention (UNC) syntax to access the network file. UNC syntax is the following:

```
\\hostname\sharefolder\file
```

When using UNC syntax, you must use the actual hostname of the machine and not its IP address.

Configuring SOL Ports

The OOBM software is installed on the RCA server with default settings for the serial over LAN (SOL) starting port and for the maximum number of SOL ports you can have open at one time to have multiple simultaneous SOL sessions on vPro devices. You can change these values. For more information, see "Setting Configuration Parameters" on page 41.

Note: On vPro devices, SOL sessions launch Windows HyperTerminal, which is bundled with most Windows operating systems. Check to see if HyperTerminal is already installed on the web browser machine that you will use to access the RCA server. If HyperTerminal is not already installed, see Microsoft documentation for installation instructions.

HyperTerminal is not bundled with the Windows Vista® operating system. In this case, SOL sessions launch Telnet.

Configuring the SNMP Port

This is the SNMP port used to get alert messages from vPro devices. This port is configurable. For more information, see "Setting Configuration Parameters" on page 41.

Configuring the IDE-R and SOL Time-out Values

Remote operations performed on vPro devices with wireless NICs can fail because the time-out value for the IDE-R and SOL sessions are exceeded since wireless communication tends to be slower. IDE-R and SOL time-out and heartbeat interval values are configurable. For more information, see "Setting Configuration Parameters" on page 41.

Configuring Web Service Time-out Value

The OOBM Service communicates with the vPro devices by making web services calls to the device. A time-out value is specified for this communication. You can reconfigure this value if it is not appropriate for the current network conditions. For more information, see "Setting Configuration Parameters" on page 41.

Configuring the Cache Size for DASH Devices

You can configure the number of DASH devices that are cached in memory for a particular user session. For more information, see "Setting Configuration Parameters" on page 41. Modifying this value affects performance. This value is dependent on the availability of memory resources.

Configuring Security Parameters

Note: This step is required only if you have TLS configured.

Note: If TLS AMT Authentication is enabled, the Tomcat server must be run under the domain user account to have the proper permissions for accessing the Java key store.

There are a number of configuration parameters that must be set for TLS authentication. They enable OOBM to locate the trusted root and client certificates, to know the passwords associated with them, and the FQDN of the Certification Authority server.

You must configure the following:

- Full path to the root certificate in PEM format (`root_certificate)`
- Full path to the client certificate in PEM format (`client_certificate_pem)`
- Full path to the client certificate in PFX format (`client_certificate_pfx)`
- Client Certificate CN (`ca_server_commonname`*)*

For information on how to set these parameters, see "Setting Configuration Parameters" on next page.

For information about certificates in PEM format, see "Converting Certificates to PEM Format" on page 51.

In addition, you must specify the password for the PEM and PFX client certificate. When executing the commands in the following procedures, specify the path without double quotes.

To Specify the PEM Client Certificate Password

1. From the <*InstallDir*>`/OOBM/bin` directory, run the `amtpem_chgpwd.bat` file.
2. When prompted, enter the RCA Installation Directory.
3. When prompted, enter the password for PEM Client Certificate.

To Specify the PFX Client Certificate Password

1. From the <*InstallDir*>`/OOBM/bin` directory, run the `amtpfx_chgpwd.bat` file.
2. When prompted, enter the RCA Installation Directory.
3. When prompted, enter the password for PFX Client Certificate.

Configuring Watchdog Settings

When you are creating a watchdog, two of the settings for the watchdog are the OOBM agent’s heartbeat interval (time between heartbeats sent to the watchdog) and the startup time before the OOBM agent starts sending heartbeats to the watchdog. You can change the default values to reflect the needs of your network. For more information, see "Setting Configuration Parameters" below.

Configuration Settings Used for Debugging

There are two configuration parameters that you can set to help debug performance-related problems. They are the `cache_update_thread_size` and the `blocking_timer_time` parameters.

The `cache_update_thread_size` parameter enables you to change the number of threads that are used to update the cache layer. This value need not be changed under normal conditions. However, this value can be changed in association with the `blocking_timer_time` parameter to resolve performance issues.

`The blocking_timer_time` setting enables you to change the time-out value in case there are any socket problems on the RCA server when calling on vPro web services. If there are any problems related to the sockets, it is recommended that you increase the time-out value.

For more information, see "Setting Configuration Parameters" below.

Setting Configuration Parameters

You can set configuration parameters by modifying the two properties files located in the <<*RCA_Install_DIR*>`\oobm\conf\` directory.

> **Note:** If you change the configuration parameters in the properties files located in this directory, you must restart the Tomcat service

The following parameters can be found in or added to the `config.properties` file. You can edit this file to reconfigure the value of any of the parameters listed by entering a new value for an existing **key=value** pair or adding a new **key=value** pair.

> **Note:** When specifying path and fully qualified file names in `config.properties`, you must use "`\\`" or "`/`" as the separator between directories or the name will not be read correctly. For example, `C:\\certs\\cc.pem` or `C:/certs/cc.pem` is correct while `C:\certs\cc.pem` is incorrect.

The following table lists the parameters contained in this file with their default settings and descriptions.

Configuration Parameters in the config.properties File

Parameter (key)	Default Value	Description
scsserver_url	No default value	URL for the SCS server. You can change the SCS path currently configured.
radia_gateway	No	URL of the RCA Console.

Parameter (key)	Default Value	Description
	default value	
default_cddrive_ path	D:	Default IDE-R CD drive setting. The CD path must point to a real drive or image.
default_fddrive_ path	A:	Default IDE-R floppy drive setting. The floppy drive path must point to a real drive or image.
sol_port_start	9999	Starting SOL port
sol_number_of_ port	10	Maximum number of SOL ports
snmp_trapd_port	162	SNMP port
vPro_ webservice_ timeout	15000 ms	Web service time-out value
devices_ cachequeuesize	50	Cache size for DASH devices. Modifying this value affects performance.
root_certificate	No default value	Full path to root certificate in PEM format
client_ certificate_pem format	No default value	Full path to client certificate in PEM
client_ certificate_pfx	No default value	Full path to client certificate in PFX format
ca_server_ commonname	No default value	Client certificate CN
apwatchdog_ heartbeat_ interval	60 seconds	Watchdog OOBM agent heartbeat interval
apwatchdog_ startup_time	300 seconds	Watchdog OOBM agent startup time interval
device_ synchronization_ timeperiod	0	Time period to reload device list from the SCS repository. The synchronization time interval has a default value of zero, indicating that automatic synchronization will not occur. If you want synchronization to occur automatically, set value to a non-zero value. The unit for this value is minutes.

Parameter (key)	Default Value	Description
group_ synchronization_ timeperiod	0	Time period to reload group device list from the CA repository. The synchronization time interval has a default value of zero, indicating that automatic synchronization will not occur. If you want synchronization to occur automatically, set value to a non-zero value. The unit for this value is minutes.
cache_update_ thread_size	25	Cache thread size (for debugging only)
blocking_timer_ time	100	Blocking time-out value (for debugging only)
devices_ cachequeuesize	100	Size of the cache used to store vPro-related Java objects that are used for performing operations such as power management, deployment of system defense features, and so on (for debugging purposes only).
scsserver_url	No default value	URL for the SCS server. You can change the SCS path currently configured.
radia_gateway	No default value	URL of the RCA Console.

Additional configuration parameters can be found in the configuration.properties file also located in the <*RCA_Install_DIR*>`\oobm\conf\` directory. All of these parameters have been assigned default values, but some may require reconfiguration depending on your setup. The following table "Configuration Parameters in the configuration.properties File" lists the parameters contained in this file with their default settings and descriptions.

> **Note:** The data in this file is critical for the proper functioning of Out of Band Management. Make sure you do not modify or delete items that are listed as “Not for end users” in the **Description** column in the following table "Configuration Parameters in the configuration.properties File".

Configuration Parameters in the configuration.properties File

Parameter	Default Value	Description
Active_Directory_ FQDN_or_Hostname_ property	name	Device identification information returned from AD. You can choose the hostname (**name**) or the FQDN (**dNSHostName**). Using the default value (name) is safer since FQDN can fail because of subdomain DNS.
BEV_BOOT_ SOURCE_VALUES	BEV	Boot source names for Boot Entry Vector

Parameter	Default Value	Description
CACHE_SIZE	50	Cache size of OOBM web services system. For example, `CACHE_SIZE=50` specifies that at any point in time, a maximum of 50 devices will be cached by the system. When the cache is full and a new device needs to be added, the least accessed/used device is removed to accommodate the new device.
CACHE_WAIT_DURATION	2000	Cache wait duration in milliseconds. For example, `CACHE_WAIT_DURATION=2000` specifies that the system should not wait for more than 2000 milliseconds for the cache manager to respond. If the cache manager is busy for more than 2000 milliseconds, the system will not use the cache for the current operation.
CDDVD_BOOT_SOURCE_VALUES	CD/DVD,CD-ROM	Boot source names for CD
DASH_PORTS	623	Comma-separated list of DASH ports
DASH_TEXTREDIRECTION_TIME_DELAY	2	Time delay (in seconds) between text redirection connection and the power operation invocation.
DISCOVERY_DELAY	100	Discovery delay time. You can increase this value to overcome the socket connection exhaustion problem.
DISCOVERY_REQUEST	Contains actual content of the DASH discover request	Content of the DASH request for the discovery of DASH devices.
DISCOVERY_SEQUENCE	dash,vpro	Sequence in which an OOBM device is discovered. For example, `DISCOVERY_SEQUENCE ="dash,vpro"` means that the system will first check if the device is a DASH device, and if its not , the system will check if its a vPro device.
ENABLE_BLIND_DISCOVERY	true	Blind discovery for OOBM devices. If enabled, the system will honor operational requests to currently undiscovered OOBM devices by first discovering them automatically and then performing the requested operation. If disabled, the OOBM device should be already discovered in the OOBM system. Otherwise, the system will throw an error.
FLOPPY_BOOT_SOURCE_VALUES	Floppy,Diskette Drive	Boot source names for Floppy

Parameter	Default Value	Description
HDD_BOOT_ SOURCE_VALUES	Hard Drive,Hard-Disk	Boot source names for Hard Drive
HTTP_CONNECT_ TIMEOUT	3000	HTTP connection time out (maximum milli seconds HTTP connection can wait for a response)
HTTP_READ_ TIMEOUT	200	HTTP read time (maximum milli seconds HTTP connections can wait for read response)
IDER_CLIENT_RX_ TIMEOUT	10000	Client receive time-out value in milliseconds. If the time-out value elapses before the client receives any messages from the RCA server, the client will shut down the IDE-R session. When an IDE-R session is open, the RCA server continually sends out messages to make sure that the receive time-out value for the client does not expire (the RCA server heartbeat interval is based on the client receive time-out setting). Minimum value: 10000 Maximum value: 65535 Default value: 10000
IDER_CLIENT_ COMMAND_ TIMEOUT	0	Client command transmit time-out value in milliseconds. This is the amount of time the client waits when sending out an IDE command. If the client does not receive a response from the RCA server to the command within the specified amount of time, the client will close the IDE-R session. A value of 0 means that no command transmit time-out is used. Minimum value: 0 Maximum value: 65535 Default value: 0
IDER_CLIENT_HB_ INTERVAL	5000	Client heartbeat interval in milliseconds. This is the amount of time the client waits before sending a heartbeat message to the RCA server. A value of 0 means that no heartbeat messages are sent. In this case, the RCA server will periodically send IDE-R keep-alive ping messages to the client when there is no activity to determine if it is still alive. Minimum value: 0 Maximum value: 65535

Parameter	Default Value	Description
		Default value: 5000
NETWORK_BOOT_ SOURCE_VALUES	Network,PXE	Boot source names for PXE
NUMBER_OF_ DISCOVER_ WORKER_THREADS	5	Maximum number of threads that can be used for discovery
PCMCIA_BOOT_ SOURCE_VALUES	PCMCIA	Boot source names for PCMCIA(For more info: http://en.wikipedia.org/wiki/PC_Card)
REVERTBACK_ PREVIOUS_BOOT_ ORDER	0	Boot order reset flag. You can choose to disable (**0**) or enable (**1**) to revert back to the previous boot order of the boot configuration when booting the device with a particular boot source. The default is to disable reverting back since this has a performance impact.
RevertBack_Previous_ Boot_Order_Wait_ Timer	10000	Time to wait (in milliseconds) for reverting back the boot order to the previous order after initiating the reboot operation. If the default value is not working, increase the value based on the machine's performance.
SOL_CLIENT_TX_ BUFFERING_ TIMEOUT	100	Client transmit buffering time-out value in milliseconds. This is the amount of time the client waits for its transmit buffer to become full before sending its buffered transmit bytes. A value of 0 means that the client will transmit its data only when its buffer becomes full. Minimum value: 0 Maximum value: 65535 Default value: 100
SOL_CLIENT_TX_ OVERFLOW_ TIMEOUT	0	Client transmit overflow time-out value in milliseconds. This is the amount of time the client waits when its transmit buffer is full before starting to drop transmit bytes. A value of 0 means no time-out. Minimum value: 0 Maximum value: 65535 Default value: 0
SOL_CLIENT_HB_ INTERVAL	5000	Client heartbeat interval in milliseconds. This is the amount of time the client waits between sending

Parameter	Default Value	Description
		heartbeat messages to the RCA server indicating that the client is active. A value of 0 means that no heartbeats are sent. In this case, the RCA server will not monitor the receive activity from the client to determine if it is active. Minimum value: 0 Maximum value: 65535 Default value: 5000
SOL_CLIENT_RX_ TIMEOUT	10000	Client receive time-out value in milliseconds. If this amount of time elapses before receiving any messages from the RCA server, the client shuts down the SOL session. When an SOL session is open, the RCA server periodically sends heartbeat messages to make sure that the receive time-out for the client does not expire (the interval between RCA server heartbeat messages is based on the client receive time-out). Minimum value: 10000 Maximum value: 65535 Default value: 10000
SOL_CLIENT_FIFO_ RX_FLUSH_ TIMEOUT	100	Client FIFO receive flush time-out value in milliseconds. This is the amount of time the client waits when its receive FIFO buffer is full before flushing its received data. A value of 0 means that the client never flushes its received data when it is not read by the operating system. Minimum value: 0 Maximum value: 65535 Default value: 100 (The default value internal to the RCA server is 0. Use of a value below 100 is not recommended. A value of 0 causes the client to not flush the received data. As a result, if the buffer overflows, the client will cancel the session.)
SOL_THREADS_ SLEEP_TIME	500	SOL thread sleep time
USB_BOOT_ SOURCE_VALUES	USB	Boot source names for USB

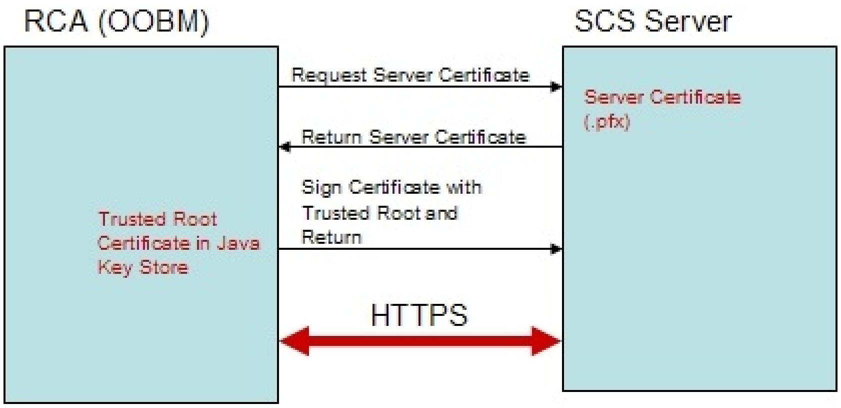
Parameter	Default Value	Description
WSMAN_MAX_ ENUMERATION_ RECORDS	5	Maximum number of elements that can be fetched on a single WSMAN Enumeration or Pull call
WSMAN_TIMEOUT	30000	Time out for WSMAN calls (maximum milli seconds a WSMAN call can wait for a response
DEVICE_DELETED_ IN_SINGLE_QUERY	30	A single SQL query used to perform delete operation on multiple devices.

Note: The values you give to the `*BOOT_SOURCE_VALUES` parameters are used in the RCA server GUI to provide user friendly names for these boot devices. If you do not provide values for these parameters, you may see some non-intuitive text strings displayed representing these boot devices. The string value you provide must be based on the boot source output of the DASH device. For example, if the boot source output is `BRCM:CD/DVD:3`, the user must specify the boot source as `CD/DVD` (*not* CD) to see CD/DVD in the GUI.

Configuring Secure Access between OOBM Service and SCS

You can provide secure communication between the SCS server and the OOBM Service running on the RCA server with this same server certificate. To secure communication between these two components, you must export the trusted root certificate of the Microsoft CA on the SCS server and import it into the Java key store on the RCA server thus enabling the RCA server to sign the server certificate to authenticate the SCS server.

Secure Access between OOBM and SCS


RCA (OOBM)
SCS Server
Request Server Certificate
Server Certificate (.pfx)
Return Server Certificate
Sign Certificate with Trusted Root and Return
Trusted Root Certificate in Java Key Store
HTTPS

Note: If you have already exported the root certificate as part of the TLS mutual authentication setup as described in "Task 7: Exporting the Root Certificate" on page 25, you do not have to perform this task again.

To export the root certificate, follow the steps in "Task 7: Exporting the Root Certificate" on page 25.

To import the root certificate into the Java key store, follow the steps in "Importing the Root Certificate into the Java Key Store" on next page.

Disabling Secure Access between OOBM Service and SCS

After OOBM installation and configuration, the secure hypertext transport protocol (HTTPS) is enabled between the Out of Band Management Service and the SCS server. HTTPS is enabled because of the following:

- You have configured the SCS path to use HTTPS as part of the OOBM device type settings or by specifying it in the `config.properties` file.
- You have exported the trusted root certificate and imported it into the Java key store on the RCA server. For more information, see "Configuring Secure Access between OOBM Service and SCS" on previous page.

If you want to use HTTP instead of the secure transport protocol, you can disable HTTPS through the IIS Manager.

> **Note:** This is not recommended. If you disable HTTPS, user credentials will no longer be encrypted. They will be transmitted in clear text.

To Disable HTTPS

1. Open the IIS Manager on the SCS machine.
2. In the navigation panel on the left-hand side of the window, navigate to **Web Sites** > **Default Web Site** > **AMTSCS**. `AMTSCS` is the virtual directory in the SCS URL.
3. Right-click **AMTSCS** and select **Properties** from its context menu. The AMTSCS Properties window opens.
4. Select the **Directory Security** tab.
5. In the **Secure communications** section at the bottom of the window, click **Edit**. The Secure Communications window opens.
6. Clear the **Require secure channel (SSL)** check box at the top of the window.
7. Click **OK** twice and exit the IIS Manager.
   In the `config.properties` file, change the value for the `scsserver_url` parameter to one that specifies the HTTP protocol in its URL.
8. Restart the Tomcat Service.

Importing the Root Certificate into the Java Key Store

For TLS authentication, it is necessary to import the trusted root certificate into the Java key store of the RCA server. This is used by OOBM to authenticate vPro devices. You exported this root certificate as a `.cer` file in the "Task 7: Exporting the Root Certificate" on page 25.

> **Note:** If you have already imported the root certificate into the Java key store of the RCA server to secure communication between OOBM and the SCS server as described in the "Configuring Secure Access between OOBM Service and SCS" on page 48, you do not have to perform this procedure again.

To Import the Root Certificate into the Java Key Store

1. On the RCA server, backup the existing trusted certificate file. This is the `cacerts` file which is typically located in <*InstallDir*>`\jre\lib\security`.

2. Run the following command from the JRE directory. The default `JRE` directory is `C:\Program Files\Hewlett Packard\HPCA\jre\bin`.
   `keytool -import -noprompt -alias customcacert -keystore ..\lib\security\cacerts -storepass` <*store-password*> `-file` <*ca_file.cer*>
   - The <*store-password*> is the password of the certificate store. By default, this password is **changeit**.
   - The <*ca_file.cer*> is the full path to the root certificate you exported in "Task 7: Exporting the Root Certificate" on page 25 and copied over to the RCA server (if it is different from the SCS server machine).

   This command imports the root certificate into the `cacerts` store.

3. For verification, compare the size of the new `cacerts` file with the backed up version. The new file will be larger by 1 or 2 KB.

   > **Note:** The location of the `cacerts` file and the JRE bin directory can vary if the application has been installed in a non-default location. The default installation directory for the RCA server is `C:\Program Files\Hewlett Packard\HPCA`.

4. Stop the Tomcat service.

5. Run the following commands from the Tomcat bin directory. The default Tomcat bin directory is <*InstallDir*>`\tomcat\bin`.
   a. `tomcat.exe //US//HPCA-Tomcat ++JvmOptions "-Djavax.net.ssl.keyStore=` <*Client Certificate Path in PFX format*>**"**

   b. `tomcat.exe //US//HPCA-Tomcat ++JvmOptions "-Djavax.net.ssl.keyStoreType=pkcs12"`

c. `tomcat.exe //US//HPCA-Tomcat ++JvmOptions "-Djavax.net.ssl.keyStorePassword=`*<PFX client certificate password>*"

> **Note:** The *Client Certificate Path in PFX format* and *PFX client certificate password* are same as specified when "Configuring Security Parameters " on page 40.

6. Start the Tomcat Service.

Converting Certificates to PEM Format

> **Note:** This step is required only if you have TLS configured.

For IDE-R and SOL sessions to be secure when TLS is turned on, the certificates must be available in PEM format on the RCA server. The root certificate was exported as a `.cer` file as described in "Task 7: Exporting the Root Certificate" on page 25. The client certificate was exported as a `.pfx` file as described in the "Task 6: Exporting the Client Certificate" on page 24. These files were copied over to the RCA server if this machine is different from the SCS server machine where the certificates were exported.

Converting the Root Certificate to PEM Format

Run the following command from the `OpenSSL` directory. The default `OpenSSL` directory is *<InstallDir>* `\Media\oobm\win32\sca\CertGenerator\OpenSSLHPCA\Media\oobm\win32\sca\CertGenerator\OpenSSL.`

`Openssl x509 -inform DER -outform PEM -in` *<root.cer>* `-out` *<root.pem>*

where *<root.cer>* is the Microsoft CA server root certificate in the `.cer` format and *<root.pem>* is Microsoft CA server root certificate in the `.pem` format.

Example:

```
Openssl x509 -inform DER -outform PEM -in C:\SCS\RootCA.cer -out
C:\SCS\RootCA.pem
```

Converting the Client Certificate to PEM Format

Run the following command from the `OpenSSL` directory. The default `OpenSSL` directory is *<InstallDir>* `\Media\oobm\win32\sca\CertGenerator\OpenSSLHPCA\Media\oobm\win32\sca\CertGenerator\OpenSSL.`

`Openssl pkcs12 -in` *<client.pfx>* `-out` *<client.pem>*

where *<client.pfx>* is the client certificate exported to the RCA Server in the `.pfx` format and *<client.pem>* is the client certificate in `.pem` format to the RCA server converted from the `.pfx` format.

Example:

```
Openssl pkcs12 -in C:\SCS\ClientAuth.pfx -out C:\SCS\ClientAuth.pem
```

Chapter 4

Administrative Tasks

This chapter describes the configuration tasks you will want to perform in the Administrator role to get ready to manage OOB devices. All of these tasks are available on the **Configuration** tab of the RCA Console. They include the following:

- "Enablement " below
- "Device Type Selection" on next page
- "vPro System Defense Settings " on page 55
- "Performing Provisioning Tasks" on page 72

Note: For optimum viewing results in the RCA Console, set the screen resolution for the display console to 1280x1024.

Enablement

To perform OOBM tasks, the first thing you want to do when you log into the RCA Console is to enable Out of Band Management if it is not enabled already.

When OOBM is disabled, its options (except for **Enablement**) are not visible on the **Configuration** and **Operations** tabs of the RCA Console. Also, you do not have the option to access the Out of Band Device Console from the **Management** tab in the RCA Console.

To enable OOBM:

1. Log into RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management**, click **Enablement**. The Enablement window opens.
3. Check the box next to **Enable** and click **Save**. Out of Band Management becomes enabled. You are automatically logged off.
4. Log into the RCA Console.

When you log back into the RCA Management Console, you will see additional OOBM options as described in the following list:

- Configuration tab: In addition to **Enablement**, you will see **Device Type Selection** under **Out of Band Management** on the **Configuration** tab. Depending on your "Device Type Selection" on next page, another option may appear. For more information, see "vPro System Defense Settings " on page 55.
- Operations tab: **Out of Band Management** will now be visible in the left navigation pane on the **Operations** tab. Your "Device Type Selection" on next page determines the options you will see under Out of Band Management.

- Management tab: You will now be able to access OOB Device Details directly from the **Management** tab of the RCA console. This is in addition to the way you can normally access it from the **Operations** tab as described in "Device Management" on page 76 and "Group Management" on page 114.

Accessing OOB Device Details

You can access the OOB Device Details from the **Management** tab in RCA Console using one of the following procedures:

Using Device Pull-down Menu

1. Under **Directories**, expand **Zone** and click **Devices**. The Directory Object window opens.
2. From the pull-down menu next to the device name, select **Out of Band Device Details**. If the device supports OOBM, the Out of Band Device Details window opens. Otherwise, an error message is displayed.

Using the OOB Device Details Icon

1. Under **Directories**, expand **Zone** and click **Devices**. The Directory Object window opens.
2. Click a device name link. In the toolbar above the Information section, the ▦ Out of Band Devices icon appears.
3. Select a device in the Device table, and click ▦. If the device supports OOBM, the Out of Band Device Details window opens. Otherwise, an error message is displayed.

Using the View/Edit Properties Icon

1. Under **Directories**, expand **Zone** and click **Devices**. The Directory Object window opens.
2. Click a device name link. In the toolbar above the Information section, the ☰ View/Edit Properties icon appears.
3. Click ☰. In the toolbar of the Directory Object window that opens for the specific device, the ▦ Out of Band Devices icon appears.
4. Click ▦. If the device supports OOBM, the Out of Band Device Details window opens. Otherwise, an error message is displayed.

Using Groups

1. Under **Directories**, expand **Zone** and click **Groups**. The Directory Object window opens.
2. Select any group containing devices. The Directory Object window opens displaying the devices in the selected group.

You can use any of the preceding device procedures to access the Out of Band Device Details window.

Device Type Selection

The next configuration task to perform is to select the type of OOB device you want to manage.

To select the device type, complete the following steps:

1. Log into RadiaCA Console and select the **Configuration** tab.
2. Under **Out of Band Management**, click **Device Type Selection**. The Device Type Selection window opens.
   It is possible to make one of three choices for device type:
   - DASH Devices
     To manage DASH devices, select **Manage Dash Devices** check box. You can specify the common credentials for the DASH devices if the DASH administrator configured all of the devices to have the same credentials.
     - Select **Yes** for **Use Common Credentials for All DASH Devices**. The DASH Device Credentials fields appear.
     - Enter the **User Name** and **Password** for all DASH devices.
   - vPro Devices
     To manage vPro device, select **Manage vPro Devices** check box. The SCS Properties fields appear. You must enter SCS login credentials and the URL for the SCS Service.
     - Enter the **SCS Service URL**. (For example, http(s)://provisionserver.yourenterprise.com/amtscs)
     - Enter the SCS **User Name** and **Password** for the SCS administrator.
   - Both Devices
     To manage both DASH and vPro devices, select **Manage Dash Devices** check box for DASH devices and select **Manage vPro Devices** check box.
     - If you select both types of devices, you can enter the common credentials for the DASH devices and you must enter the SCS login credentials and the URL for the SCS Service to access vPro devices
3. Click **Save**. The credentials are saved.
   The next time you go to the Device Type Selection window, you will have the opportunity to re-enter the common credentials or the SCS credentials if you have made a mistake entering them or the DASH or SCS administrator has changed them.
4. Log out and log back into the RCA Console to see the Out of Band Management options that are now available on the **Configuration** and **Operations** tab reflecting your device type selection.

Configuration and Operations Options

After you make your device type selection, you will see options on the **Configuration** and **Operations** tab that reflect this selection. They are summarized in the following table:

Configuration and Operations options

	DASH	vPro
Configuration	No additional options	"vPro System Defense Settings " on next page
Operations	"Device Management" on page 76	"Performing Provisioning Tasks" on page 72, "Device Management" on page 76, "Group Management" on page 114, "Alert Notifications" on page 122

> **Note:** You must log out and log in again to the RCA Console when you make or change your device type selection to see the device-type related options in the navigation panel on the **Configuration** and **Operations** tab.

vPro System Defense Settings

Before getting down to the business of managing vPro devices and device groups, you will want to define your vPro System Defense Settings.

> **Note:** This configuration option appears only if you have selected the vPro device type. System Defense settings do not apply to DASH devices.

On the **Configuration tab**, under **Out of Band Management**, click **vPro System Defense Settings**. The vPro System Defense Settings window opens.

You can create policies, filters, heuristics, and watchdogs for the network in general when managing vPro devices.

The options include:

- "Managing System Defense Filters" below
- "Managing System Defense Policies" on page 59
- "Managing Heuristics Information" on page 63
- "Managing Watchdogs" on page 67

Managing System Defense Filters

You can use the RCA Console to view, create, update, and remove System Defense filters for vPro devices in the System Defense filters repository. System Defense filters monitor the packet flow on the network and can drop or limit the rate of the packets depending if the filter condition is matched. System Defense filters are assigned to System Defense policies that can be enabled to protect the network. The filters are activated when their corresponding policy becomes the active policy.

The icons on the toolbar of the System Defense filter list enable you to manage the filters.

System Defense Filter List Toolbar

Icon	Function
🔄	Refreshes the System Defense filters displayed in the list
➕	Adds System Defense filters to the repository
❌	Removes System Defense filters from the repository

Refreshing the System Defense Filter View

To refresh the System Defense filter view, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Filters**. The Filters window opens. It displays the System Defense filters that have been created through the RCA Console.
3. Click the 🔄 refresh icon on the toolbar.

Adding System Defense Filters

To add System Defense filters, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Filters**. The Filters window opens. It displays the System Defense filters that have been created through the RCA Console.
3. Click the ➕ add icon on the toolbar. The Network Filter Wizard opens.
4. Click **Next** to continue. The Filter Details window opens. In this window, specify the following:
    - **Filter Name**: Enter the name of the filter.
    - **Filter Type**: Select the type of filter you want to create. Each type is explained on the page.
    - **Number of packets per sec**: This field is enabled only if you have selected Rate Limit Filter for the filter type. Enter the packet rate limit for the filter. Specify the packet rate in seconds.
    - **Create Event on Filter Match**: Select **Yes** if you want an event to be created. Event creation can cause the event to be written to the vPro log and/or an event alert to be sent to the RCA Console depending on the entries the Event Manager finds in the Event Filter.
5. Click **Next**. The Parameters window opens. In this window, specify the following:
    - **Packet Type**: Select the packet type from the pull-down menu. It can be TCP Packets (IPv4), UDP Packets (IPv4), IP Packets (IPv4), or Ethernet Frames. The packet type you specify in this field determines the packet header to which the filter will be applied.
    - **Next Protocol**: This field appears only if you have selected IP packets in the Packet Type field since it is applicable to filtering IP packets only. Select the next level packet protocol from the pull-down menu. The next level protocols are TCP, UDP, and ICMP. These protocols are higher level protocols in the Internet layer of the TCP/IP abstract model.
    - **Other Protocol**: This field appears only if you have selected IP packets in the Packet Type field and is enabled only if you have selected –Other- for Next Protocol. You can find additional IP protocols at http://www.iana.org/assignments/protocol-numbers.
    - **TCP Flag**: The flag types appear only if you have selected TCP packets in the Packet Type field since it is applicable to filtering TCP packets only. Check the required flag types. You can check as many types as are required. These flags are optional. If you create a TCP filter without specifying flags, all types of TCP packets will be matched.
    - **Ethernet Frame Type**: This field appears only if you have selected Ethernet Frame packets in the Packet Type field since it is applicable to filtering Ethernet packets only. Select the frame type from the pull-down menu. The frame type can be IPv4 or IPv6.

- **Other Ethernet Frame Type**: This field appears only if you have selected Ethernet Frame packets in the Packet Type field and is enabled only if you have selected –Other- in the Ethernet Frame Type field. Enter an alternative Ethernet frame type. You can find different Ethernet frame types at http://www.iana.org/assignments/ethernet-numbers.
- **Filter Mode or Direction**: Select the filter mode. This specifies if the packet is to be received by (Receive) the vPro device or if it is to be transmitted from (Transmit) the vPro device.
- **Network Address**: This section appears only if you have selected IP, TCP, or UDP packets in the Packet Type field since it is applicable to filtering IP, TCP, and UDP packets only. You can select one of the following options:
- **Filter Packets from/to Device**: This option enables you to filter packets for a single device. Enter an IP address of the remote device. If you selected Receive for the filter mode, the filter will be applied to packets coming from this IP address and going to the vPro device. If you selected Transmit for the filter mode, the filter will be applied to packets going to this IP address and coming from the vPro device.
- **Filter Packets from/to Subnet**: This option enables you to filter packets for a range of subnet addresses. Enter an IP address and subnet mask. The combination of the IP address and subnet mask specifies a range of subnet addresses for filtering. If you selected Receive for the filter mode, the filter will be applied to packets coming from this subnet address range of remote devices and going to the vPro device. If you selected Transmit for the filter mode, the filter will be applied to packets going to this subnet address range of remote devices and coming from the vPro device.
- **Filter Packet from/to Network**: This option enables you to filter packets for the entire network. If you have selected Receive for the filter mode, the filter will be applied to packets coming from all remote devices and going to the vPro device. If you have selected Transmit for the filter mode, the filter will be applied to packets going to all remote devices and coming from the vPro device.
- **Port Type**: This section appears only if you have selected TCP or UDP packets in the Packet Type field since it is applicable to filtering TCP and UDP packets only. You can select one of the following options:
- **Source Port Range**: This option enables you to specify a range of source ports (minimum and maximum port values) to which you want to apply the filter. Packets transmitted from this source port range will be filtered for all destination ports. For more information, see "Adding System Defense Filters" on previous page.
- **Destination Port Range**: This option enables you to specify a range of destination ports (minimum and maximum port values) to which you want to apply the filter. Packets transmitted from all ports will be filtered for this destination port range. For more information, see "Adding System Defense Filters" on previous page.

Port Determination

	Filter Mode	
	Packets Transmitted from vPro Device	Packets Received by vPro Device

		Filter Mode	
IP Port Direction	Source Port Range	Refers to ports on the vPro device. Packets are filtered from this source port range on the vPro device to all ports on the remote destination device or devices.	Refers to the ports on the remote device or devices. Packets are filtered from this source port range on the remote source device or devices to all the ports on the vPro device.
	Destination Port Range	Refers to the ports on the remote device or devices. Packets are filtered from all ports on the vPro device to this port range on the remote destination device or devices.	Refers to ports on the vPro device. Packets are filtered to this destination port range on the vPro device from all the ports on the remote source device or devices.

6. Click **Next**. A confirmation message is displayed.
7. Click **Close**. The new filter is displayed in the System Defense Filters table for the filters repository.

Updating System Defense Filters

To update System Defense filters, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Filters**. The Filters window opens. It displays the System Defense filters that have been created through the RCA Console.
3. Click the filter name link of the filter you want to modify in the Filter Name column of the filters table. The Network Filter Wizard opens.
4. Click **Next** to continue. Edit the fields as necessary in the Filter Details and Parameters pages.
5. Click **Next**. A confirmation message is displayed.
6. Click **Close**. The updates are applied to the filter repository.

Removing System Defense Filters

To remove System Defense filters, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Filters**. The Filters window opens. It displays the System Defense filters that have been created through the RCA Console
3. Check the box next to each filter that you want to delete from the filter repository.
4. Click the ❌ delete icon. The selected filters are removed from the System Defense Filters table for the filter repository.

You can use the System Defense filter interface to:

- View the existing set of filters that can be applied to policies.
- Define filters to isolate the network from virus infections.
- Define filters to divert network traffic to perform various heal scenarios.
- Define filters to proactively monitor packets for System Defense.
- Remove filters that are no longer needed.

Managing System Defense Policies

You can use the RCA Console to view, create, and remove System Defense policies in the System Defense policies repository. These policies can then be deployed to multiple vPro devices on the network. When a policy becomes the active policy, the filters associated with this policy become activated. System Defense policies can selectively isolate the network to protect vPro devices from malware attacks.

The icons on the toolbar of the System Defense policy list enable you to manage the policies.

System Defense Policy List Toolbar

Icon	Function
🔄	Refreshes the System Defense policies displayed in the list
➕	Adds System Defense policies to the repository
	Deploys System Defense policies to vPro devices
	Undeploys System Defense policies from vPro devices
	Assigns System Defense and Agent Presence policies to wired and wireless interfaces
❌	Deletes System Defense policies from the repository

Refreshing the System Defense Policy View

To refresh the System Defense policy view, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Policies**. The Policies window opens. It displays the System Defense policies that have been created through the RCA Console.
3. Click the 🔄 refresh icon on the toolbar.

Adding System Defense Policies

To add System Defense policies, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Policies**. The Policies window opens. It displays the System Defense policies that have been created through the RCA Console.
3. Click the + add icon to create a new policy. The Network Policy Wizard opens.
4. Click **Next** to continue. In this window, specify the following:
   - **Policy Name**: Enter the name of the policy.
   - **Priority**: Enter a priority for the policy. The higher the number, the higher the priority. The priority is used to determine which policy will become the active policy if both a System Defense and Agent Presence policy are enabled.
   - **Enable Anti Spoofing Filter**: Select Yes or No. Anti spoofing uses a transmit filter. If this filter is enabled, it prevents a host from falsifying its identity by sending IP packets with a source IP address that is different from its assigned IP address.
   - **Default Receive (Rx) Filter Type**: Select Pass or Drop. The default Receive filter catches all the receive packets that do not match any of the other policy receive filters. Receive filters can be either of the pass or drop type.
   - **Default Transmit (Tx) Filter Type**: Select Pass or Drop. The default Transmit filter catches all the transmit packets that do not match any of the other policy transmit filters. Transmit filters can be either of the pass or drop type.
5. Click **Next**. The Filters page of the wizard opens.
6. Drag the filters you want to associate with the policy from the **Available filter** list to the **Filters to assign to policy** list.
7. Click **Add Policy**. A confirmation message is displayed.
8. Click **Close**. The new policy is displayed in the System Defense Policies table for the policies repository.

Updating System Defense Policies

To update System Defense policies, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Policies**. The Policies window opens. It displays the System Defense policies that have been created through the RCA Console.
3. Click the policy name link of the policy you want to modify in the Policy Name column of the policies table. The Network Policy Wizard opens.
4. Click **Next**. Edit the fields as necessary.
5. Click **Next** to see the filters currently associated with the policy.
6. Drag and drop filters from one list to another depending on how you want to change the filters associated with the selected policy.

7. Click **Update Policy**. A confirmation message is displayed.
8. Click **Close**. The updates are applied to the policy repository.

> **Note:** If the policy is already deployed to the vPro device, it will not be updated on the device, only in the repository.

Deploying System Defense Policies

To deploy System Defense policies, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Policies**. The Policies window opens. It displays the System Defense policies that have been created through the RCA Console.
3. Check the box next to each policy that you want to deploy.
4. Click the deploy icon on the toolbar. The Policy Deployment Wizard opens.
5. Click **Next** to continue. The Select Devices window opens.
6. Check the box next to each device to which you want to deploy the policies.
7. Click **Next**. The Set Policies window opens. You can use this window to select the default System Defense and/or the Agent Presence policy to be assigned to the wired and wireless NICs for the group of selected devices. You can select the same policy from the pull-down menu next to each field for both System Defense and Agent Presence. If you have specified a policy for a NIC (wired or wireless) that does not exist on a device, an exception will be displayed in the Result window, but this will not affect the deployment process.
8. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
9. Click **Next** to continue with the deployment process. The Result window opens showing the results of the deployment process.
10. Click **Close** to exit the wizard.

Undeploying System Defense Policies

To undeploy System Defense policies, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Policies**. The Policies window opens. It displays the System Defense policies that have been created through the RCA Console.
3. Check the box next to each policy that you want to undeploy.
4. Click the undeploy icon on the toolbar. The Policy Undeployment Wizard opens.
5. Click **Next**. The Select Devices window opens.
6. Check the box next to each device from which you want to undeploy the policies.

7. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
8. Click **Next** to continue with the undeployment process. The Result window opens showing the results of the undeployment process.
9. Click **Close** to exit the wizard.

Setting the Agent Presence Policy

To set the Agent Presence policy, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Policies**. The Policies window opens. It displays the System Defense policies that have been created through the RCA Console.
3. Check the box next to the policy that you want to set as the Agent Presence policy.
4. From the pull-down menu on the policy management icon, select Set Agent Presence Policy (Wired NIC). The Set Agent Presence Policy Wizard opens.
5. Click **Next** to continue. The Select Devices window opens. It displays only the available vPro devices that have wired NICs.
6. Check the box next to each device to which you want to set the selected Agent Presence policy.
7. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
8. Click **Next** to continue with the set policy process. The Result window opens showing the results of the process.
9. Click **Close** to exit the wizard.
10. To set the Agent Presence policy for a wireless NIC, select the Set Agent Presence Policy (Wireless NIC) option from the set policy icon pull-down menu. In this case, the Select Devices window displays only the available vPro devices that have wireless NICs. Repeat the same steps you followed for the wired NIC to set the Agent Presence policy.

Enabling System Defense Policy

To enable System Defense policy, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Policies**. The Policies window opens. It displays the System Defense policies that have been created through the RCA Console.
3. Check the box next to the policy that you want to enable as the System Defense policy.
4. From the pull-down menu on the policy management icon, select Enable System Defense Policy (Wired NIC). The Enable System Defense Policy Wizard opens.
5. Click **Next** to continue. The Select Devices window opens. It displays only the available vPro devices that have wired NICs.

6. Check the box next to each device to which you want to enable the selected System Defense policy.
7. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
8. Click **Next** to continue with the enable policy process. The Result window opens showing the results of the process.
9. Click **Close** to exit the wizard.
10. To enable the System Defense policy for a wireless NIC, select the Enable System Defense Policy (Wireless NIC) option from the set policy icon pull-down menu. In this case, the Select Devices window displays only the available vPro devices that have wireless NICs. Repeat the same steps you followed for the wired NIC to enable the System Defense policy.

Removing System Defense Policies

To remove System Defense policies, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Policies**. The Policies window opens. It displays the System Defense policies that have been created through the RCA Console.
3. Check the box next to each policy that you want to delete.
4. Click the ✖ delete icon on the toolbar. You are warned that this action deletes the selected policies from the repository and also undeploys them from all provisioned vPro devices.
5. Click **OK** to continue. The policies are removed from the repository as reflected in the System Defense Policies table and are also undeployed from the provisioned vPro devices.

You can use the System Defense policy interface to:

- Define new System Defense policies as needed.
- Add or remove filters to a policy to further fine-tune the policy to meet the defense needs of the network.
- Enable a policy to become the active policy based on event alerts and/or logging.
- Enable the anti spoofing filter to prevent a host from falsifying its identity by sending IP packets with a source IP address different from its assigned IP address.
- Remove policies that are no longer needed.
- Deploy (and undeploy) policies to multiple vPro devices.

Managing Heuristics Information

You can use the RCA Console to view, create, update, remove, and add actions to heuristic information. These heuristics can then be deployed to multiple vPro devices. These heuristics serve to protect the devices on the network by detecting conditions that indicate a worm infestation and then containing that device so that other devices are not contaminated.

The icons on the toolbar of the heuristics list enable you to manage the heuristics specifications.

Heuristics List Toolbar

Icon	Function
🔄	Refreshes the heuristics displayed in the list
➕	Adds a heuristics information to the repository
🛡	Deploys heuristics information to selected vPro devices
🛡	Undeploys heuristics information from selected vPro devices
❌	Removes heuristics information from the repository

Refreshing the Heuristics View

To refresh the heuristics view, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Heuristics**. The Heuristics window opens. It displays the heuristics that have been created through the RCA Console.
3. Click the 🔄 refresh icon on the toolbar.

Adding Heuristics

To add heuristics, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Heuristics**. The Heuristics window opens. It displays the heuristics that have been created through the RCA Console.
3. Click the ➕ add icon to create new heuristics information. The Heuristics Wizard opens.
4. Click **Next** to continue. The Heuristics Details window opens. In this window, specify the following:
   - **Settings Type:** Select Default if you want to use the default values provided for the Fast Packet Count, Fast Time Count, Slow Packet Count, and Slow Time Count parameters. These are the Intel recommended values. Select Custom if you want to modify these values. Be aware that if you change these values, you may introduce severe network issues.
   - **Parameters**
     - **Name**: Enter a unique name for the heuristics specification.
     - **Fast Packet Count**: If you did not select the Default Settings Type, enter a threshold value for a fast worm invasion. The threshold (packet count) represents a limit value, which when exceeded by the counter, indicates an anomalous event. The configurable threshold range is from 8 to 64. The default value of 8 is recommended.

- ○ **Fast Time Count**: If you did not select the Default Settings Type, enter a time window size value for a fast worm invasion. The window size (time count) indicates the period at which the heuristic resets its counters. The configurable window size range is from 10 milliseconds to 1 second (1000 milliseconds). The default value of 10 milliseconds is recommended.
- ○ **Slow Packet Count**: If you did not select the Default Settings Type, enter a threshold value for a slow worm invasion. The threshold (packet count) represents a limit value, which when exceeded by the counter, indicates an anomalous event. The configurable threshold range is from 8 to 64. The default value of 64 is recommended.
- ○ **Slow Time Count**: If you did not select the Default Settings Type, enter a time window size value for a slow worm invasion. The window size (time count) indicates the period at which the heuristic resets its counters. The configurable window size range is from 1 second (1000 milliseconds) to 50 seconds (50000 milliseconds). The default value of 50 seconds is recommended.
- ○ **Encounter Timeout**: Enter a value that specifies how long the containment actions should be applied to the vPro device after an anomalous event had been encountered. Values of 20 and greater are recommended. Enter the value of 0 if want to apply the containment actions permanently.
  For more information, see "Window Size and Threshold Values" on page 153 and "Containment Actions and Timeout Values" on page 154.

- ▪ **Actions**
  - ○ **Block TX Traffic**: Select **All TX Traffic** or **Offensive Port Only** from the pull-down list. The latter option (port traffic only) is recommended for most situations
- ▪ **Policy**
  - ○ **Policy Name**: Select a policy name from the pull-down list if you want to enable a System Defense filter when the heuristics conditions are met. If you select a policy, the **view policy information** link appears. If you click the link, you can see the policy details. Click **Close** to close the policy details window.

5. Click **Next**. The status of the operation is displayed.
6. Click **Close** to exit the wizard. The new heuristics information is displayed in the Heuristics table, and it is added to the repository.

Updating Heuristics

To update heuristics, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Heuristics**. The Heuristics window opens. It displays the heuristics that have been created through the RCA Console.
3. Click the heuristics name link of the heuristics specification that you want to modify in the Heuristic Name column of the heuristics table. The Heuristics Wizard opens.
4. Click **Next** to continue. The Heuristics Details window opens. Edit the fields as necessary. You can edit all fields except for the name field.
5. Click **Next**. The status of the operation is displayed.

6. Click **Close** to exit the wizard. The updates are displayed in the Heuristics table and applied to the repository.

> **Note:** If the heuristics information is already deployed to the vPro device, it will not be updated on the device, only in the repository.

Deploying Heuristics

To deploy heuristics, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Heuristics**. The Heuristics window opens. It displays the heuristics that have been created through the RCA Console.
3. Check the box next to each heuristic that you want to deploy.
4. Click the deploy heuristics icon on the toolbar. The Heuristics Wizard opens.
5. Click **Next** to continue. The Select Devices window opens.
6. Check the box next to each device to which you want to deploy the heuristics information.
7. Click **Next**. The Heuristics Setting window opens.
8. Select the heuristics that you want to apply to the wired and wireless network interfaces on the selected devices. You can set the same heuristics information for both interfaces. If you have specified heuristics information for a NIC (wired or wireless) that does not exist on a device, an exception will be displayed in the Result window, but this will not affect the deployment process.
9. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
10. Click **Next** to continue with the deployment process. The Result window opens displaying the results of the operation.
11. Click **Close** to exit the wizard.

Undeploying Heuristics

To undeploy heuristics, complete the following steps:

1. Log in to the RCA Console and select the Configuration tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Heuristics**. The Heuristics window opens. It displays the heuristics that have been created through the RCA Console.
3. Check the box next to each heuristics that you want to undeploy.
4. Click the undeploy heuristics icon on the toolbar. The Heuristics Undeployment Wizard opens.
5. Click **Next**. The Select Devices window opens.
6. Check the box next to each device from which you want to undeploy the heuristics.

7. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
8. Click **Next** to continue with the undeployment process. The Result window opens showing the results of the undeployment process.
9. Click **Close** to exit the wizard.

Removing Heuristics

To remove heuristics, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Heuristics**. The Heuristics window opens. It displays the heuristics that have been created through the RCA Console.
3. Check the box next to each heuristic that you want to delete.
4. Click the ✖ delete icon on the toolbar. You are warned that this action deletes the selected heuristics from the repository and also undeploys them from all provisioned vPro devices.
5. Click **OK** to continue. The heuristics are removed from the repository as reflected in the Heuristics table and are also undeployed from the provisioned vPro devices.

You can use the heuristics interface to:

- Configure time window size (time count) and threshold values (packet count) to heuristically determine if a worm has invaded a vPro device.
- Specify actions to take if the heuristics conditions are met to contain the worm.
- Remove heuristic information that is no longer needed.
- Deploy (and undeploy) heuristics to multiple vPro devices.

Managing Watchdogs

You can use the RCA Console to view, create, update, remove, and add actions to watchdogs in the watchdog repository. These watchdogs can then be deployed to multiple vPro devices on the network. Watchdogs monitor the presence of OOBM agents on the vPro device. You can specify the actions the watchdog must take if there is a change in state of the OOBM agent. In addition, you can create a customized system message that is displayed to the console if the Agent Presence policy is activated and a software list of applications that you want the OOBM agent to monitor.

The icons on the toolbar of the watchdog list enable you to manage the watchdogs.

Watchdog List Toolbar

Icon	Function
🔄	Refreshes the watchdogs that are displayed to the list
➕	Adds watchdogs to the repository
	Deploys selected watchdogs to vPro devices

Icon	Function
	Undeploys selected watchdogs from vPro devices
✖	Deletes watchdogs from the repository
	Configures the OOBM agent system message and software list
	Deploys the OOBM agent system message and software list

Refreshing the Agent Presence View

To refresh the agent presence view, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Watchdogs**. The Watchdogs window opens. It displays the watchdogs that have been created through the RCA Console.
3. Click the 🔄 refresh icon on the toolbar.

Adding a Watchdog

To add a watchdog, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Watchdogs**. The Watchdogs window opens. It displays the watchdogs that have been created through the RCA Console.
3. Click the ➕ add icon to create a watchdog. The Watchdog Wizard opens.
4. Click **Next** to continue. In this window, specify the following:
   - **Agent Type**: Select OOBM Agent or third party vendor agent to specify which agent you have installed on the vPro device. The OOBM Agent is selected by default.
   - **Name**: Enter a unique name for the watchdog.
   - **Agent GUID**: Enter the GUID for a third party vendor agent. This field is grayed out if you have selected the OOBM Agent because the GUID for the OOBM Agent is known.
   - **Heart Beat Interval**: Enter the time between heartbeats from the agent to the watchdog. A default value is provided.
   - **Startup Interval**: Enter the time after the system comes up that the agent must send the first heartbeat to the watchdog. A default value is provided.
5. Click **Next**. The Watchdog Actions page of the wizard opens. In this window, specify the following:
   - **Transition States**:
     From: Select the initial state for the agent that will trigger the actions.
     To: Select the final state for the agent that will trigger the actions.

- **Actions**:
  For **Agent Presence Policy**, select Enable or Disable to specify if you want the Agent Presence policy enabled or disabled if the agent transitions from and to the specified states. If the policy is enabled, it will become the active policy if it has a higher priority than an enabled System Defense policy.
  For **Event Creation**, select Enable or Disable to specify if you want an event to be created or not if the specified agent transition occurs. If event creation is enabled, an event will be logged to the vPro log of the device and/or an event alert will be sent to the RCA Console depending on the Event Filter processing and alert subscription.

6. Click **Add Action**. The action is added to the actions table at the bottom of the window. You can add any number of actions to the watchdog as defined by different valid transition states.
7. Click **Save**. A confirmation message displays to the screen.
8. Click **Close** to exit the wizard. The new watchdog is displayed in the Watchdogs table with the number of actions count properly set. The watchdog and actions are applied to the repository.

Updating Watchdogs

To update watchdogs, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Watchdogs**. The Watchdogs window opens. It displays the watchdogs that have been created through the RCA Console.
3. Click the watchdog name link of the watchdog you want to modify in the Watchdog Name column of the watchdogs table. The Watchdog Wizard opens.
4. Click **Next** to continue. Edit the fields as necessary.
5. Click **Next**. The Watchdog Actions page of the wizard opens. In this window, you can add more actions or remove existing ones.
   - Add actions by following in the "Adding a Watchdog" on previous page.
   - Remove actions by clearing the check box next to each watchdog action that you want to remove at the bottom of the window and clicking the ✖ delete icon.
6. Click **Save**. A confirmation message displays to the screen.
7. Click **Close** to exit the wizard. The updates are displayed in the watchdog table and applied to the watchdog repository.

> **Note:** If the watchdog is already deployed to the vPro device, it will not be updated on the device, only in the repository.

Deploying Watchdogs

To deploy watchdogs, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Watchdogs**. The Watchdogs window opens. It displays the watchdogs that have been created through the RCA Console.
3. Select the check box next to each watchdog that you want to deploy. You can deploy only one OOBM agent watchdog. You can deploy multiple third party agent watchdogs, one per third party agent running on the vPro device.
4. Click the deploy watchdog icon on the toolbar. The Watchdog Deployment Wizard opens.
5. Click **Next** to continue. The Select Devices window opens.
6. Select the box next to each device to which you want to deploy the watchdog.
7. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
8. Click **Next** to continue with the deployment process. The Result window opens displaying the results of the operation.
9. Click **Close** to exit the wizard.

Undeploying Watchdogs

To undeploy watchdogs, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Watchdogs**. The Watchdogs window opens. It displays the watchdogs that have been created through the RCA Console.
3. Select the check box next to each watchdog that you want to undeploy.
4. Click the undeploy watchdog icon on the toolbar. The Watchdog Undeployment Wizard opens.
5. Click **Next**. The Select Devices window opens.
6. Select the check box next to each device from which you want to undeploy the watchdogs.
7. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
8. Click **Next** to continue with the undeployment process. The Result window opens showing the results of the undeployment process.
9. Click **Close** to exit the wizard.

Removing Watchdogs

To remove watchdogs, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Watchdogs**. The Watchdogs window opens. It displays the watchdogs that have been created through the RCA Console.

3. Select the check box next to each watchdog that you want to delete.
4. Click the ✖ delete icon on the toolbar. You are warned that this action deletes the selected watchdogs from the repository and also undeploys them from all provisioned vPro devices.
5. Click **OK** to continue. The watchdogs are removed from the repository as reflected in the Watchdog table and are also undeployed from the provisioned vPro devices

Configuring the System Message and Software List

To configure the system message and software list, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Watchdogs**. The Watchdogs window opens. It displays the watchdogs that have been created through the RCA Console.
3. Click the OOBM agent settings icon. The Software List Dialog opens.
4. In the System Message text box, enter the system message that you want to be displayed to the console on the vPro device on Agent Presence policy activation. A default message is provided, which you can edit.
5. In the Software Name box, enter the name of a security application running on the vPro devices that you want the OOBM agent to monitor. For example, you can enter `symantec.exe`.

   > **Note:** Only applications with an `.exe` extension can be monitored. This product does not support monitoring any other type of executable.

6. Click **Add**. You can repeat this process to create a list of software applications that you want the OOBM agent to monitor.
7. Click **Save**. An information message is displayed to the screen.
8. Click **Close** to exit the dialog. The system message and agent software list are stored in the XML repository.

Deploying the System Message and Software List

To deploy the system message and software list, complete the following steps:

1. Log in to the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management** > **vPro System Defense Settings**, click **Watchdogs**. The Watchdogs window opens. It displays the watchdogs that have been created through the RCA Console.
3. Click the deploy software list and system message icon. The Software Deployment Wizard opens.
4. Click **Next**. The Software Titles window opens.
5. Select the software applications that you want the OOBM agent to monitor.

6. Click **Next**. The Devices window opens.
7. Select the devices to which you want to deploy the list and message.
8. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
9. Click **Next** to continue. The Result window opens displaying the results of the operation.
10. Click **Close** to exit the wizard. The system message and the software list of applications are written to the Third Party Data Store (3PDS) on the targeted vPro devices. You can view this information for a specific vPro device by clicking the hostname of the device in the Device Management window and then under the **Diagnostics** section, go to **Device Assets** > **Software Information** > **Registered Applications** > **HPCA** > **HPCABlock**.

Note: Since the software application list is written to the 3PDS on the vPro device, and the OOBM agent reads the list from the 3PDS, if you re-deploy a modified list, you must stop and restart the OOBM agent on that device.

You can use the watchdog interface to:

- Define a watchdog to monitor an OOBM agent on the vPro device.
- Configure heartbeat rate and startup interval for the OOBM agent when it is being monitored by the watchdog.
- Remove a watchdog that is no longer needed.
- Deploy (and undeploy) watchdogs to multiple vPro devices.
- Customize and deploy the system message that is displayed to the console of the vPro device if the Agent Presence policy is activated and the master list of software applications from which you can select a customized list of applications that you want the OOBM agent to monitor on the target vPro device.

This is the last administrative task you have to perform on the **Configuration** tab to get the RCA Console ready for you to manage OOB devices.

Now, in the role of Operator or Administrator, you can go to the **Operations** tab and start to manage the OOB devices in your network.

Performing Provisioning Tasks

One of the Out of Band Management options on the **Operations** tab in the RCA Console is **vPro Provisioning**.

Note: This option will not be present in the RCA Console unless you have selected to manage vPro devices.

This option enables you to perform several provisioning tasks on vPro devices. These include provisioning, reprovisioning, and partial and full unprovisioning. You may need to reprovision or unprovision certain vPro devices in the course of administering the network. Reasons for doing this include the following:

- Reprovision: Completely reprovisions the vPro device. Use this option if several parameters have changed on the vPro device.
- Partial Unprovision: Only removes the PID and PPS from the vPro device. Use this option when the SCS server information (IP address and host name) has not changed and only the keys need to be modified.
- Full Unprovision: Deletes all provisioning information from the vPro device. Use this option if the SCS server’s IP address and name have changed. It enables you to clear everything and proceed with fresh provisioning.

To perform any of the provisioning tasks you must first do the following:

- Install the OOBM agent on the vPro device if you have not done so already. For more information, see "Installing the OOBM Agent" on page 31.
- If additional security is required as part of your network security policy, go back into the SCS setup and enable one-time password (OTP). For more information, see "Creating and Configuring the Profile" on page 27.

Provisioning the vPro Device

To provision the vPro device, complete the following steps:

1. Log into the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management**, click **vPro Provisioning**. The vPro Provisioning window opens.
3. If no devices are displayed in the device table, click the discover icon on the toolbar. The vPro Discovery window opens.
4. Enter the login credentials for Active Directory (AD) and the fully qualified domain name (FQDN) of the AD server. This is necessary because RCA Console communicates with AD to get a list of devices in that specific domain.
   For example, if the information for the AD host is the following:
   Domain name: oobm.hp.com
   Domain user: Administrator
   Domain password: password
   Domain host name: DomainSystem.oobm.hp.com
   Enter the following information in the fields:
   User Name: `Administrator` (only acceptable format)
   Password: `password`
   FQDN: `DomainSystem.oobm.hp.com` (IP address or hostname are not acceptable)
5. Click **Discover** to initiate the discovery process. Click **Cancel** to stop the discovery process. On discovery completion or cancellation, you are returned to the vPro Provisioning window.
   A list of devices are displayed with their provisioning status (vPro Status), namely already provisioned, unprovisioned, or in the process of being provisioned. Also, the UUID of the vPro device and the status of the OOBM agent on the vPro device are displayed.

   > **Note:** The UUID does not appear for unprovisioned, in provisioning, and some fully-provisioned devices. This is considered normal behavior.

6. Select the devices you want to provision.
7. Click the provision icon on the toolbar. The Remote Configuration Wizard opens.
8. In the Introduction window, click **Next** to continue. The Profile window opens.
9. In the Profile window, select the profile you want for provisioning the vPro devices.
10. Click **Next**. The Summary window opens. Review the information in this window.
11. Click **Next** to confirm. The Complete window opens displaying the results of the operation.
12. Click **Close** to exit the wizard and return to the vPro window. The status of the selected vPro devices will be updated in the device list.

Reprovisioning the vPro Device

To reprovision the vPro device, complete the following steps:

1. Under **Out of Band Management**, click **vPro Provisioning**. The vPro Provisioning window opens.
2. Click the provisioning tasks icon on the toolbar, and select **Reprovision** from its pull-down list.
3. To track the success or failure of the action, click the provisioning tasks icon, and select **Provisioning Status Log** from its pull-down list. The status of the action is displayed in the log.

Partially Unprovisioning the vPro Device

To partially unprovision the vPro device, complete the following steps:

1. Under **Out of Band Management**, click **vPro Provisioning**. The vPro Provisioning window opens.
2. Click the provisioning tasks icon on the toolbar, and select **Partial Unprovision** from its pull-down list.
3. To track the success or failure of the action, click the provisioning tasks icon, and select **Provisioning Status Log** from its pull-down list. The status of the action is displayed in the log.

Fully Unprovisioning the vPro Device

To fully unprovision the vPro device, complete the following steps:

1. Under **Out of Band Management**, click **vPro Provisioning**. The vPro Provisioning window opens.
2. Click the provisioning tasks icon on the toolbar, and select **Full Unprovision** from its pull-down list.
3. To track the success or failure of the action, click the provisioning tasks icon, and select **Provisioning Status Log** from its pull-down list. The status of the action is displayed in the log.

Chapter 5

Device Management

This section provides information on how to manage OOB devices through the RCA Console. You can manage OOB devices regardless of their power state, the health of their operating systems, or the existence of management agents.

One of the Out of Band Management options on the **Operations** tab in the RCA Console is **Device Management**. This option enables:

- "Managing Multiple Devices" below
- "Managing Individual Devices" on page 84

Managing Multiple Devices

You can perform a management task on multiple OOB devices at a time by selecting the relevant devices in the device list displayed in the Device Management window.

When managing multiple devices, you can specify what devices are displayed and how they are sorted in the device list by doing the following:

- Search for specific devices based on search criteria
- Select the number of devices to be displayed at a time to see a subset of devices for ease of viewing
- Sort the devices based on column headings

The icons on the toolbar of the device list enable you to manage multiple OOB devices at once. Some of the icons in this table are relevant to vPro devices only. Review the Function description in the following table to understand which operations are applicable to each device type.

Device List Toolbar

Icon	Function
🔄	Refreshes the OOBM device information displayed in the list from the information stored in the OOBM
🔄	Synchronizes the selected devices or all of the devices displayed in the list with the device information currently stored on each device
🖥	Discovers OOB devices on your network
⏻	Manages powering on and off and rebooting of selected OOB devices
⚠	Manages alert subscriptions to selected vPro devices
🔧	Manages common utilities for vPro devices

Icon	Function
	Deploys System Defense policies to selected vPro devices
	Deploys heuristics worm containment information to selected vPro devices
	Deploys watchdogs to selected vPro devices
	Deploys agent software list and system message to selected vPro devices
✖	Deletes selected devices from the OOBM database

Note: When you log in to the RCA Console for the first time, you may have to click the 🔄 refresh icon multiple times before seeing the list of managed devices displayed in the window.

Note: As indicated in the device list toolbar table, the discovery icon enables you to manually discover OOB devices on your network. For vPro devices, this can be a full or incremental discovery as explained in "Device Discovery" below. In addition to a manual discovery, OOBM can automatically discover devices at regular time intervals. This time interval is configurable in the `config.properties` file (located in <*RCA_Install_DIR*>`\oobm\conf\` directory) by setting the `device_synchronization_timeperiod` parameter to the new value. The synchronization time interval has a default value of zero, indicating that automatic synchronization will not occur. If you want synchronization to occur automatically, set the new value to a non-zero value. The unit for this value is minutes. When OOBM performs automatic discovery, it will do an incremental discovery. For newly discovered devices, OOBM will go out and retrieve device information from each device.

Device Discovery

The discover devices icon on the toolbar enables you to discover OOB devices on your network.

For DASH-enabled devices, you must specify IP address/hostname information or Active Directory information in the RCA Console. For vPro devices, you must indicate if you want full or incremental device discovery. The vPro devices are then read from the list of devices in the SCS repository.

To discover devices, complete the following steps:

1. Login into the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the discover devices icon. The Devices Discovery Wizard opens.
4. Click **Next** to continue, The Discovery Options window opens.
5. The device type you selected on the **Configuration** tab of the RCA Console determines the discovery options displayed on this page. If you have selected both types of devices, you will see all of the following options; otherwise you will see one or the other.
   For DASH devices:
   If you click the **Discover DASH devices** radio button, you will see options where you can

enter IP addresses and/or hostnames or Active Directory (AD) information.

- **Discover DASH devices by Manual Input**: When specifying host information, you can supply a comma separated list of multiple IP addresses and hostnames of those devices you want to discover.

- **Discover DASH devices by Active Directory**: To import devices automatically from AD, you must enter the **LDAP Host** (hostname or IP address of the Active Directory server), **LDAP Port** (386 is the default port), **User ID**, **Password** (Active Directory credentials of user with administrative privileges), and **DN to Query** (Domain Name lists to query in Active Directory).
  For example, if the information for the AD host is the following:
  Domain name: oobm.hp.com
  Domain user: Administrator
  Domain password: password
  Port: 386 (default)
  Domain host name: DomainSystem.oobm.hp.com
  Assume the computer list is in “computers” node in AD.
  Enter the following information in the fields:
  LDAP Host: `DomainSystem.oobm.hp.com`
  LDAP Port: `386`
  User ID: `Administrator@oobm.hp.com`
  Password: `password`
  DN to Query: `cn=computers, dc=oobm, dc=hp, dc=com`

  > **Note:** Choose the Active Directory (AD) mechanism only if you have a large number of DASH devices that you need to manage. The AD discovery mechanism is a time-consuming process taking a long period of time to complete for hundreds of devices. As part of AD discovery, the RCA Console makes calls to each of the devices to identify which ones are DASH devices. If the device is not available, the Management Console waits for a certain time-out period thus increasing the time it takes to discover devices through AD discovery. For greater efficiency, use the manual discovery method if you have a small number of devices to discover.

For vPro devices:
If you click the **Discover vPro devices** radio button, you will see options where you can select a full or incremental discover.

- **Discover all vPro devices**: Specifying this option causes OOBM to discover all of the vPro devices on your network.

- **Discover updated vPro devices**: Specifying this option causes OOBM to discover just those vPro devices that are new or have been modified since the last discovery process. This option greatly improves performance but will not notify you of vPro devices that have been removed from your network since the last discovery process.

6. Click **Next**. The Summary window opens. It displays summary information about the discovery information that you have entered.

7. Click **Next** to continue. The Complete window opens displaying the status of the operation. It will indicate if specific DASH devices could not be discovered. If you have attempted to discover the devices by manually entering IP addresses or hostnames, a specific message will be displayed indicating why the device could not be discovered.

8. Click **Close** to exit the wizard. The newly discovered devices are displayed in the list of devices on the **Devices** tab. If you do not see the newly discovered devices immediately, click the 🔄 icon on the toolbar.

You can use this functionality to easily discover OOB devices on your network so that you can then manage them through the RCA Console.

Multiple Device Selection

You can perform device management operations on multiple devices at one time.

To select multiple devices:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Select the OOB devices that you want to access by selecting the check box for the device or by selecting the select all check box in the upper left. You can search on devices with certain criteria and sort the devices to aid in selection.

Credentials for DASH Device Management

To manage a DASH device, you must enter the username and password that was specified when configuring the device. The credentials are used to secure the communication between the DASH device and the RCA Console for any kind of management operation.

DASH devices can be configured to have common credentials (all devices have the same credentials) or different individual credentials. You must get this information from the administrator who configured the device.

> **Note:** You can decide to use common credentials or individual credentials. You cannot use common credentials for some devices and individual credentials for others. When you select to use common credentials, the individual credentials are erased. If you select **No** for the common credentials option, the common credentials are erased if they existed.

If the DASH devices were configured with common credentials, you can enter the common credentials in the Device Type Selection window as explained in "Device Type Selection" on page 53.

If the DASH devices have not been configured with common credentials, you must enter the individual credentials the first time you attempt to access the device to perform a management operation. After the first time, the credentials will be “remembered,” and you will not need to re-enter them unless you change the credentials for the DASH device.

Specifying individual credentials for DASH devices

1. Log into the RCA Console and select the **Configuration** tab.
2. Under **Out of Band Management**, click **Device Type Selection**. The Device Type Selection window opens.
3. Check **Manage Dash Devices**.

4. Select **No** for **Use Common Credentials for All DASH Devices**.
5. Click **Save**.
6. Select the **Operations** tab.
7. Under **Out of Band Management**, click **Device Management**. The Device Management window opens.
8. Click the hostname link for a DASH device. The Credentials Management window opens.
9. The Credentials Management window opens the first time you access the DASH device or if you have changed the credentials for that device. Otherwise, it is a one-time login step.
10. Enter the **Device Username** and **Device Password** for the DASH device.
11. Click **Submit**. The Device Details window for the DASH device opens.

Note: If at some later date, the DASH devices are reconfigured to use common credentials, you can come back to the Device Type Selection window and select **Yes**. This effectively erases the individual credentials from the RCA Console.

Refreshing Device Information

You can synchronize the device information displayed in the RCA Console with the device information currently stored on the devices in your network.

To refresh device information, complete the following steps:

1. Select the OOB devices you want to manage as described in "Multiple Device Selection" on previous page
2. Click the 🔄 reload device information icon. The device information displayed for the selected devices in the RCA Console will now be synchronized with the information stored on the OOB device.

Note: If there are no System Defense policies in the RCA OOBM console, the summary table columns in the console will show **N/A** for the four columns of information related to System Defense and Agent Presence features.

Note: It is recommended that you do not create any System Defense policies unless you actually intend to use the System Defense functionality. Retrieving System Defense information from the vPro devices greatly impedes the performance of the reload operation.

Power Management

Note: If more than one user is performing a remote power operation on the same target OOB device at the same time, the resulting state of the system cannot be predicted. For example, if one user performs a reboot task at the same time that another user performs a power down task on the same device, the outcome cannot be determined.

To power manage multiple devices, complete the following steps:

1. Select the OOB devices you want to manage as described in the procedure "Multiple Device Selection" on page 79.
2. Select the power state from the ⏻ power icon pull-down menu. You can power up to Hard Disk or reboot the Hard Disk or Network. You have more options when you perform power operations on an individual device. A confirmation message appears.
3. Click **OK** if you want to continue. A progress bar appears monitoring the process. The new power state for the selected devices is displayed in the device list table. A power status link is created in the lower right of the window. You can click this link to see a summary of the results of the power management process.

You can use this functionality to effectively power up and down multiple devices at specific times for cost savings.

Alert Subscription Management

To manage alert subscriptions on multiple devices, complete the following steps:

1. Select the vPro devices you want to manage as described in "Multiple Device Selection" on page 79.
2. From the alert subscription icon pull-down menu, select if you want to subscribe to alerts or cancel an alert subscription. A confirmation message appears.
3. Click **OK** if you want to continue. A progress bar appears monitoring the process. When it disappears, your subscription has been created or cancelled depending on the option you selected. A check mark appears in the Alert Subscription column for the device after you create a subscription. An X mark appears in the Alert Subscription column for the device after you cancel a subscription.

You can use this functionality to subscribe and cancel subscriptions to multiple devices so that pertinent event alerts can be sent to the RCA Console.

Management of Common Utilities

The common utilities icon on the toolbar enables you to perform various housekeeping tasks on vPro devices as described in the following sections.

They include:

- Flash Limit Reset

All deployment activities write to the Third Party Data Store (3PDS) on the provisioned vPro devices. This non-volatile memory has a flash limit protection mechanism to prevent misuse of this area. When you perform an action that causes this limit to be exceeded, the following message is displayed to the RCA Console:

```
Error getting application blocks: Flash write limit exceeded - Click
'Reset Flash Limit' option to reset the flash limit
```

The flash limit reset feature enables you to reset the counter for flash memory so that you can continue to perform activities that write to this non-volatile memory store.

> **Note:** It is recommended that you reset this limit frequently to prevent failure of your deployment activities caused by exceeding the flash limit of the 3PDS on the vPro device.

Resetting the flash limit on multiple vPro devices

1. Select the vPro devices you want to manage as described in "Multiple Device Selection" on page 79.
2. From the common utilities pull-down menu, select the **Reset Flash Limit** option. A confirmation message appears.
3. Click **OK** to continue. The counter in the Third Party Data Store (3PDS) of the selected vPro devices is reset to zero.

You can use this option to reset the 3PDS counter, which serves as a flash wear-out protection mechanism. A flash limit exception can occur if you have made several read/write accesses to the non-volatile memory on the same vPro device. Resetting the counter enables you to continue to perform actions that use this non volatile memory.

Deployment of System Defense Policies

To deploy System Defense policies to multiple devices, complete the following steps:

1. Select the vPro devices you want to manage as described in "Multiple Device Selection" on page 79.
2. Click the System Defense policies deploy icon. The Policy Deployment Wizard opens.
3. Click **Next** to continue. The Select Policies window opens.
4. Select the policies you want to deploy.
5. Click **Next**. The Set Policies window opens. You can use this window to select the default System Defense and/or the Agent Presence policy to be assigned to the wired and wireless NICs for the group of selected devices. You can select the same policy from the pull-down menu next to each field for both System Defense and Agent Presence. If you have specified a policy for a NIC (wired or wireless) that does not exist on a device, an exception will be displayed in the Result window, but this will not affect the deployment process.

   > **Note:** Only one Agent Presence policy can be set for a vPro device regardless of the number of NICs on the device. If a vPro device has multiple NICs and you specify a different Agent Presence policy for each NIC, the most recent setting will apply.

6. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
7. Click **Next** to continue. The Result window opens displaying the results of the operation.
8. Click **Close** to exit the wizard.

You can use this functionality to easily deploy multiple System Defense policies to multiple vPro devices to protect these systems from malware attacks.

Deployment of Heuristics

To deploy heuristics to multiple devices, complete the following steps:

1. Select the vPro devices you want to manage as described in "Multiple Device Selection" on page 79.
2. Click the heuristics deploy icon. The Heuristics Deployment Wizard opens.
3. Click **Next** to continue. The Select Heuristics window opens.
4. Select the heuristics that you want to deploy.
5. Click **Next**. The Set Heuristics window opens.
6. Select the heuristics that you want to apply to the wired and wireless network interfaces on the vPro device. You can set the same heuristics information for both interfaces. If you have specified heuristics information for a NIC (wired or wireless) that does not exist on a device, an exception will be displayed in the Result window, but this will not affect the deployment process.
7. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
8. Click **Next** to continue. The Result window opens displaying the results of the operation.
9. Click **Close** to exit the wizard.

You can use this functionality to easily deploy multiple heuristics to multiple vPro devices for worm containment of infected devices.

Deployment of Watchdogs

To deploy watchdogs to multiple devices, complete the following steps:

1. Select the vPro devices you want to manage as described in "Multiple Device Selection" on page 79.
2. Click the watchdog deploy icon. The Watchdog Deployment Wizard opens.
3. Click **Next** to continue. The Select Watchdogs window opens.
4. Select the watchdogs you want to deploy. You can deploy only one OOBM agent watchdog. You can deploy multiple third party agent watchdogs, one per third party agent running on the vPro device.
5. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
6. Click **Next** to continue. The Result window opens displaying the results of the operation.
7. Click **Close** to exit the wizard.

You can use this functionality to easily deploy multiple watchdogs to multiple vPro devices to monitor the OOBM agents on these systems. Monitoring OOBM agents enhances the security of the network because these agents are in turn monitoring security software running on provisioned devices. If the security software stops running (inadvertently through user intervention or otherwise), the watchdog can alert the system administrator of this event.

Deployment of Agent Software List and System Message

To deploy an agent software list and system message to multiple devices, complete the following steps:

1. Select the vPro devices you want to manage as described in "Multiple Device Selection" on page 79.
2. Click the deploy software list and system message icon. The Deployment Wizard opens.
3. Click **Next**. The Software List window opens.
4. Select the software applications that you want the OOBM agent to monitor.
5. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
6. Click **Next** to continue. The Result window opens displaying the results of the operation.
7. Click **Close** to exit the wizard. The system message and the software list of applications are written to the Third Party Data Store (3PDS) on the targeted vPro devices. You can view this information for a specific vPro device by selecting the device on the **Devices** tab and then under the **Diagnostics** section, go to **Device Assets** > **Software Information** > **Registered Applications** > **HPCA** > **HPCABlock**.

   > **Note:** Since the software application list is written to the 3PDS on the vPro device, and the OOBM agent reads the list from the 3PDS, if you re-deploy a modified list, you must stop and restart the OOBM agent on that device.

You can use this functionality to easily deploy the OOBM agent system message and software list to the 3PDS on multiple vPro devices.

Deleting Devices

To delete devices from the OOBM database, complete the following steps:

1. Select the devices you want to delete. For information on how to select multiple devices, see "Multiple Device Selection" on page 79.
2. Click the ✖ Delete Devices icon. The following confirmation message appears:
   ```
   Do you want to delete the selected devices ?
   ```
3. Click **OK** to continue.

Managing Individual Devices

The device list table displayed in the Device Management window shows the power state of the device, its hostname, and other attributes.

To manage an individual device, click its hostname link under the Device column of the table.

The management window for the selected device opens. This window enables you to do the following:

- "Viewing power state of the OOB device" on page 89.
- "Viewing vPro Event Log" on page 89.
- "Viewing vPro General Asset Information" on page 91.
- "Viewing Hardware Assets" on page 91.
- View a list of applications registered with the Third Party Data Store (vPro) or located in the network controller’s NVRAM (DASH) as described in "Viewing Software Assets" on page 92.
- Perform remote operations such as power up, power down, and reboot as described in "Changing Power State" on page 93.
- Perform KVM redirection in text or graphical mode as described in "KVM Redirection on vPro Devices" on page 102.
- View and delete System Defense filters on vPro devices as described in "Managing System Defense Filters on the vPro Device" on page 104.
- View, delete, and enable System Defense policies and set an Agent Presence policy on vPro devices as described in "Managing System Defense Policies on the vPro Device" on page 105.
- View and delete heuristics information on vPro as described in "Managing Heuristics on the vPro Device" on page 107.
- View and delete watchdogs on vPro devices as described in "Managing Watchdogs on the vPro Device" on page 109.
- "Configuring Front Panel Settings on the vPro Device" on page 109.
- "Resetting Flash Limit on the vPro Device" on page 110.

> **Note:** See the table "OOBM Management Operations" on page 17 to be clear about the management operations that are supported per device type.

Viewing Power State

The **Power State** area of the workspace shows the power state of the OOB device at a glance.

The Advanced Configuration and Power Interface (ACPI) defines several power states. Depending on the state of the support of the motherboard, BIOS, and operating system, some of these states may not be available.

Power state values

The power state can range from S0 (normal working state) through successively deeper sleep states to S5 (soft off state) and the mechanical off state. S0 to mechanical off states map to G0 to G3 states as follows:

- G0
  - S0: Awake. The system is fully powered up and running. No power is saved.
- G1
  - S1: Standby. The CPU is throttled down and some components are powered down. The system state is maintained in RAM. The system wakes up almost instantly, but only a small amount of power is saved.

  - S2: Also Standby. The CPU is powered down along with some components. The system state is maintained in RAM. Less power is used, but the system takes longer to wake up.
  - S3: Suspend to RAM. The CPU and most components are powered down. Only the system state is maintained in RAM. This provides greater power savings, but the wakeup time is increased.
  - S4: Hibernation. The system state (including RAM contents) is saved to non-volatile storage and everything is powered down. This state saves the most power, but the wakeup time is quite long depending on the size of RAM.
- G2
  - S5: Soft off. The operating system is shut down and the system is powered down. PC enters this state, when the user instructs the PC to shutdown. This represents an orderly shutdown.
- G3
  - Mechanical off state. The operating system is shut down and the system is disconnected from the power supply (usually by a switch on the back of the PSU). On reconnection, the system enters G2 without further intervention.

Each successively deeper sleep state has a longer latency to wake up to G0/S0, as well as a higher level of system context lost, with the exception of the context-saving characteristics of S4. S4 is a special state that enables the context to be saved to non-volatile storage before going to sleep, as in the case when the battery level becomes critically low. S5 is a “powered-off” condition, while mechanical off (G3) indicates that the battery and external power are disconnected.

The power operations that you can perform on vPro and DASH devices in the RCA Console are mapped to the ACPI power states in the following table:

> **Note:** Not all power operations are supported on both types of OOB devices. Refer back to this table when reviewing the procedures for the various power operations to be clear of the device type to which it is relevant.

> **Note:** "Not Supported" for DASH devices could mean that the DASH standard does not support the power operation or some hardware vendors do not support it.

Mapping between Power Operations and Power States

The following table lists the mapping between the power operations and power states:

Mapping Power Operations to Power States

vPro Power Operation	DASH Power Operation	Description	ACPI State
Power Up to Hard Drive	Power On Boot Source: Hard-Disk	Awake state	G0/S0
Power Up to Local CD/DVD	Power On Boot Source: CD/DVD	Awake state	G0/S0

vPro Power Operation	DASH Power Operation	Description	ACPI State
Power Up to IDE-R CD/DVD	Not Supported	Awake state	G0/S0
Power Up to IDE-R Floppy	Not Supported	Awake state	G0/S0
Power Up to BIOS Setup	Not Supported	Awake state	G0/S0
Power Up to BIOS Pause	Not Supported	Awake state	G0/S0
Power Up to Primary Boot Device	Not Supported	Awake state	G0/S0
Power Down Device	Power Off (Soft) Boot Source: N/A	Soft off state	G2/S5
Reboot to Hard Drive	Power Cycle (Soft) Boot Source: Hard-Disk	Soft off state followed by Awake state	S0 to S5 with return to G0/S0 (If S0 context is lost, requires master bus reset of system or full boot from POST and BIOS)
Reboot to Local CD/DVD	Power Cycle (Soft) Boot Source: CD/DVD	Soft off state followed by Awake state	S0 to S5 with return to G0/S0 (If S0 context is lost, requires master bus reset of system or full boot from POST and BIOS)
Reboot to Primary Boot Device	Not Supported	Soft off state followed by Awake state	S0 to S5 with return to G0/S0 (If S0 context is lost, requires master bus reset of system or full boot from POST and BIOS)
Reboot to IDE-R CD/DVD	Not Supported	Soft off state followed by Awake state	S0 to S5 with return to G0/S0 (If S0 context is lost, requires master bus reset of system or full boot from POST and BIOS)
Reboot to IDE-R Floppy	Not Supported	Soft off state followed by Awake state	S0 to S5 with return to G0/S0 (If S0 context is lost, requires master bus reset of system or full boot

vPro Power Operation	DASH Power Operation	Description	ACPI State
			from POST and BIOS)
Reboot to BIOS Setup	Not Supported	Soft off state followed by Awake state	S0 to S5 with return to G0/S0 (If S0 context is lost, requires master bus reset of system or full boot from POST and BIOS)
Reboot to BIOS Pause	Not Supported	Soft off state followed by Awake state	S0 to S5 with return to G0/S0 (If S0 context is lost, requires master bus reset of system or full boot from POST and BIOS)
Reboot to LAN (PXE)	Power Cycle (Soft) Boot Source: Network	Soft off state followed by Awake state	S0 to S5 with return to G0/S0 (If S0 context is lost, requires master bus reset of system or full boot from POST and BIOS)
Not Supported	Not Supported	Standby state	S1 or S2
Not Supported	Suspend Boot Source: N/A	Suspend state	S3
Not Supported	Hibernate (Soft) Boot Source: N/A	Hibernation state	S4
Not Supported	Power Off (Soft Graceful) Boot Source: N/A	Soft off state (preceded by request to perform orderly shutdown)	G2/S5
Not Supported	Power Off (Hard Graceful) Boot Source: N/A	Mechanical off state (preceded by request to perform orderly shutdown)	G3
Not Supported	Power Off (Hard) Boot Source: N/A	Mechanical off state	G3
Not Supported	Power Cycle (Soft Graceful) Boot Source: *<boot_source>*	Soft off state (preceded by request to perform orderly shutdown) followed by Awake state	S0 to S5 with return to G0/S0 (If S0 context is lost, requires master bus reset of system or full boot from POST and BIOS)
Not	Power Cycle	Mechanical off state	G0 to G3 with return to G0/S0

vPro Power Operation	DASH Power Operation	Description	ACPI State
Supported	(Hard Graceful) Boot Source: <*boot_source*>	(preceded by request to perform orderly shutdown) followed by Awake state	
Not Supported	Power Cycle (Hard) Boot Source: <*boot_source*>	Mechanical off state followed by Awake state	G0 to G3 with return to G0/S0
Not Supported	Master Bus Reset (Graceful) Boot Source: <*boot_source*>	Off state (hardware reset) (preceded by request to perform orderly shutdown) followed by Awake state	G2/S5 with return to G0/S0
Not Supported	Master Bus Reset Boot Source: <*boot_source*>	Off state (hardware reset) followed by Awake state	G2/S5 with return to G0/S0
Not Supported	Diagnostic Interrupt Boot Source: <*boot_source*>	Off state (hardware reset) followed by Awake state	G2/S5 with return to G0/S0

Viewing power state of the OOB device

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the OOB device you want to manage. A management window opens.
4. Review the information under the **Power State** section on the left-side of the window.

> **Note:** The power state displayed is the last known state. This may not be the same as the current power state. To be sure that you are seeing the current power state, you must use the 🔄 refresh icon next to the power state message.

Viewing vPro Event Log

The **Diagnostics** area of the workspace enables you to view and clear the event log on a remote vPro device. Various occurrences on the managed vPro device cause events to be created and logged to the event log on the vPro device.

To view vPro event log, complete the following steps:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the vPro device you want to manage. A management window opens.
4. Click the **Event Log** link under the **Diagnostics** section on the left-side of the window. The contents of the event log are displayed in the content area of the console. Summarized at the top of the window, you can see the log attributes. It displays the number of event records in the log, the time the last event was recorded, and the state of the log (frozen or unfrozen). When the log is frozen, no event can be written to the log. Below the summary, you can see the event type (what caused the event to be created), the severity of the event, the date and time that the event was logged, and the description of the event. If you click the detail icon in the Detail column, a window opens that displays the property details for the selected event.
5. Click the refresh icon on the toolbar to refresh the event log view.
6. Click the clear icon on the toolbar to clear the event log file.
7. Click the freeze icon on the toolbar to freeze or unfreeze the event log file changing the status of the event log.

You can use the event log interface to:

- Determine if a noteworthy event has occurred that requires immediate action.
- Clear the log at regular intervals to ensure that new events can be logged to it.
- Determine the general status or health of the vPro device.

Viewing vPro Event Filters

The **Diagnostics** area of the workspace enables you to view the default event filters that exist on a remote vPro device. Event filters determine the actions that will be taken if an event is raised on the device.

To view vPro event filters, complete the following steps:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the vPro device you want to manage. A management window opens.
4. Click the **Event Filter** link under the **Diagnostics** section on the left-side of the window. The default event filters exist on the selected vPro device are displayed in the content area of the console.
5. Click the name link of the event filter whose details you want to see. The Event Filter Details page opens displaying the property details for the selected event filter.
6. Click the refresh icon to refresh the event filters.

You can use the information in the event filter to understand what actions will be taken when certain types of events are raised on the selected device.

Viewing vPro General Asset Information

The **Diagnostics** area of the workspace enables you to view general asset information about a remote vPro device regardless of its power state or general health.

To view general asset information, complete the following steps:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the vPro device you want to manage. A management window opens.
4. Click the **Device Assets** link under **Diagnostics** on the left-side of the window.
5. Click **General Information**.
6. Click **vPro Information** to see general asset information about the vPro device. General asset information for that device including its IP address, listening port, provisioning mode, BIOS version, etc. is displayed in the content area of the console.
7. Click **Security Settings** to see asset information related to security. Security-related information for that device including enablement of TLS, encryption, SOL, IDE-R, etc. is displayed in the content area of the console.

You can use this information to:

- Inspect the general assets of a vPro device
- View asset information for a vPro device relevant to security and see if any reconfiguration action needs to be taken

Viewing Hardware Assets

The **Diagnostics** area of the workspace enables you to view the hardware assets on a remote OOB device. It does not matter what state the operating system is in or if the device is powered on or off. This reduces or eliminates the need for manual inventory audits because you are able to locate devices regardless of their health or power state. This accurate remote visibility of hardware assets provides better planning, more efficient upgrades, faster deployments, and improved management of field replaceable unit (FRU) inventories.

> **Note:** A Centrino Pro notebook computer cannot be managed via the wireless network if it is in OFF, Standby or Hibernate power mode.

To view hardware assets, complete the following steps:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.

3. Click the hostname link for the OOB device you want to manage. A management window opens.
4. Click the **Device Assets** link under **Diagnostics** on the left-side of the window.
5. Click **Hardware Information**.
6. Click a hardware component. Specifications for that component are displayed in the content area of the console.

   > **Note:** In some cases, you may not see the hardware information for a vPro device. If this occurs, wait for some time period and retry the operation.

You can use this information to:

- Determine the exact specifications for any hardware component on the device that may need to be replaced
- Identify compatibility issues
- Inspect its configuration before provisioning a new operating system
- Retrieve ad-hoc inventory information even when the machine is powered off.

Viewing Software Assets

The **Diagnostics** area of the workspace enables you to view the software assets on a remote OOB enabled device.

For vPro devices, this feature enables you to view the list of software applications that are being monitored by the OOBM agent on the vPro device. For more information, see "Managing Watchdogs" on page 67. This list is registered in the third party data storage (3PDS) on that device.

For DASH devices, this feature enables you to view the software inventory information located in the network controller's NVRAM for that device.

To view software applications, complete the following steps:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the OOB device you want to manage. A management window opens.
4. Click **Device Assets** link under **Diagnostics** on the left-side of the window.
5. Click **Software Information**.
6. Click **Registered Applications** for a vPro device or **Installed Software** for a DASH device.
7. Click an application. The links for the application enable you to view the information for that application.

You can use this information to:

- Determine the software applications that are being monitored by the OOBM agent on the vPro device.
- Determine the software applications that are installed on the DASH device.

Changing Power State

You can perform remote power management operations from the RCA Console. The **Diagnostics** area of the workspace of the console enables you to change the power state on a remote OOB device.

> **Note:** See the table "OOBM Management Operations" on page 17 to be clear about the power operations that are supported per device type.

Through the console redirection capabilities, you can view the power management process on the RCA Console without user intervention or leaving the management console.

> **Note:** On vPro devices, SOL sessions launch Windows HyperTerminal. When exiting the HyperTerminal session, you will be prompted to save the settings of your configuration session. It is recommended that you save session settings for two reasons. If you have made customizations to your HyperTerminal session, they will be saved. Also, after you save the configuration, you will not be prompted again. The configuration is saved as an .ht file on the machine you used to launch the web browser to access the RCA Console. If HyperTerminal is not available (on Vista systems) or fails, Telnet is used instead.

SOL provides keyboard and text redirection to the management console *except* when powering up to local drives on the vPro device.

Security for this capability is provided through TLS.

> **Note:** On vPro devices, KVM redirection is also available, which provides console redirection in both graphical and text mode. JRE 1.6.x and the VNC Viewer must be installed on the machine where you run the browser to access the RCA console. KVM functionality is not available on vPro machines with AMT before release 6.0. For more information, see "KVM Redirection on vPro Devices" on page 102.

> **Note:** Before performing the remote operations via BIOS/IDE-R, you must enable the Telnet service on RCA server and vPro device. By default, the `telnet.exe` is stored at `C:\Windows\System32`. Copy the `telnet.exe` to a different location. Set the `TELNET_PATH` system environment variable to the new path of the `telnet.exe`. If you change the value of the `TELNET_PATH` system environment variable, you must log out and log back into the system for the new value to take effect.

> **Note:** On DASH devices, the RCA Console attempts to use the SSH PuTTY client for text console redirection if the client is installed and configured on the DASH device. To configure the device to use the PuTTY client, you must set the `PUTTY_PATH` system environment variable to the full path of the PuTTY executable, for example, `C:\Putty\putty.exe`. If you

change the value of the `PUTTY_PATH` environment variable, you must log out and log back into the system for the new value to take effect. If the PuTTY client is not available, the console will use Telnet instead.

Powering Up the Device

To power up the device, complete the following steps:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the OOB device you want to manage. A management window opens.
4. Click the **Remote Operations** link under the **Diagnostics** section on the left-side of the window. The Remote Operation Wizard window opens.
5. Click **Next** to continue. The Task window opens. You can power up the device from various drives or to the BIOS (vPro only) as shown in the following table.
   In the Task window, you can also indicate the following:
   - For vPro devices, you can specify if you want to use the front panel settings for that device. If you select **No**, the front panel settings for the vPro device will be ignored. For more information, see "Configuring Front Panel Settings on the vPro Device" on page 109.
   - For DASH devices, you have the **Display Client Console** option where you can specify if you want text to be displayed to the console or not.

Note: In the following tables, when a remote operation is supported by a vPro device or both types of OOB devices, the terminology for the vPro remote operation is used. See the table "OOBM Management Operations" on page 17 to see the mapping to the DASH remote operation.

Powering up a Device

Drive/BIOS	Steps
Local Hard Drive	1. From the pull-down menu next to **Remote Operation**, select **Power Up to Hard Drive**. 2. Click **Next**. For DASH devices, the Boot Settings window opens. In this window, you can specify a Boot Source or Boot Configuration to be used when the device boots up. Select **Hard-Disk** as the Boot Source. For more information, see "Configuring the Boot Settings on the DASH Device" on page 111. 3. Click **Next.** The Confirmation Summary window opens. Review the information in this window. 4. Click **Next** to continue. Summary information displays to your management console.

Drive/BIOS	Steps
	5. Click **Close**.
Local CD Drive	1. From the pull-down menu next to **Remote Operation**, select **Power Up to Local CD/DVD**. 2. Click **Next**. For DASH devices, the Boot Settings window opens. In this window, you can specify a Boot Source or Boot Configuration to be used when the device boots up. Select **CD/DVD** as the Boot Source. For more information, see "Configuring the Boot Settings on the DASH Device" on page 111. 3. Click **Next.** The Confirmation Summary window opens. Review the information in this window. 4. Click **Next** to continue. Summary information displays to your management console. 5. Click **Close**.
IDE-R CD Drive (vPro only)	1. From the pull-down menu next to **Remote Operation**, select **Power Up to IDE-R**. 2. From the pull-down menu next to **IDE-R Option**, select **IDE-R CD/DVD**. The Drive Path field is populated with the default setting for the CD/DVD drive. If you do not want to use the default drive in the Drive Path field, you can specify another drive or the path to an ISO file that is on the management console server. If you specify an ISO file in the Drive Path that is a shared network resource, you must use UNC syntax, namely, \\hostname\sharefolder\file.iso 3. Click **Next.** The Confirmation Summary window opens. Review the information in this window. 4. Click **Next** to continue. The Remote Operation Wizard closes and a HyperTerminal window opens displaying the power up process. This window stays open until you close it.
IDE-R Floppy Drive (vPro only)	1. From the pull-down menu next to **Remote Operation**, select **Power Up to IDE-R**. 2. From the pull-down menu next to **IDE-R Option**, select **IDE-R Floppy**. The Drive Path field is populated with the default setting for the floppy drive. If you do not want to use the default drive in the Drive Path field, you can specify another drive or the path to an IMG file that is on the management console server. If you specify an IMG file in the Drive Path that is a shared network resource, you must use UNC syntax, namely, \\hostname\sharefolder\file.img 3. Click **Next.** The Confirmation Summary window opens. Review the information in this window. 4. Click **Next** to continue. The Remote Operation Wizard closes and a HyperTerminal window opens displaying the power up process. This window stays open until you close it.

Drive/BIOS	Steps
BIOS Setup (vPro only)	1. From the pull-down menu next to **Remote Operation**, select **Power Up to BIOS**. The **BIOS Option** is displayed. 2. From the pull-down menu next to **BIOS Option**, select **BIOS Setup**. 3. Click **Next.** The Confirmation Summary window opens. Review the information in this window. 4. Click **Next** to continue. The Remote Operation Wizard closes and a HyperTerminal window opens displaying the power up process. This window stays open until you close it.
BIOS Pause (vPro only)	1. From the pull-down menu next to **Remote Operation**, select **Power Up to BIOS**. The **BIOS Option** is displayed. 2. From the pull-down menu next to **BIOS Option**, select **BIOS Pause**. 3. Click **Next.** The Confirmation Summary window opens. Review the information in this window. 4. Click **Next** to continue. The Remote Operation Wizard closes and a HyperTerminal window opens displaying the power up process. This window stays open until you close it.
Primary Boot Device (vPro only)	1. From the pull-down menu next to **Remote Operation**, select **Power up to Primary Boot Device**. This option enables you to power up to the default boot device configured in the BIOS of the vPro device. The **SOL Option** is displayed. This local boot option enables you to see the operation displayed to the RCA Console if you select to do so. 2. For the **SOL Option**, you can select **Display to console** or **Do not display to console.** 3. Click **Next**. The Confirmation Summary window opens. Review the information in this window. 4. Click **Next**. ▪ If you selected **Display to console**, the Remote Operation Wizard closes and a HyperTerminal window opens displaying the power up process. This window stays open until you close it. ▪ If you selected **Do not display to console**, the Summary information window opens. It displays the result of the operation when it completes. You must click **Close** to return to the Device Details window.

Powering Down the Device

To power down the device, complete the following steps:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.

3. Click the hostname link for the OOB device you want to manage. A management window opens.
4. Click the **Remote Operations** link under the **Diagnostics** section on the left-side of the window. The Remote Operation Wizard window opens.
5. Click **Next** to continue.
6. From the pull-down menu next to **Remote Operation**, select **Power Down Device**.
7. Click **Next.** The Confirmation Summary window opens. Review the information in this window.
8. Click **Next** to continue. Summary information displays to your management console.
9. Click **Close**.

You can use this capability to:

- Confirm that a device is powered on/off in preparation for a management operation
- Remotely turn on a device in preparation for a management operation
- Troubleshoot non-responsive devices
- Remotely reboot non-responsive devices

Rebooting the System

The Diagnostics area of the workspace enables you to reboot a remote OOB device. Through the built-in redirection capabilities, you can view the reboot process without user intervention or leaving the management console. SOL and KVM on vPro devices provide keyboard and video redirection to the management console (except when powering up to local devices on the OOB device).

To reboot the system from a local device, complete the following steps:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the OOB device you want to manage. A management window opens.
4. Click the **Remote Operations** link under the **Diagnostics** section on the left-side of the window. The Remote Operation Wizard window opens.
5. Click **Next** to continue. The Task window opens. You can reboot the device from drives local to the OOB device as shown in the following table:

Rebooting a Device from a Local Drive

Drive	Steps
Local Hard Drive	a. From the pull-down menu next to **Remote Operation**, select **Reboot to Hard Drive**. b. Click **Next**. For DASH devices, the Boot Settings window opens. In this window, you can specify a Boot Source or Boot Configuration to be used when the device boots up. Select **Hard-Disk** as the Boot Source. For more

	information, see "Configuring the Boot Settings on the DASH Device" on page 111. c. Click **Next.** The Confirmation Summary window opens. Review the information in this window. d. Click **Next** to continue. Summary information displays to your management console. e. Click **Close**.
Local CD Drive	a. From the pull-down menu next to **Remote Operation**, select **Reboot to Local CD/DVD**. b. Click **Next**. For DASH devices, the Boot Settings window opens. In this window, you can specify a Boot Source or Boot Configuration to be used when the device boots up. Select **CD/DVD** as the Boot Source. For more information, see "Configuring the Boot Settings on the DASH Device" on page 111. c. Click **Next.** The Confirmation Summary window opens. Review the information in this window. d. Click **Next** to continue. Summary information displays to your management console. e. Click **Close**.
Primary Boot Device (vPro only)	a. From the pull-down menu next to **Remote Operation**, select **Reboot to Primary Boot Device**. This option enables you to reboot to the default boot device configured in the BIOS of the vPro device. The **SOL Option** is displayed. This local boot option enables you to see the operation displayed to the RCA Console if you select to do so. b. For **SOL Option**, you can select **Display to console** or **Do not display to console.** c. Click **Next**. The Confirmation Summary window opens. Review the information in this window. d. Click **Next**. ○ If you selected **Display to console**, the Remote Operation Wizard closes and a HyperTerminal window opens displaying the reboot process. This window stays open until you close it. ○ If you selected **Do not display to console**, the Summary information window opens. It displays the result of the operation when it completes. You must click **Close** to return to the Device Details window.

In the Task window, you can also indicate the following:

- For vPro devices, you can specify if you want to use the front panel settings for that device. If you select **No**, the front panel settings for the vPro device will be ignored. For more information, see "Configuring Front Panel Settings on the vPro Device" on page 109.
- For DASH devices, you have the **Display Client Console** option where you can specify if you want text to be displayed to the console or not.

The following table lists the steps to perform, based on the drive that you are booting from:

You can use this capability to:

- Remotely reboot non-responsive devices
- Troubleshoot non-responsive devices by using console redirection to view the BIOS boot process and identify a failed component when it does not respond during this process.

Rebooting vPro System with IDE-R

The **Diagnostics** area of the workspace enables you to redirect the boot device for a problem vPro device to a clean image on another remote drive. Integrated drive electronics redirect (IDE-R) provides this CD/Floppy Drive redirection.

Note: IDE-R technology is currently supported on vPro devices only.

Note: vPro devices require a greater amount of time to communicate with the OOBM Server over wireless communication. This can cause a time-out to occur for the SOL/IDE-R remote operations. To avoid this situation, it is possible to configure the IDER* and SOL* parameters as described in "Configuring the IDE-R and SOL Time-out Values" on page 39.

Through the built-in redirection capabilities, you can view the reboot process without user intervention or leaving the management console. SOL and KVM of vPro devices provide keyboard and video redirection to the management console.

Rebooting vPro System to BIOS Settings

The **Diagnostics** area of the workspace enables you to access preboot BIOS settings for verifying configuration information and changing settings as needed to help resolve vPro device problems.

Note: Rebooting to BIOS setting is supported on vPro devices only.

Through the built-in redirection capabilities, you can view the BIOS settings without user intervention or leaving the management console. SOL and KVM on vPro devices provide keyboard and video redirection to the management console.

To reboot the system to BIOS settings, complete the following steps:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the vPro device you want to manage. A management window opens.
4. Click the **Remote Operations** link under the **Diagnostics** section on the left-side of the window. The Remote Operation Wizard window opens.
5. Click **Next** to continue. The Task window opens. You can reboot the device to BIOS settings using various options as shown in the following table:

Rebooting a vPro device to BIOS Settings

BIOS	Steps
BIOS Setup (vPro only)	a. From the pull-down menu next to **Remote Operation**, select **Reboot to BIOS**. The **BIOS Option** is displayed. b. From the pull-down menu next to **BIOS Option**, select **BIOS Setup**. c. Click **Next.** The Confirmation Summary window opens. Review the information in this window. d. Click **Next** to continue. The Remote Operation Wizard closes and a HyperTerminal window opens displaying the reboot process. This window stays open until you close it.
BIOS Pause (vPro only)	a. From the pull-down menu next to **Remote Operation**, select **Reboot to BIOS**. The **BIOS Option** is displayed. b. From the pull-down menu next to **BIOS Option**, select **BIOS Pause**. c. Click **Next.** The Confirmation Summary window opens. Review the information in this window. d. Click **Next** to continue. The Remote Operation Wizard closes and a HyperTerminal window opens displaying the reboot process. This window stays open until you close it.

Also in the Task window for vPro devices, you can specify if you want to use the front panel settings for the vPro device. If you select **No**, the front panel settings for the vPro device will be ignored. For more information, see "Configuring Front Panel Settings on the vPro Device" on page 109.

You can use this capability to:

- Verify configuration information
- Change settings as needed to troubleshoot non-working devices
- Change BIOS settings without having to physically access the device

Rebooting System to Preboot Execution Environment

The **Diagnostics** area of the workspace enables you to reboot OOB devices to Preboot Execution Environment (PXE). This reboot option lets you boot computers using a network interface card without relying on a local hard disk or installed operating system. The OOB device can reboot from the boot image on the PXE server.

> **Note:** This assumes that there is a PXE boot server in your network environment. A PXE boot server requires setting up a DHCP server, a TFTP server, and a boot server to handle PXE boot requests.

To reboot the system to PXE, complete the followings steps:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the device you want to manage. A management window opens.
4. Click the **Remote Operations** link under the **Diagnostics** section on the left-side of the window. The Remote Operation Wizard window opens.
5. Click **Next** to continue. The Task window opens.
6. From the pull-down menu next to **Remote Operation**, select **Reboot to LAN (PXE)**.
   In the Task window, you can also indicate the following:
   - For vPro devices, you can specify if you want to use the front panel settings for that device. If you select **No**, the front panel settings for the vPro device will be ignored. For more information, see "Configuring Front Panel Settings on the vPro Device" on page 109.
   - For DASH devices, you have the **Display Client Console** option where you can specify if you want text to be displayed to the console or not.
7. Click **Next**. For DASH devices, the Boot Settings window opens. In this window, you can specify a Boot Source or Boot Configuration to be used when the device boots up. Select **Network** as the Boot Source. For more information, see "Configuring the Boot Settings on the DASH Device" on page 111.
8. Click **Next.** The Confirmation Summary window opens. Review the information in this window.
9. Click **Next** if you want to continue. Summary information displays to your management console.
10. Click **Close** to exit the wizard.

You can use this capability to:

- Reboot a non-working device to a temporary troubleshooting environment to more accurately identify hardware problems as opposed to software problems
- Rebuild an operating system image on a non-working device
- Provision an operating system to a bare-metal device

Booting to DASH-only Supported Power States

DASH-enabled devices support more power states than vPro devices. The power operations that you can perform in the RCA Console to boot the DASH device to one of these states are the following;

- Suspend
- Hibernate (Soft)
- Power Off (Soft Graceful)
- Power Off (Hard Graceful)
- Power Off (Hard)
- Power Cycle (Soft Graceful)

- Power Cycle (Hard Graceful)
- Power Cycle (Hard)
- Master Bus Reset (Graceful)
- Master Bus Reset
- Diagnostic Interrupt

See "Viewing Power State" on page 85 for a description of these operations and the power states to which they map.

The procedure in the RCA Console to boot a DASH device to one of these power states is the same. The only difference is to specify the specific power operation for that state in the following procedure.

Booting a DASH device using one of the preceding operations

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the DASH device you want to manage. A management window opens.
4. Click the **Remote Operations** link under the **Diagnostics** section on the left-side of the window. The Remote Operation Wizard window opens.
5. Click **Next** to continue. The Task window opens.
6. From the pull-down menu next to **Remote Operation**, select the power operation that will boot the DASH device to the desired power state.
7. In the Task window, you can also select the **Display Client Console** option from the pull-down menu indicating if you want text to be displayed to the console or not.
8. Click **Next**. The Boot Settings window opens. In this window, you can specify a Boot Source or Boot Configuration to be used when the device boots up. For more information, see "Configuring the Boot Settings on the DASH Device" on page 111. This step is not relevant for the Power Off and sleep operations.
9. Click **Next.** The Confirmation Summary window opens. Review the information in this window.
10. Click **Next** to continue. Summary information displays to your management console.
11. Click **Close.**

You can use this capability to boot DASH devices to various power state levels.

KVM Redirection on vPro Devices

The **Diagnostics** area of the workspace enables you to access the remote console of the vPro device in both text and graphical mode using Keyboard Video Mouse Redirection (KVM) technology.

The requirements for KVM to function correctly are the following:

- vPro device must have AMT 6.0 or later.
- JRE 1.6.x and the VNC Viewer must be installed on the machine where you run the browser to access the RCA console. The VNC Viewer uses port 5900.
- On the machine where you access the RCA Console, you must set the **VNC_PATH** environment variable to the path where VNC Viewer is installed. For example: **VNC_PATH=C:\viewer\VNCViewer.exe**.
- You must have administrative rights for vPro web services. To acquire these rights, you must select the **PT Administration** realm when you create your SCS profile in the Intel AMT Console.

Performing KVM redirection on a vPro device

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the vPro device you want to manage. A management window opens.
4. Click the **KVM Redirection** link under the **Diagnostics** section on the left-side of the window. The Settings for KVM Redirection window opens.
5. In the Settings for KVM session section, specify the following:
   - Create and confirm your password for the VNC session. This is a one-time password, which must be reset for each new VNC session for security reasons.
   - Check the box next to the **Enable Opt-in** option if you want to get explicit permission from the user before accessing the user’s machine. This provides greater security requiring a second level of password authentication.

     > **Note:** It is possible to enable this option in the RCA Console, only if the option is enabled on the client vPro device. To enable the option on the vPro device, go into the MEBx console of the client vPro device. Select **Main Menu** > **Intel ® AMT Configuration** > **KVM Configuration** > **Opt-in Configurable from remote IT** > **Enable Remote Control of KVM Opt-In Policy**.
     > This option is enabled by default.
6. Click **Submit**. The VNC Viewer opens prompting for your password.
7. Type the session password that you created in the Password for KVM Redirection window for authentication purposes.
8. Click **OK**.
   If you have enabled the opt-in option, the AMT KVM opt-in window opens prompting for a second password. You obtain this password from the user of the vPro device that you want to access. On the user’s vPro device, the KVM Remote Assistance pop-up window appears (when opt-in is enabled) with a user consent code. You must get this user consent code from the user, enter it in the AMT KVM opt-in window, and click **Yes**.
   The remote console of the vPro device opens.

Managing System Defense Filters on the vPro Device

The **System Defense** area of the workspace is available for vPro devices only. It enables you to manage System Defense filters for individual vPro devices. You can view and remove System Defense filters that have been deployed to a specific vPro device. System Defense filters are assigned to System Defense policies. The filters assigned to a policy become activated when their corresponding policy becomes the active policy.

Opening the System Defense filters management window

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the vPro device you want to manage. A management window opens.
4. Click the **Filters** link under the **System Defense** section on the left-side of the window. A window opens displaying the System Defense filters that have been created and deployed to the vPro device through the RCA Console.

Refreshing the System Defense filter view

1. Open the System Defense filters management window as described in "Opening the System Defense filters management window" above.
2. Click the 🔄 refresh icon on the toolbar.

Viewing the details of a System Defense filter

1. Open the System Defense filters management window as described in "Opening the System Defense filters management window" above.
2. Click the filter name link of the System Defense filter whose detail information you want to see. The Network Filter Detail window opens displaying the specifications for the filter.

Removing System Defense filters

1. Open the System Defense filters management window as described in "Opening the System Defense filters management window" above.
2. Check the box next to each filter that you want to delete.
3. Click the ✖ delete icon. The selected filters are removed from the System Defense Filters table for that vPro device.

You can use the System Defense filter interface to:

- View the existing set of filters that can be applied to policies that have been deployed to the vPro device.
- Remove filters that are no longer needed on the vPro device.

Managing System Defense Policies on the vPro Device

The **System Defense** area of the workspace is available for vPro devices only. It enables you to view, remove, and enable System Defense policies that have been deployed to a specific vPro device. When an enabled policy becomes the active policy based on priority, the filters associated with this policy become activated

Opening the System Defense Policies Management Window

To open the System Defense policies management window, complete the following steps:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the vPro device you want to manage. A management window opens.
4. Click the **Polices** link under the **System Defense** section on the left-side of the window. A window opens displaying the System Defense policies that have been created and deployed to the vPro device through the RCA Console.

Refreshing the System Defense Policy View

To refresh the System Defense policy view, complete the following steps:

1. Open the System Defense policies management window as described in "Opening the System Defense Policies Management Window" above.
2. Click the 🔄 refresh icon on the toolbar.

Toggling Between Policies

To toggle between policies deployed to the wired and wireless NIC, complete the following steps:

> **Note:** This procedure is applicable only if a vPro device has both a wired and wireless Network Interface Card (NIC).

1. Open the System Defense policies management window as described in "Opening the System Defense Policies Management Window" above. If the device has 2 NICs, a window opens displaying the System Defense policies that have been created and deployed to the wired NIC on the vPro device.
2. Click the 📶 wireless icon (this icon appears only if there are both wired and wireless NICs on the vPro device). A window opens displaying the System Defense policies that have been created and deployed to the wireless NIC on the vPro device.

3. Click the wired icon to toggle back to the window that displays the System Defense policies deployed to the wired NIC on the vPro device.

Viewing the Details of a System Defense Policy

To view the details of a System Defense policy, complete the following steps:

1. Open the System Defense policies management window as described in "Opening the System Defense Policies Management Window" on previous page.
2. Click the policy name link of the System Defense policy whose detail information you want to see. The System Defense Policy Detail window opens displaying the specifications for the policy.
3. Click **Next** to see the filters associated with the policy.
4. If there is more than one NIC on the vPro device, click the toggle icon as described in "Toggling Between Policies" on previous page and repeat this procedure for the other NIC.

Setting an Agent Presence Policy

To set an Agent Presence policy, complete the following steps:

1. Open the System Defense policies management window as described in "Opening the System Defense Policies Management Window" on previous page.
2. Check the box next to the policy that you want to set as an Agent Presence policy to be enabled by a watchdog action. You can select only one policy to be an Agent Presence policy.
3. Click the set icon on the toolbar. The selected policy becomes the Agent Presence policy. This policy can become enabled through a watchdog action. It will become the active policy if it has a higher priority than the enabled System Defense policy.
4. If there is more than one NIC on the vPro device, click the toggle icon as described in "Toggling Between Policies" on previous page and repeat this procedure for the other NIC.

Enabling a System Defense Policy

To enable a System Defense policy, complete the following steps:

1. Open the System Defense policies management as described in "Opening the System Defense Policies Management Window" on previous page.
2. Check the box next to the policy that you want to enable. You can select only one policy.
3. Click the enable icon on the toolbar. The selected policy becomes the new System Defense default policy.
4. If there is more than one NIC on the vPro device, click the toggle icon as described in "Toggling Between Policies" on previous page and repeat this procedure for the other NIC.

Removing System Defense Policies

To remove System Defense policies, complete the following steps:

1. Open the System Defense policies management window as described in "Opening the System Defense Policies Management Window" on page 105.
2. Check the box next to each policy that you want to delete.
3. Click the ✖ delete icon on the toolbar. The selected policies are removed from the System Defense Policies table for the specific vPro device.
4. If there is more than one NIC on the vPro device, click the toggle icon as described in "Toggling Between Policies" on page 105 and repeat this procedure for the other NIC.

You can use the System Defense policy interface to:

- View System Defense policies on a vPro device.
- Enable a System Defense policy that can become the active policy based on priorities.
- Set a policy to be the Agent Presence policy that can become enabled through a watchdog action. If this policy has the higher priority, it becomes the active policy.
- Remove policies that are no longer needed.

Managing Heuristics on the vPro Device

The **System Defense** area of the workspace is available for vPro devices only. It enables you to view and remove heuristics information that has been deployed to a specific vPro device.

Opening the Heuristics Management Window

To open the heuristics management window, complete the following steps:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the vPro device you want to manage. A management window opens.
4. Click the **Heuristics** link under the **System Defense** section on the left-side of the window. A window opens displaying the heuristics that have been created and deployed to the vPro device through the RCA Console.

Refreshing the Heuristics View

To refresh the heuristics view, complete the following steps:

1. Open the heuristics management window as described in "Opening the Heuristics Management Window" above.
2. Click the 🔄 refresh icon on the toolbar

Viewing the Details for a Heuristics Specification

To view the details for a heuristics specification, complete the following steps:

1. Open the heuristics management window as described in the "Opening the Heuristics Management Window" on previous page.
2. Click the heuristics name link of the heuristics whose detail information you want to see. The Heuristics Details window opens displaying the specifications for the heuristics.
3. Click **Close** to close the details window.

Viewing the Heuristics State Information

To view the heuristics state information for a NIC interface on the device, complete the following steps:

1. Open the heuristics management window as described in "Opening the Heuristics Management Window" on previous page.
2. Click the heuristics NIC Type link of the heuristics whose NIC interface state information you want to see. The Heuristics State Information window opens displaying the state information for the specific NIC interface. It will indicate if the heuristics conditions have been met and what actions have been taken.
3. Click **Close** to close the state information window.

Clearing the Heuristics Actions

To clear the heuristics actions, complete the following steps:

1. Open the heuristics management window as described in "Opening the Heuristics Management Window" on previous page.
2. Check the box next to each heuristics for which you want to clear the actions associated with it.
3. Click the ⊗ clear heuristics actions icon on the toolbar. The actions associated with the selected heuristics are cleared. As a result, outbound packets are no longer blocked, the suspected port is opened, and the specified System Defense policy is deactivated.

Removing Heuristics

To remove heuristics, complete the following steps:

1. Open the heuristics management window as described in "Opening the Heuristics Management Window" on previous page.
2. Check the box next to each heuristic that you want to delete.
3. Click the ✖ delete icon on the toolbar. The selected heuristics are removed from the heuristics table for the specific vPro device.

You can use the heuristics interface to:

- View the heuristics on the vPro device.
- Remove heuristics information that is no longer needed.

Managing Watchdogs on the vPro Device

The **System Defense** area of the workspace is available for vPro devices only. It enables you to view and remove watchdogs that have been deployed to a specific vPro device.

Opening the watchdog management window

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the vPro device you want to manage. A management window opens.
4. Click the **Watchdogs** link under the **System Defense** section on the left-side of the window. A window opens displaying the Watchdogs that have been created and deployed to the vPro device through the RCA Console.

Refreshing the watchdog view

1. Open the watchdog management window as described in "Opening the watchdog management window" above.
2. Click the 🔄 refresh icon on the toolbar.

Viewing the details of a watchdog

1. Open the watchdog management window as described in "Opening the watchdog management window" above.
2. Click the watchdog name link of the watchdog whose detail information you want to see. The Watchdog Detail window opens displaying the specifications for the watchdog.
3. Click **Close** to close the detail window.

Removing watchdogs

1. Open the watchdog management window as described in "Opening the watchdog management window" above.
2. Select the check box next to each watchdog that you want to delete.
3. Click the ✖ delete icon on the toolbar. The selected watchdogs are removed from the watchdog table for the specific vPro device.

You can use the watchdog interface to:

- View the watchdog agents on the vPro device.
- Remove a watchdog that is no longer needed.

Configuring Front Panel Settings on the vPro Device

The **General Settings** area of the workspace is available for vPro devices only. It enables you to lock and unlock the keyboard and power button on the vPro device during remote power operations.

> **Note:** Front panel settings can be set by the user based on the capabilities of the target device. The front panel settings feature is dependent on the BIOS of the specific vPro device. If the BIOS of the device does not support front panel settings, this feature cannot be controlled from the RCA Console. It is recommended that you check with your hardware vendor for specific support-related information.

To configure front panel settings, complete the following steps:

1. Log into the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the vPro device you want to manage. A management window opens.
4. Click the **Front Panel Settings** link under the **General Settings** section on the left-side of the window. The Front Panel Settings Dialog opens.
5. Click the **here** link to enable the **Front Panel Settings** section of the dialog. If front panel settings are supported by the device, the default lock settings are set to **Yes**.
6. Keep the default settings if you want the keyboard and/or power button on the vPro device to be locked during remote power operations.
7. Click **Update**. A confirmation message displays to the screen.
8. Click **Close** to exit the dialog.

You can use the front panel settings to ensure that there is no local interference when performing remote power operations from the RCA Console.

Resetting Flash Limit on the vPro Device

The **General Settings** area of the workspace is available for vPro devices only. It enables you to reset the flash limit for the vPro device. For more information about flash memory, see "Management of Common Utilities" on page 81.

To reset the flash limit, complete the following steps:

1. Log into the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link for the vPro device you want to manage. A management window opens.
4. Click the **Flash Limit Reset** link under the **General Settings** section on the left-side of the window. The Flash Limit Reset Dialog opens.
5. Click **Reset**. A confirmation message is displayed.
6. Click **OK** to continue. The counter for the 3PDS memory on the device is reset to zero.

You can use flash limit reset to reset the 3PDS counter on the vPro device, which serves as a flash wear-out protection mechanism. This feature enables you to continue to perform activities that write to this non-volatile memory store.

Configuring the Boot Settings on the DASH Device

The **Configuration Settings** area of the workspace is available for DASH devices only. A DASH device can have multiple boot configuration settings. You can choose any one of the available boot configuration settings to be used during a boot process.

Each boot configuration setting can have any number of available boot sources attached to it, for example, Hard Drive, CD, USB, and so on. Also, each boot configuration setting can have its own boot order for the attached boot sources. The same boot source can be attached to multiple boot configuration settings.

This area of the workspace enables you to view the available boot configuration settings, configure the one time boot configuration, and change the boot order when performing a remote operation on a DASH device. For more information, see "Changing Power State" on page 93.

Configuring the boot settings

1. Log into the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Device Management**. The Device Management window opens.
3. Click the hostname link of the DASH device you want to manage. A management window opens.
4. Click the **Boot Configuration** link under the **Configuration Settings** section on the left-side of the window. The Boot Configuration list is displayed.

   > **Note:** Currently for Broadcom DASH devices, only two boot configuration settings are available, **Boot Configuration Setting #1** and **Boot Configuration Setting #2**.

   The list indicates the following about the boot configuration settings:

   - **Default**: If checked, it is the boot configuration setting that the computer system manufacturer has tagged as its default boot configuration. The **Default** setting does *not* affect which boot configuration applies during the boot process.
   - **Next**: If checked, it is the boot configuration setting that will be used during the next boot of the DASH device (and subsequent reboots), unless the **Only Next** is selected.

     > **Note:** In case of the current Broadcom DASH devices, **Boot Configuration Setting#1** is always the **Next** boot configuration setting, and it cannot be changed.

   - **Only Next**: If checked, it is the boot configuration setting that will be used during the very next boot of the DASH device and then not used again. The **Only Next** boot configuration setting takes precedence over the **Next** boot configuration setting.
   - **Current**: If checked, it is the boot configuration setting that was used the last time the DASH device was successfully booted.

> **Note:** Currently, you will see check marks only in the **Next** and in the **Only Next** columns when **One time boot configuration** is selected.

- **Boot Order**: The boot sources and order attached to the boot configuration setting.

> **Note:** If the boot sources in the **Boot Order** column are displayed in green text, it represents an erroneous condition indicating that these boot source devices are being used in the current boot process. This is an error with the hardware. If you see the devices displayed in green text, you must change the boot order using the Boot Configuration Wizard as explained in the following steps.

5. Select the boot configuration setting you want to manage in the Boot Configuration list.

6. From the pull-down menu on the☰ boot configuration parameters icon on the toolbar of the Boot Configuration list table, select the boot configuration option you want to perform. Currently, you can select only the following option:
   - **One time boot configuration**: Changes the boot order for the very next time the device is powered on or rebooted. After this one time, it will revert back to the boot order of the current boot configuration.

   When you select this option, the Update Boot Configuration Wizard opens.

7. Click **Next** to continue. The Settings window opens.

8. In the **Current Boot Order** list, select a boot device and click **Add** to include it in the **New Boot Order** list. To remove a boot device from the **New Boot Order list,** select the device and click **Remove**.
   The **Current Boot Order** list displays all the boot devices from which the device can boot. The boot devices that are currently being used in the current boot order are displayed in black text. The boot devices that are available but not being used in the current boot order are displayed in gray.

9. Click **Next** when you are satisfied with the new boot order. The Complete window opens displaying status information.

10. Click **Close** to exit the wizard. The changes you have made will be reflected in the Boot Configuration list.

You can use the ability to view and change the boot configuration settings for DASH devices as a tool to help troubleshoot remote power management problems.

Chapter 6

Group Management

This chapter tells you how to manage Client Automation device groups that contain vPro devices through the RCA Console. You can remotely manage Client Automation groups that contain vPro devices regardless of their power state, the health of their operating systems, or the existence of management agents

One of the Out of Band Management options on the **Operations** tab in the RCA Console is **Group Management**.

> **Note:** This option will not be present in the RCA Console unless you have selected to manage vPro devices.

This option enables you to do the following:

- "Managing Multiple Groups of vPro Devices" below
- "Managing Individual vPro Devices" on page 120

Managing Multiple Groups of vPro Devices

When managing groups, you can specify what groups are displayed and how they are sorted in the group list by doing the following:

- Search for specific groups based on search criteria
- Select the number of groups to be displayed at a time to see a subset of groups for ease of viewing
- Sort the groups based on column headings

The icons on the toolbar of the group list enable you to manage multiple groups at once.

Group List Toolbar

Icon	Function
🔄	Refreshes the groups displayed in the list
🔄	Synchronizes the device groups displayed in the list with the Client Automation repository
⏻	Performs power management tasks to selected groups
⚠	Manages alert subscription to selected groups
📋	Deploys OOBM agent software list to selected groups
▣	Provisions device groups

Icon	Function
📜	Deploys and undeploys System Defense policies to selected groups
●	Deploys and undeploys watchdogs to selected groups
🛡	Deploys and undeploys heuristics to selected groups

Note: As indicated in the device list toolbar table, the 🔄 icon enables you to manually reload the group device information displayed in the group list by synchronizing it with the current device information. In addition to a manual reload, OOBM can automatically reload the group list at regular time intervals. This time interval is configurable in the config.properties file (located in <*RCA_Install_DIR*>\oobm\conf\ directory) by setting the group_synchronization_timeperiod parameter to the new value.
The synchronization time interval has a default value of zero, indicating that automatic synchronization will not occur. If you want synchronization to occur automatically, set the new value to a non-zero value. The unit for this value is minutes.

Multiple Group Selection

To select multiple groups, complete the following steps:

1. Login into the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management** in the left navigation pane, click **Group Management**. The Group Management window opens displaying all Client Automation groups. The groups that contain vPro devices will be displayed as active links in the table indicating that they can be managed through the console.
3. Select the groups that you want to access by selecting the check box for the group or by selecting the select all check box in the upper left. You can search on groups with certain criteria and sort the groups to aid in selection.

Synchronizing the Group List with the Client Automation Repository

To synchronize the group list with the Client Automation repository:

- To immediately reload the group list from the Client Automation repository, select **Immediate Group Reload** from the pull-down menu on the 🔄 reload icon. When you select this option, the reload is performed immediately and you will see activity in the group list window as the process occurs. When the process completes, the group list will display the groups that are currently found in the Client Automation repository.
- To reload the group list from the Client Automation repository as a background process, select **Background Group Reload** from the pull-down menu on the 🔄 reload icon. When you select this option, you will see no activity in the group list window. You can check the status of this background process by selecting **View Reload Status** from the pull-down menu on the 🔄 reload icon. When the process completes, you must click the 🔄 refresh icon to see the reloaded group list.

Power Management

To power manage device groups, complete the following steps:

1. Select the groups you want to manage as described in "To select multiple groups, complete the following steps:" on previous page.
2. Click the power management icon on the toolbar. The Power Operation Wizard opens.
3. Click **Next**. The Options window opens.
4. Select the power operation you want to perform on the selected group(s).
5. Click **Next**. The Summary window opens.
6. Click **Next**. The Complete window opens displaying the results of the operation.
7. Click **Close** to exit the wizard.

You can use this functionality to effectively power up and down multiple device groups at specific times for cost savings.

Alert Subscription Management

To manage alert subscriptions on device groups, complete the following steps:

1. Select the groups you want to manage as described in "To select multiple groups, complete the following steps:" on previous page.
2. Click the alert subscription management icon. The Alert Subscription Management Wizard opens.
3. Click **Next**. The Options window open.
4. Select whether you want to subscribe to or cancel an alert subscription.
5. Click **Next**. The Summary window opens.
6. Click **Next**. The Complete window opens displaying the results of the operation.
7. Click **Close** to exit the wizard.

You can use this functionality to subscribe and cancel subscriptions to multiple device groups so that pertinent event alerts can be sent to the RCA Console.

Deployment of OOBM Agent Software List

To deploy OOBM agent software list, complete the following steps:

1. Select the groups you want to manage as described in "To select multiple groups, complete the following steps:" on previous page.
2. Click the deploy software list icon. The Software Deployment Wizard opens.
3. Click **Next**. The Software window opens.

4. Select the software names you want to add to the software list to be deployed to the selected group(s).
5. Click **Next**. The Summary window opens.
6. Click **Next**. The Complete window opens displaying the results of the operation.
7. Click **Close** to exit the wizard.

You can use this functionality to create a master list of software applications from which you can select a customized list of applications that you want the OOBM agent to monitor on the target vPro device group.

Provisioning

This section lists the steps to perform provisioning operations on device groups and view the results with minimal effort.

Performing provisioning operations

1. Select the groups you want to manage as described in "To select multiple groups, complete the following steps:" on page 115.
2. Select **Perform Provisioning Operations** from the pull-down menu on the provisioning icon. The Provisioning Operations Wizard opens.
3. Click **Next**. The Options window opens.
4. Select the provisioning operation you want to perform to the selected group(s). See "Performing Provisioning Tasks" on page 72 for an explanation of the provisioning operations.
5. Click **Next**. The Summary window opens.
6. Click **Next**. The Complete window opens displaying the results of the operation.
7. Click **Close** to exit the wizard.

Viewing the provisioning status log

1. Select the groups you want to manage as described in "To select multiple groups, complete the following steps:" on page 115.
2. Select **View the Provisioning Status Log** from the pull-down menu on the provisioning icon. The Provisioning Status Log window opens. The status of the provisioning operations is displayed in the log.

Deployment of System Defense Policies

This section lists the procedures that you can use to deploy multiple System Defense policies to multiple vPro device groups to protect these systems from malware attacks.

Deploying System Defense Policies

1. Select the groups you want to manage as described in "To select multiple groups, complete the following steps:" on page 115.
2. Select **Deploy System Defense Policies** from the pull-down menu on the manage System Defense policies icon. The Policy Deployment Wizard opens.

3. Click **Next**. The Policies window opens.
4. Select the System Defense policies you want to deploy to the selected group(s).
5. Click **Next**. The Settings window opens.
6. From the pull-down menus, select the Agent Presence and System Defense policies you want to assign to the wired and wireless NICs on your device groups.
7. Click **Next**. The Summary window opens.
8. Click **Next**. The Complete window opens displaying the results of the operation.
9. Click **Close** to exit the wizard.

Undeploying System Defense Policies

1. Select the groups you want to manage as described in "To select multiple groups, complete the following steps:" on page 115.
2. Select **Undeploy System Defense Policies** from the pull-down menu on the manage System Defense policies icon. The Policy Undeployment Wizard opens.
3. Click **Next**. The Policies window opens.
4. Select the policies you want to undeploy from the selected group(s).
5. Click **Next**. The Summary window opens.
6. Click **Next**. The Complete window opens displaying the results of the operation.
7. Click **Close** to exit the wizard.

Deployment of Watchdogs

This section lists the procedures that you can use to deploy multiple watchdogs to multiple vPro device groups to monitor the OOBM agents on these systems. Monitoring OOBM agents enhances the security of the network because these agents are in turn monitoring security software running on provisioned devices. If the security software stops running (inadvertently through user intervention or otherwise), the watchdog can alert the system administrator of this event.

Deploying watchdogs

1. Select the groups you want to manage as described in "To select multiple groups, complete the following steps:" on page 115.
2. Select **Deploy Watchdogs** from the pull-down menu on the manage watchdogs icon. The Watchdog Deployment Wizard opens.
3. Click **Next**. The Watchdogs window opens.
4. Select the watchdogs you want to deploy to the selected group(s).
5. Click **Next**. The Summary window opens.
6. Click **Next**. The Complete window opens displaying the results of the operation.
7. Click **Close** to exit the wizard.

Undeploying watchdogs

1. Select the groups you want to manage as described in "To select multiple groups, complete the following steps:" on page 115.
2. Select **Undeploy Watchdogs** from the pull-down menu on the manage watchdogs icon. The Watchdog Undeployment Wizard opens.
3. Click **Next**. The Watchdogs window opens.
4. Select the watchdogs you want to undeploy from the selected group(s).
5. Click **Next**. The Summary window opens.
6. Click **Next**. The Complete window opens displaying the results of the operation.
7. Click **Close** to exit the wizard.

Deployment of Heuristics

This section lists the procedures that you can use to deploy multiple heuristics to multiple vPro device groups for worm containment of infected devices.

Deploying heuristics

1. Select the groups you want to manage as described in "To select multiple groups, complete the following steps:" on page 115.
2. Select **Deploy Heuristics** from the pull-down menu on the manage heuristics icon. The Heuristics Deployment Wizard opens.
3. Click **Next**. The Heuristics window opens.
4. Select the heuristics you want to deploy to the selected group(s).
5. Click **Next**. The Settings window opens.
6. From the pull-down menus, select the heuristics you want to assign to the wired and wireless NICs on your device groups.
7. Click **Next**. The Summary window opens.
8. Click **Next**. The Complete window opens displaying the results of the operation.
9. Click **Close** to exit the wizard.

To undeploy heuristics

1. Select the groups you want to manage as described in "To select multiple groups, complete the following steps:" on page 115.
2. Select **Undeploy Heuristics** from the pull-down menu on the manage heuristics icon. The Heuristics Undeployment Wizard opens.
3. Click **Next**. The Heuristics window opens.
4. Select the heuristics you want to undeploy from the selected group(s).
5. Click **Next**. The Summary window opens.
6. Click **Next**. The Complete window opens displaying the results of the operation.

7. Click **Close** to exit the wizard.

Managing Individual vPro Devices

The group list table displayed on the **Group Management** window shows the group type, the number of devices in the group, its creation date, and other attributes.

To drill down to manage individual devices within a group, click the group name link under the Description column of the table. The Group Details window opens. This window has the following tabbed sections:

- "General Tab" below
- "Properties Tab" below
- "Devices Tab" below

General Tab

The **General** tab has Common Tasks and Summary areas. The Common Tasks area provides links that serve as shortcuts to functionality that is provided on the other tabbed sections. The Summary area provides statistics about the device group.

Properties Tab

The **Properties** tab displays the properties of the selected group. To better understand group properties, see the *Radia Client Automation Enterprise User Guide*.

Devices Tab

The **Devices** tab displays the list of vPro devices belonging to the selected group. You can manage multiple or individual devices within the group. For more information, see "Device Management" on page 76.

Chapter 7

Alert Notifications

This chapter provide information about "Viewing Alerts on the vPro Device" below.

Viewing Alerts on the vPro Device

You can use the RCA Console to view event alerts. These alerts are created by provisioned vPro devices when an event occurs, and they are sent to the RCA Console. You will see the alerts if you have an alert subscription to the device.

To refresh the alerts view:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management**, click **Alert Notifications**. The Alert Notifications window opens. This tab displays the alerts that have been created by vPro devices to which you have an alert subscription.
3. Click the refresh icon on the toolbar.

To see details about a vPro alert:

1. Log in to the RCA Console and select the **Operations** tab.
2. Under **Out of Band Management**, click **Alert Notifications**. The Alert Notification window opens. This tab displays the alerts that have been generated by vPro devices to which you have an alert subscription.
3. Click the detail icon in the Detail column. A window opens that displays the property details for the selected alert.
4. You can use alerts subscriptions to determine if a noteworthy event alert has occurred that requires immediate action.

Chapter 8

Use Case Scenarios

This chapter explains how you can use the RCA Console to perform some standard scenarios when managing OOB devices. These scenarios take into account how you can discover assets on devices, perform various heal functions, and protect vPro devices on your network from malware attacks. You can use the RCA Console to remotely manage devices regardless of their power state, the health of their operating systems, or the existence of management agents. These scenarios are not intended to be a complete, exhaustive representation of how you will use the Out of Band Management (OOBM) features in the RCA Console in your enterprise but rather serve as illustrative examples.

The following use cases are described in this section:

- "Hardware Failure and Replacement" below
- "Operating System Failure and Reboot" on page 126
- "Virus Infection Detection and Quarantine" on page 127
- "Device Quarantine and Remediation" on page 130
- "Monitoring Critical Software" on page 132
- "Worm Infection and Containment" on page 139

Note: Most of the use cases described here are relevant to vPro devices. DASH devices are mentioned wherever applicable. However, the navigation and procedural details may vary for DASH devices. For detailed procedural information, see "Device Management" on page 76.

Hardware Failure and Replacement

This use case is divided into the following sections:

- "Overview" below
- "Use Case Process" on next page

Overview

A hardware sensor type failure occurs. The failure causes the Event Manager residing on the vPro chip to raise an event. Based on the information in the Event Filter, the Event Manager sends an event alert to the RCA Console.

The administrator wants to

- Subscribe to vPro devices for event alert notification (subscription must already be in place before the hardware failure occurs).
- Discover the hardware assets on the vPro or DASH device to get the correct replacement part.

By subscribing to the vPro device for alert notification, the event alert is automatically sent to the RCA Console. The administrator then looks up the hardware inventory for that device and orders the exact replacement part to get the machine up and running again.

Use Case Process

Complete the following tasks to implement this scenario:

- "Subscribe for Event Alert Notifications" below
- "View Alerts" below
- "View Hardware Assets" below

Subscribe for Event Alert Notifications

To subscribe to vPro devices for event alert notifications, complete the following steps:

1. On the **Operations** tab under **Out of Band Management** in the left navigation menu, click **Device Management**. The Device Management window opens.
2. Select the devices that you want to subscribe to by selecting the check box for the device or by checking the select all check box in the upper left.
3. From the alert subscription management icon pull-down list, select **Subscribe to Alerts**.

For more information, see "Alert Subscription Management" on page 81.

View Alerts

To view alerts, complete the following steps:

1. On the **Operations** tab under **Out of Band Management** in the left navigation menu, click **Alert Notifications**. The Alert Notifications window opens.
2. View the alerts of interest that have been sent to the RCA Console. In this case, you are specifically looking for event alerts caused by hardware failures.

For more information, see "Viewing Alerts on the vPro Device" on page 122.

View Hardware Assets

To view hardware assets, complete the following steps:

1. On the **Operations** tab under **Out of Band Management** in the left navigation menu, click **Device Management**. The Device Management window opens.
2. Click the hostname link for the vPro device with the hardware failure.
3. Click the **Device Assets** link in the Device column of the table under **Diagnostics** on the left-side of the window.
4. Click **Hardware Information**.
5. Click the failed hardware component. Specifications for that component are displayed in the content area of the console.

For more information, see "Viewing Hardware Assets" on page 91.

You can then order a replacement part based on the information obtained from the vPro or DASH device through the RCA Console.

Operating System Failure and Reboot

This use case is divided into the following sections:

- "Overview" below
- "Use Case Process" below

Overview

The operating system on a vPro or DASH device is not responding. The administrator is notified by the user of the PC.

The administrator wants to:

- Lock the front panel of the remote vPro device (in this example, we are assuming that this is supported on the vPro device) so that there is no user interference while performing the remote power operation. The front panel setting feature is not available on DASH devices.
- Reboot the PC from an operating system image file that is on the RCA Console Server to further diagnose the problem.

Use Case Process

Complete the following tasks to implement this scenario:

- "Lock the Front Panel on the vPro Device" below
- "Reboot the System with IDE-R CD Drive" below

Lock the Front Panel on the vPro Device

To lock the front panel on the vPro device, complete the following steps:

1. On the **Operations** tab under **Out of Band Management** in the left navigation menu, click **Device Management**. The Device Management window opens.
2. Click the hostname link in the Device column for the OOB device with the operating system failure.
3. Click the **Front Panel Settings** link under **General Settings** on the left-side of the window.
4. Click the **here** link to enable the **Front Panel Settings** section of the dialog.
5. Ensure that the settings for the keyboard and power button are set to **Yes**.

For more information, see "Configuring Front Panel Settings on the vPro Device" on page 109.

Reboot the System with IDE-R CD Drive

To reboot the system with IDE-R CD Drive, complete the following steps:

1. On the **Operations** tab under **Out of Band Management** in the left navigation menu, click **Device Management**. The Device Management window opens.
2. Click the hostname link for the vPro device with the operating system failure.
3. Click the **Remote Operations** link under **Diagnostics** on the left-side of the window.
4. In the Remote Operations Wizard, select **Reboot to IDE-R** for the Remote Operation and select **Yes** for Apply Front Panel Settings option.
5. Enter the path to an ISO file that is on the management console server in the Drive Path field.
6. Follow the remaining steps in the wizard.

For more information, see "Rebooting vPro System with IDE-R" on page 99.

Virus Infection Detection and Quarantine

This use case is divided into the following sections:

- "Overview" below
- "Use Case Steps" below

Overview

A virus attack is suspected because the vPro device has detected network traffic that matches the rate limit filter in the currently active System Defense policy. The match causes the Event Manager residing on the vPro chip to raise an event. Based on the information in the Event Filter, the Event Manager sends an event alert to the RCA Console.

The administrator wants to:

- Subscribe to vPro devices for event alert notification.
- Create a quarantine policy with the necessary filter so that the virus is contained on the infected device and not permitted to spread to the other devices on the network.
- Enable, activate, and deploy the policy to the infected vPro device.
- Repair, replace, or remove the device.
- Disable the policy when the device is no longer a threat.

When the policy is created, deployed, and activated, the vPro device inspects packets and performs the actions specified by the filters associated with the Quarantine policy. In this case, the filter will drop all TCP packets that are transmitted by this device. After the machine is isolated from the network, the administrator performs the remediation tasks required to restore the vPro device and then disables the quarantine policy.

Use Case Steps

Complete the following tasks to implement this scenario:

- "Subscribe for Event Alert Notifications" on next page
- "View Alerts" on next page

- "Create the Quarantine Filter" below
- "Create the Quarantine Policy" below
- "Enable, Activate, and Deploy the Quarantine Policy" on next page
- "Deactivate the Quarantine Policy" on next page

Subscribe for Event Alert Notifications

To subscribe to vPro devices for event alert notifications, follow the steps in "Subscribe for Event Alert Notifications" on page 125 in use case "Hardware Failure and Replacement" on page 124.

View Alerts

To view alerts, follow the steps in "View Alerts" on page 125 in use case "Hardware Failure and Replacement" on page 124. In this case, you are specifically looking for event alerts triggered by a rate limit filter.

Create the Quarantine Filter

To create the quarantine filter, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Filters**. The Filters window opens.
2. Click the ✚ add icon on the toolbar. The System Defense Filter wizard opens.
3. Click **Next** to continue. The Filter Details window opens. In this window, specify the following:
   - **Filter Name**: Enter **Quarantine**.
   - **Filter Type**: Select **Drop**.
   - **Create Event on Filter Match**: Select **Yes**.
4. Click **Next**. The Parameters window opens. In this window, specify the following:
   - **Packet Type**: Select **TCP**.
   - **Filter Mode or Direction**: Select **Transmit**.
   - **Network Address**: Select **Filter Packets to Network**.
   - **Port Range**: Select **Source Port Range**. Enter `1` and `655535` for the **Min Port** and **Max Port** values. This refers to the ports on the vPro device. You want to block packets from all source ports on the vPro device to all destination ports on all of the devices in the network to prevent the vPro device from infecting the other devices.
5. Click **Next** and **Close**.

For more information, see "Managing System Defense Filters" on page 55.

Create the Quarantine Policy

To create the quarantine policy, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Policies**. The Policies window opens.
2. Click the ✚ add icon on the toolbar. The System Defense Policy wizard opens.
3. Click **Next** to continue. The Policy Details window opens. In this window, specify the following:
   - **Policy Name**: Enter **Quarantine**.
   - **Priority**: Enter **98**.
   - **Enable Anti Spoofing Filter**: Select **Yes**.
   - **Default Receive (Rx) Filter Type**: Select **Pass**.
   - **Default Transmit (Tx) Filter Type**: Select **Pass**.
4. Click **Next** to see all available filters.
5. Drag the Quarantine filter to the **Filters to assign to policy** list.
6. Click **Add Policy**.

For more information, see "Managing System Defense Policies" on page 59.

Enable, Activate, and Deploy the Quarantine Policy

To enable, activate, and deploy the Quarantine policy to the vPro device, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Policies**. The Policies window opens.
2. Check the box next to the Quarantine policy.
3. Click the deploy icon on the toolbar The Policy Deployment wizard opens.
4. Click **Next** to continue. The Select Devices window opens.
5. Check the box next to the infected vPro device.
6. Click **Next**. The Set Policies window opens.
7. Select the Quarantine policy as the System Defense Policy for the wired NIC. This enables the Quarantine policy as the System Defense policy for the infected vPro device. Since you specified the highest priority (98) for this policy (with regard to the other System Defense policies currently defined) when you created the policy, it also becomes the active policy for the infected vPro device.
8. Follow the remaining steps in the wizard.

For more information, see "Managing System Defense Policies" on page 59.

Deactivate the Quarantine Policy

To deactivate the Quarantine policy from the vPro device, complete the following steps:

1. On the **Operations** tab under **Out of Band Management** in the left navigation menu, click **Device Management**. The Device Management window opens.
2. Click the hostname link of the vPro device that was infected with the virus.
3. Click the **Policies** link under the **System Defense** section on the left-side of the window. A window opens displaying the System Defense policies that have been deployed to this device.
4. Check the box next to the Quarantine.
5. Click the enable/disable icon on the toolbar. The Quarantine is no longer the enabled System Defense policy.

For more information, see "Managing System Defense Policies on the vPro Device" on page 105.

Device Quarantine and Remediation

This use case is divided into the following sections:

- "Overview" below
- "Use Case Steps" below

Overview

An administrator needs to quarantine a specific device from the corporate network to prevent any attacks. However, the device will need to connect to a management server to receive the remediation it requires. The remediation may consist of an update to its virus definitions, a new version of its firewall software, or remote control by the administrator into the suspect device.

If all network traffic is blocked, it makes remediation of the device virtually impossible. As a result, the administrator must block all network traffic except to and from the remediation management server, so that the infected device can be repaired.

The administrator wants to:

- Create a remediation policy with the necessary filters so that all network traffic is blocked except to the Radia Client Automation Server that contains the necessary software to repair the infected device.
- Enable, activate, and deploy the policy to all vPro devices on the network.
- Disable the policy when the device is repaired.

When the policy is created, deployed, and activated, the vPro devices inspect packets and perform the actions specified by the filters associated with the remediation policy. In this case, the filters will pass all TCP and UDP packets that are received from or transmitted to the device whose IP address matches the one specified in the filter. For this example, it is the IP address of the Radia Client Automation Server. All other packets will be dropped based on the default action of the policy, which is to drop the packets..

Use Case Steps

You want to create 4 filters for the remediation policy. You must complete the procedures listed in this section 4 times, once for each filter you need to create.

- "Create the Remediation Filters" below
- "Create the Remediation Policy" on next page
- "Enable, Activate, and Deploy the Remediation Policy" on next page
- "Deactivate the Remediation Policy" on next page

Create the Remediation Filters

To create the remediation filters, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Filters**. The Filters window opens.
2. Click the ✚ add icon on the toolbar. The System Defense Filter wizard opens.
3. Click **Next** to continue. The Filter Details window opens. You want to specify the following for the corresponding filters you are creating:

Remediation Filters

Filter Name	Filter Type	Create Event on Filter Match
PassTCP_Recv	Pass	Yes
PassTCP_Xmit	Pass	Yes
PassUDP_Recv	Pass	Yes
PassUDP_Xmit	Pass	Yes

4. Click **Next**. The Parameters window opens. You want to specify the following for the corresponding filters you are creating:

Remediation Filters

Filter Name	Packet Type	Next Protocol	Filter Mode	Network Address
PassTCP_Recv	IP Packets (IPv4)	TCP	Receive	Device:192.168.5.12
PassTCP_Xmit	IP Packets (IPv4)	TCP	Transmit	Device:192.168.5.12
PassUDP_Recv	IP Packets (IPv4)	UDP	Receive	Device:192.168.5.12
PassUDP_Xmit	IP Packets (IPv4)	UDP	Transmit	Device:192.168.5.12

5. Click **Next** and **Close**.

> **Note:** You could also create the filters to drop all traffic except to or from a specific subnet instead of to or from a single device. This is useful if you have several remediation servers located on a single subnet.

For more information, see "Managing System Defense Filters" on page 55.

Create the Remediation Policy

To create the remediation policy, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Policies**. The Policies window opens.
2. Click the ✚ add icon on the toolbar. The System Defense Policy wizard opens.
3. Click **Next** to continue. The Policy Details window opens. In this window, specify the following:
    - **Policy Name**: Enter **Remediation**.
    - **Priority**: Enter **98**.
    - **Enable Anti Spoofing Filter**: Select **Yes**.
    - **Default Receive (Rx) Filter Type**: Select **Drop**.
    - **Default Transmit (Tx) Filter Type**: Select **Drop**.
4. Click **Next** to see all available filters.
5. Drag the PassTCP_Recv, PassTCP_Xmit, PassUDP_Recv, and PassUDP_Xmit filters to the **Filters to assign to policy** list.
6. Click **Add Policy**.

For more information, see "Managing System Defense Policies" on page 59.

Enable, Activate, and Deploy the Remediation Policy

To enable, activate, and deploy the remediation policy to the vPro device, follow the steps in "Enable, Activate, and Deploy the Quarantine Policy" on page 129 in use case "Virus Infection Detection and Quarantine" on page 127. In this case, select the Remediation policy.

Deactivate the Remediation Policy

To deactivate the Remediation policy from the vPro device, follow the steps in "Deactivate the Quarantine Policy" on page 129 in use case "Virus Infection Detection and Quarantine" on page 127. In this case, select the Remediation policy.

Monitoring Critical Software

This use case is divided into the following sections:

- "Overview" on next page
- "View the vPro Event Filter" on page 134

Overview

An OOBM agent is installed and started on a vPro device to monitor a list of security software applications, a monitored security application stops, and the OOBM agent stops sending heartbeats to the watchdog. This transition state causes the watchdog to take the actions that the administrator specified when creating the watchdog. In this case, the watchdog raises an event and enables the Agent Presence policy.

Typically, this type of scenario occurs when users have disabled their anti-virus software thinking it hurts their performance. The security administration wants to enforce a policy that will remove a PC from the corporate network if the anti-virus software is not running.

The administrator wants to:

- Subscribe to the vPro device for event alert notification.
- Define a System Defense policy to isolate the vPro device in the event of OOBM agent failure and set this policy as the Agent Presence policy.
- Create the watchdog and specify its actions.
- Deploy the Agent Presence policy and watchdog to the vPro device.
- Manage OOBM agent settings and deploy the settings to the vPro device.
- Install the OOBM agent on the vPro host operating system (the OOBM agent is started automatically by the installer.
- Restart the security process after the event alert is sent.

After the OOBM agent is installed and started on the vPro device, it registers with the watchdog and starts to send it heartbeats at defined intervals. On agent failure, the agent stops sending heartbeats to the watchdog. The watchdog raises an event and enables the deployed Agent Presence policy. The Agent Presence policy becomes the active policy based on its higher priority. After the policy is activated, the vPro device inspects packets and performs the actions specified by the filters associated with the Agent Presence policy. The administrator performs the remediation task of restarting the security software that the OOBM agent was monitoring. After the security software is restarted, the OOBM agent registers again and starts to send heartbeats to the watchdog. The watchdog disables the Agent Presence policy and the enabled System Defense policy with the higher priority becomes the next active policy.

Use Case Steps

Complete the following tasks to implement this scenario:

- "View the vPro Event Filter" on next page
- "Subscribe for Event Alert Notifications" on next page
- "Create a Filter for the Agent Presence Policy" on next page
- "Create the Agent Presence Policy" on page 135
- "Set and Deploy the Agent Presence Policy" on page 135
- "Create the Watchdog" on page 136

- "Deploy the Watchdog" on page 137
- "Configure the System Message and Software List" on page 137
- "Deploy the System Message and Software List" on page 137
- "Install and Start the OOBM Agent" on page 138
- "Activate the Agent Presence Policy" on page 139
- "Send the Alert" on page 139
- "View Alerts" on page 139
- "Restart the Security Process" on page 139
- "Deactivate the Agent Presence Policy" on page 139

View the vPro Event Filter

To view the Event Filter for the vPro device, complete the following steps:

1. On the **Operations** tab under **Out of Band Management** in the left navigation menu, click **Device Management**. The Device Management window opens.
2. Click the hostname link for the vPro device whose Event Filter you want to review.
3. Click the **Event Filter** link under the **Diagnostics** section on the left-side of the window. The default event filters that exist on the selected vPro device are displayed in the content area of the console.
4. Click the name link of each event filter to determine which event filter will detect agent failure and send an alert to the management console.

For more information, see "Viewing vPro Event Filters" on page 90.

Subscribe for Event Alert Notifications

To subscribe to vPro devices for event alert notifications, follow the steps in the "Subscribe for Event Alert Notifications" on page 125 in use case "Hardware Failure and Replacement" on page 124.

Create a Filter for the Agent Presence Policy

To create a filter for the Agent Presence policy, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Filters**. The Filters window opens.
2. Click the ✚ add icon on the toolbar. The System Defense Filters wizard opens.
3. Click Next to continue. The Filter Details window opens. In this window, specify the following:
    - **Filter Name**: Enter **PreventInfection**.
    - **Filter Type**: Select **Drop**.
    - **Create Event on Filter Match**: Select **Yes**.

4. Click **Next**. The Parameters window opens. In this window, specify the following:
   - **Packet Type**: Select **TCP**.
   - **Filter Mode or Direction**: Select **Receive**.
   - **Network Address**: Select **Filter Packets from Network**.
   - **Port Range**: Select **Destination Port Range**. Enter `1` and `655535` for the **Min Port** and **Max Port** values. This refers to the ports on the vPro device. You want to block packets to all destination ports on this vPro device from all source ports on all of the devices in the network to prevent infection on the vPro device.
5. Click **Next** and **Close**.

For more information, see "Managing System Defense Filters" on page 55.

Create the Agent Presence Policy

To create the Agent Presence policy, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Policies**. The Policies window opens.
2. Click the add icon on the toolbar. The System Defense Policy wizard opens.
3. Click Next to continue. The Policy Details window opens. In this window, specify the following:
   - **Policy Name**: Enter **PreventInfection**.
   - **Priority**: Enter **99**.
   - **Enable Anti Spoofing Filter**: Select **Yes**.
   - **Default Receive (Rx) Filter Type**: Select **Pass**.
   - **Default Transmit (Tx) Filter Type**: Select **Pass**.
4. Click **Next** to see all available filters.
5. Drag the PreventInfection filter to the **Filters to assign to policy** list.
6. Click **Add Policy**.

For more information, see "Managing System Defense Policies" on page 59.

Set and Deploy the Agent Presence Policy

To set and deploy the Agent Presence policy to the vPro device, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Policies**. The Policies window opens.
2. Check the box next to the PreventInfection policy.
3. Click the deploy icon on the toolbar The Policy Deployment Wizard opens.
4. Click **Next** to continue. The Select Devices window opens.
5. Check the box next to the vPro device that will be running the OOBM agent.

6. Click **Next**. The Set Policies window opens.
7. Select the **PreventInfection** policy as the Agent Presence Policy for the wired NIC. This sets the PreventInfection policy as the Agent Presence policy for the vPro device. This policy will be enabled by the watchdog if the OOBM agent stops sending heartbeats to the watchdog. Since you specified, the highest priority (99) when you created the policy, it will become the active policy if enabled by the watchdog.
8. Follow the remaining steps in the wizard.

For more information, see "Managing System Defense Policies" on page 59.

Create the Watchdog

To create the watchdog, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Watchdogs**. The Watchdogs window opens.
2. Click the ➕ add icon to create an watchdog. The Watchdog wizard opens.
3. Click **Next** to continue. In this window, specify the following:
   - **Agent Type**: Select **OOBM agent**.
   - **Name**: Enter **AlphaWatchdog**.
   - **Agent GUID**: This field is grayed out for the OOBM agent because the GUID for the OOBM agent is known.
   - **Heart Beat Interval**: Accept the default value provided.
   - **Startup Interval**: Accept the default value provided.
4. Click **Next**. The Watchdog Actions page of the wizard opens. In this window, specify the following:
   - **Transition States:**
     From: Select **Agent Running**.
     To: Select Agent **Stopped**.
   - **Actions**:
     For **Agent Presence**, select **Enable** to specify that you want the Agent Presence policy enabled if the specified agent transition occurs.
     For **Event Creation**, select **Enable** to specify that you want an event to be raised if the specified agent transition occurs.
5. Click **Add Action**. The action is added to the actions table at the bottom of the window.
6. Add actions for another transition state. Now in this window, specify the following:
   - **Transition States:**
     From: Select **Agent Stopped**.
     To: Select **Agent Running**.
   - **Actions**:
     For **Agent Presence**, select **Disable** to specify that you want the Agent Presence policy disabled if the specified agent transition occurs.

For **Event Creation**, select **Enable** to specify that you want an event to be raised if the specified agent transition occurs.

7. Click **Add Action**. The action is added to the actions table at the bottom of the window.
8. Follow the remaining steps in the wizard.

For more information, see "Managing Watchdogs" on page 67.

Deploy the Watchdog

To deploy the watchdog to the vPro device, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Watchdogs**. The Watchdogs window opens.
2. Select the check box next to AlphaWatchdog.
3. Click the deploy watchdog icon on the toolbar. The Watchdog Deployment Wizard opens.
4. Click **Next** to continue. The Select Devices window opens.
5. Select the check box next to the vPro device that will be running the OOBM agent.
6. Follow the remaining steps in the wizard.

For more information, see "Managing Watchdogs" on page 67.

Configure the System Message and Software List

To configure the system message and software list, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Watchdogs**. The Watchdogs window opens.
2. Click the OOBM agent settings icon. The Software List Dialog opens.
3. Accept the default message provided in the **System Message** text box.
4. In the **Software Name** box, enter **symantec.exe**.
5. Click **Add**. You can repeat this process to create a list of software applications that you want the OOBM agent to monitor.
6. Click **Save**. An information message is displayed to the screen.
7. Click **Close** to exit the dialog. The system message and agent software list are stored in the XML repository.

For more information, see "Configuring the System Message and Software List" on page 71.

Deploy the System Message and Software List

To deploy the system message and software list, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Watchdogs**. The Watchdogs window opens.

2. Click the deploy software list and system message icon. The Software Deployment Wizard opens.
3. Click **Next**. The Software Titles window opens.
4. Select the **symantec.exe** software application.
5. Click **Next**. The Devices window opens.
6. Select the check box next to the vPro device that will be running the OOBM agent.
7. Click **Next** and follow the remaining steps of the wizard.

For more information, see "Deploying the System Message and Software List" on page 71.

Install and Start the OOBM Agent

To install and start the OOBM agent on the vPro device, complete the following steps:

1. Copy the `oobmclocalagent.msi` file located in the `Media\oobm\win32\LocalAgent` directory on the RCA Core distribution media to the vPro device. Double-click the file. Alternatively, you can also copy the `setup.cmd` file located in the same directory on the distribution media to the vPro device. Double-click the setup file or type `setup.cmd` on the command line. The `setup.cmd` file calls the `oobmclocalagent.msi` file.
2. Click **Next** and accept the license agreement.
3. Click **Next.** The Remote Configuration Parameters window opens. In this window, specify the following:
   - **SCS Configuration Client User Name**: Enter the user name of the user with the role of configuration client. In our example, it is SCSUser@vlan1.hp.com.
   - **SCS Configuration Client Password:** Enter the password for the SCSUser. For more information about this role, see "Configuration Client Role" on page 31.
   - **SCS Profile ID**: Enter the profile ID for the vPro device. You can find this information in the Profiles area of the SCS Console.
   - **SCS Remote Configuration URL**: Enter the URL path including the virtual directory for the Intel Setup and Configuration Service (SCS) web services. In our example it is https://provisionserver. vlan1.hp.com /amtscs_rcfg, where provisionserver.vlan1.hp.com is the fully qualified domain name (FQDN) of the IIS host machine and amtscs_rcfg is the SCS web services virtual directory on the host machine.
4. Click **Next**. The User Information window opens, which enables you to enter the vPro administrator credentials. In this window, specify the following:
   - **User Name**: Enter the vPro username of the administrator.
   - **Password**: Enter the vPro password of the administrator.
   - Do not select the **TLS Mode** check box since in this use case, the vPro device is not provisioned in TLS mode.
5. Click **Next** and follow the remaining steps in the install wizard.

For more information, see "Installing the OOBM Agent" on page 31.

The RCA Out of Band Management service starts as soon as the OOBM agent is installed.

> **Note:** All of the applications on the software list that the OOBM agent will monitor must be runnng when the OOBM agent starts. If not, the OOBM agent will shut down the watchdog as soon as it starts.

Activate the Agent Presence Policy

To activate the Agent Presence policy on the vPro device, complete the following steps:

The watchdog automatically enables the Agent Presence policy because you specified this action for the running to stopped transition state when you created the watchdog.

Also, since you defined the priority of the Agent Presence policy at 99 when you created the System Defense policy and set it as the Agent Presence policy, it has a higher priority than the current active System Defense policy and thus automatically becomes the new active policy.

Send the Alert

The watchdog automatically raises an event because you specified this action for the running to stopped transition state when you created the watchdog.

The default event filter for this type of event specifies to both log an event and send an alert, the event alert will automatically be sent to the management console if you have subscribed to the vPro device.

And finally, since you did subscribe to the vPro device running the OOBM agent for event alert notification, the Event Filter now has a known destination for the alert so that it can be sent to the management console.

View Alerts

To view alerts, follow the steps in "View Alerts" on page 125 in use case "Hardware Failure and Replacement" on page 124. In this case, you are looking for event alerts caused by OOBM agent failure.

Restart the Security Process

To restart the security process, enter the command line or double-click the executable file that invokes the security application.

Deactivate the Agent Presence Policy

After the OOBM agent starts sending heartbeats again to the watchdog, the watchdog automatically disables the Agent Presence policy based on its defined actions for the stopped to running transition state, and the enabled System Defense policy with the higher priority becomes the new active policy.

Worm Infection and Containment

This use case is divided into the following sections:

- "Overview" below
- "Use Case Steps" below

Overview

Although firewalls and intrusion detection systems are already in place on the network, the administrator is aware of the fact that these mechanisms are useful only against known worms and are not effective against zero-day worm outbreaks. A heuristics worm-containment system is required to protect the network from such outbreaks.

The administrator wants to:

- Subscribe to vPro devices for event alert notification.
- Create a heuristics specification defining the threshold (packet count) and window size (time) values that will trigger containment actions.
- Specify the actions to be taken if the Heuristics Rules engine residing on the vPro chip detects network traffic that may indicate worm infestation based on the threshold and window size values.
- Specify the time-out value for the containment actions taken to stay in affect.
- Deploy the heuristics specification to the vulnerable vPro devices.
- Perform the necessary remediation tasks after being alerted of a possible outbreak.

When the heuristics information is deployed to the vPro device, the Heuristics Rules engine counts packets and updates counters. If the heuristics criteria are matched, the engine triggers the actions that the administrator specified. In this use case, it will raise an event and block outbound traffic on the offending port. The criteria match always causes the Event Manager residing on the vPro chip to raise an event. (In this use case, we are assuming that the Event Filters on the vPro devices have an entry for this type of event where event alerting is enabled.

After the machine is isolated from the network, the administrator performs the remediation tasks required to restore the vPro device. The heuristics actions will stay in effect for the length of time specified in the time-out value. When that time has elapsed, the actions will be lifted and the Heuristics Rules engine will resume inspecting traffic flow.

Use Case Steps

Complete the following tasks to implement this scenario:

- "Subscribe for Event Alert Notifications" below
- "Create an Heuristics Specification" on next page
- "Deploy the Heuristics Specification" on next page
- "View Alerts" on page 142

Subscribe for Event Alert Notifications

To subscribe to vPro devices for event alert notifications, follow the steps in the section "Subscribe for Event Alert Notifications" on page 125 in use case "Hardware Failure and Replacement" on page 124.

Create an Heuristics Specification

To create an heuristics specification, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Heuristics**. The Heuristics window opens.
2. Click the add icon to create new heuristics information. The Heuristics wizard opens.
3. Click **Next** to continue. The Heuristics Details window opens. In this window, specify the following:
   - **Settings Type: Select Default.**
   - **Parameters**
     - **Name**: Enter Zero_Worm.
     - **Fast Packet Count**: Accept the default value of 8.
     - **Fast Time Count**: Accept the default value of 10.
     - **Slow Packet Count**: Accept the default value of 64
     - **Slow Time Count**: Accept the default value of 50 seconds (50000 milliseconds).
     - **Encounter Timeout**: Enter 50 seconds.
     - For more details, see "Window Size and Threshold Values" on page 153 and "Containment Actions and Timeout Values" on page 154.
   - **Actions**
     - **Block TX Traffic**: Select **Offensive Port Only** from the pull-down list.
   - **Policy**
     - **Policy Name**: Do not select a policy name from the pull-down list since we do not want to enable a System Defense filter if the heuristics conditions are met.
4. Click **Next**. The status of the operation is displayed.
5. Click **Close** to exit the wizard. The new heuristics information is displayed in the Heuristics table, and it is added to the repository.

For more information, see "Managing Heuristics Information" on page 63.

Deploy the Heuristics Specification

To deploy the heuristics specification, complete the following steps:

1. On the **Configuration** tab under **Out of Band Management** > **vPro System Defense Settings** in the left navigation menu, click **Heuristics**. The Heuristics window opens.
2. Check the box next to the Zero_Worm heuristics specification.
3. Click the deploy heuristics icon on the toolbar. The Heuristics Wizard opens.
4. Click **Next** to continue. The Select Devices window opens.
5. Check the box next to each device to which you want to deploy the heuristics information.

6. Click **Next**. The Heuristics Setting window opens.
7. Select the Zero_Worm heuristics specification for both the wired and wireless network interfaces on the selected devices.
8. Click **Next**. The Confirmation Summary window opens. Review the information in this window.
9. Click **Next** to continue with the deployment process. The Result window opens displaying the results of the operation.
10. Click **Close** to exit the wizard.

For more information, see "Managing Heuristics Information" on page 63.

View Alerts

To view alerts, follow the steps in "View Alerts" on page 125 in use case "Hardware Failure and Replacement" on page 124. In this case, you are looking for event alerts caused by the Heuristics Rules engine.

Appendix A

OOBM Features

You can perform Discover, Heal, and Protect operations (based on device type) on the provisioned devices in your network through the Out of Band Management (OOBM) options in RCA console.

The following sections describe in detail the OOBM features that enable you to "Discover" below, "Heal" on next page, and "Protect" on page 147 the OOB devices on your network.

> **Note:** Protect feature is relevant to vPro devices only.

Discover

You can discover the "Hardware Assets" below and "Software Assets" below on all of the provisioned OOB devices on your network.

Hardware Assets

Intel vPro devices store hardware asset information in flash memory. DASH devices store this information in the network controller's NVRAM. Both can be read anytime even if the device is powered off. The only conditions are that the devices are physically connected to the network and that they are plugged into a power source. The OOB devices do not rely on software agents to prevent accidental data loss. You can use the RCA Console to access this information and use it to:

- Determine the exact specifications for any hardware component on the device that may need to be replaced.
- Identify compatibility issues.
- Inspect the configuration of a device before provisioning a new operating system.
- Retrieve ad-hoc inventory information even when the machine is powered off.

Software Assets

Intel vPro enables you to view a list of applications that have registered themselves with the third party data storage (3PDS) on the vPro device. For HP applications that have registered with the 3PDS, you can also view the data that the applications have written to the scratch pad area of the vPro device. DASH devices store software asset information in the network controller's NVRAM. You can use the RCA Console to access this information and use it to:

- Determine if there are applications installed on the device that are taking advantage of vPro or DASH. The exact use of data storage is specific to the application.
- Retrieve out of band information for vPro and DASH-aware HP applications.

- Confirm that vPro and DASH-aware applications are correctly registered. This can help with troubleshooting certain applications.
- Confirm that vPro and DASH-aware HP applications are working correctly.
- View the software list of applications that you want the OOBM agent running on the vPro device to monitor.
- View the system message that the OOBM agent will display to the console of the vPro device if the Agent Presence policy is activated.

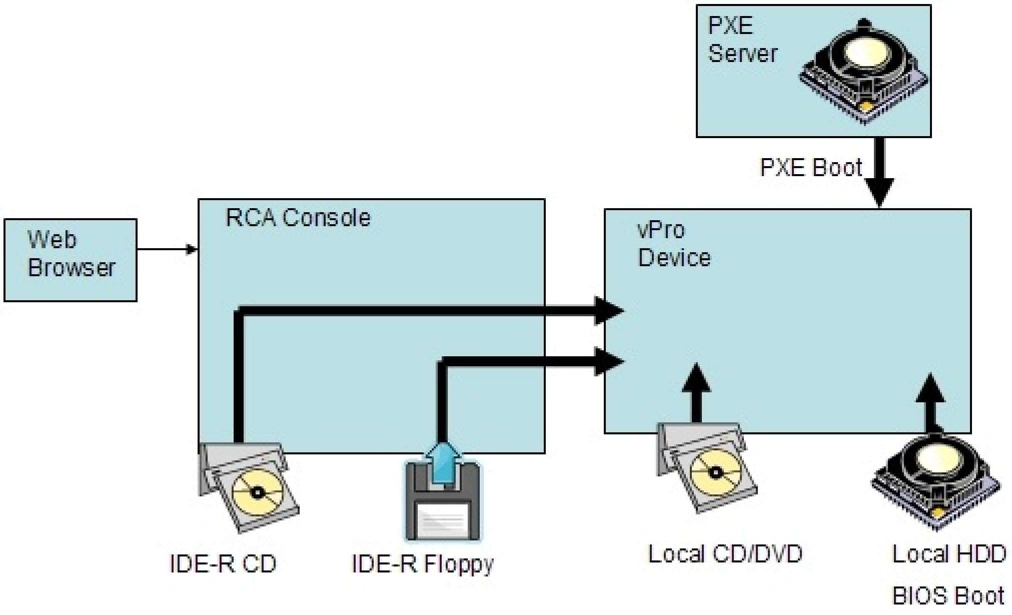
Heal

Heal operations include "Remote Operations" below and "Event Management" on next page.

Note: Event Management is relevant to vPro devices only.

The following figure illustrates the various remote management operations that can be performed through the OOBM options in the RCA Console (IDE-R pertains to vPro only).

Overview of Remote Management Operations



Remote Operations

Intel vPro and DASH devices provide out of band access to remotely diagnose and repair devices after software, operating system, and hardware failures. Through the RCA Console, you can remotely view the power state of a device, reboot from its hard disk, reboot from an image on its local CD/DVD, reboot from a remote CD or floppy drive, reboot from a PXE server, and reboot to BIOS setup. The power state of the system is changed when any remote operation is performed or the system is in an idle state.

You can use these capabilities to perform remote power management operations, which include:

- Powering devices up and down
- Restarting OOB devices using console text redirection and IDE-R

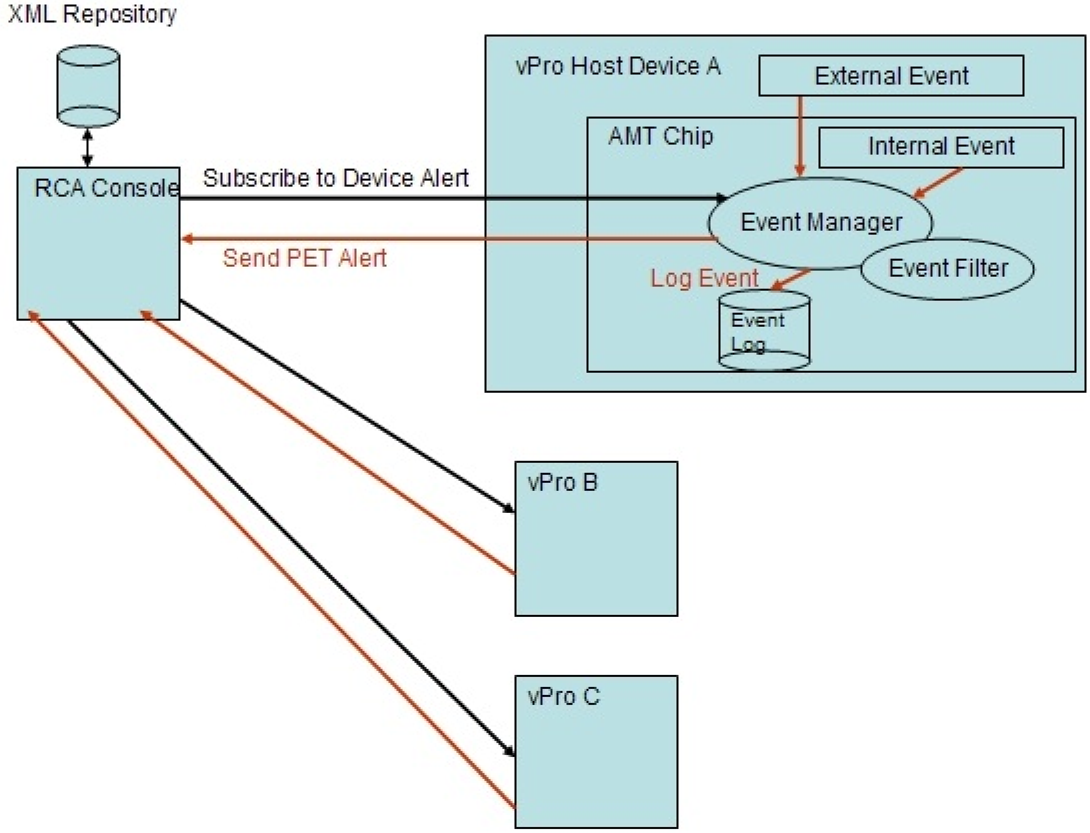
Note: Integrated drive electronic redirect (IDE-R) is available on vPro devices only.

Power management operations enable you to restore problematic OOB devices to a sane state.

Event Management

The following figure illustrates the dynamics involved in event management on vPro systems.

Event Management Overview



Intel vPro provides for alerting and event logging to assist you in diagnosing problems quickly to reduce end-user downtime. Events are created from external sources such as the System Management (SM) bus and hardware sensors. There are also internal, vPro-self created events. There are several sources for these internal events. They include events triggered by System Defense filters, by Agent Presence failure, firmware updates, and several other scenarios. So an event can be a physical occurrence, such as a fan failure or a filter-detected occurrence (due to a change in traffic pattern), such as a virus attack. If an event occurs on the system, the Event Manager residing on the vPro chip raises an event and looks in the Event Filter to determine what actions to take. The Event Filter defines a set of criteria that is applied to each incoming platform event. If the incoming event matches the criteria, the Event Filter specifies the actions to take. These actions can include sending an alert to the RCA Console, logging the event in the vPro log, or both.

You must subscribe to a vPro device for event alerts created by that device to be sent to the RCA Console. The subscription provides a destination in the Event Filter for an event alert. You can subscribe or cancel event alerting to determine what device alerts you want displayed to the RCA Console.

Intel vPro devices come with a set of default event filters built in to their firmware chip. The RCA Console also enables you to view the events in the event log for a specific vPro device to determine the type, severity, date, and description of each logged event.

You can use this capability to control event alerting and logging. The alerts sent to the console and the events written to the event log enable you to determine if heal or protect actions are required for a specific device.

Protect

You can protect the vPro devices on your network from malicious software attacks and worm proliferation. Intel vPro provides this capability through packet filtering and by monitoring the presence of critical OOBM agents running on the devices in your network. It also enables you to quarantine worm-infected devices by providing a mechanism that continuously observes outgoing traffic to detect and impede the proliferation of worms.

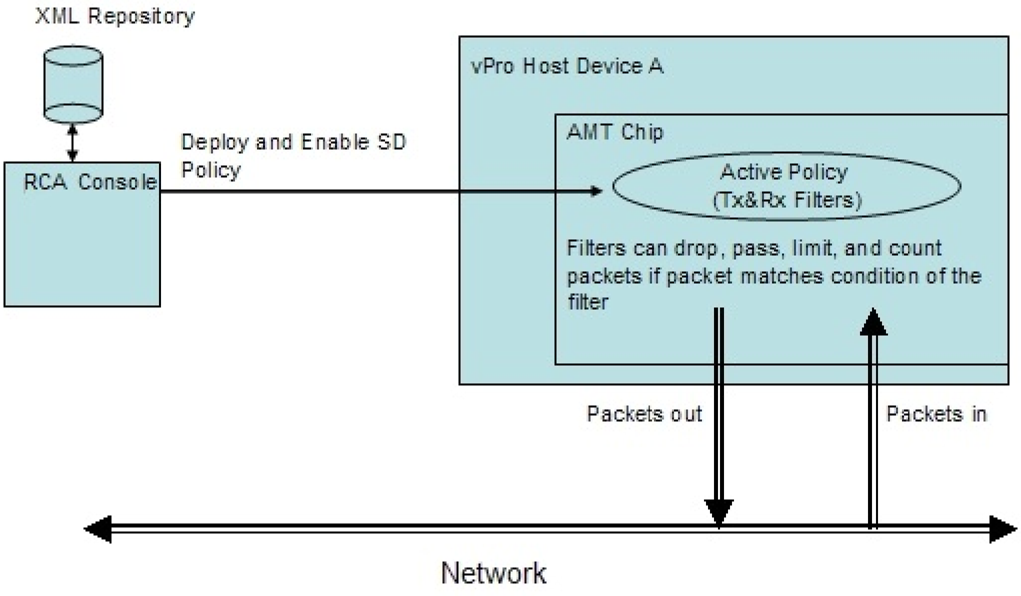
These topics are discussed in the following sections:

- "System Defense" below
- "Agent Presence" on page 150
- "Network Outbreak Containment Heuristics" on page 151

System Defense

The following figure illustrates an overview of how System Defense works by using policies and filters that monitor packets that are transmitted or received by vPro devices.

System Defense Overview


XML Repository
RCA Console
Deploy and Enable SD Policy
vPro Host Device A
AMT Chip
Active Policy (Tx&Rx Filters)
Filters can drop, pass, limit, and count packets if packet matches condition of the filter
Packets out
Packets in
Network

Policies

The System Defense vPro capability enables the RCA Console to define and enforce network security policies. A System Defense policy contains a set of filters that are applied to incoming and outgoing network packets combined with actions to take when a packet matches (or does not match) the conditions in the filter. System Defense enables for selective network isolation of Ethernet and IP protocol flows based on the filters associated with a policy. These filters enable the Management Console to pass, limit, or block specific IP-based network flows and to keep traffic counts or log the occurrence of these flows.

The RCA Console stores these filters and policies in its XML repository. The console can then deploy the System Defense policies to multiple vPro devices where they reside in the firmware of the devices.

After you have deployed policies to a vPro device, you can use the RCA Console to enable a policy on that device to become the default System Defense policy. You can also set a policy as the Agent Presence policy that can be enabled by an watchdog action. This is discussed in greater detail in "Agent Presence" on page 150. The enabled policy with the higher priority becomes the active policy for the device. After a policy is activated, the vPro device inspects each incoming and outgoing packet and performs the necessary actions specified by the filters associated with the policy. If a vPro device has more than one network interface card (NIC), that is, wired and wireless, you can enable a System Defense policy and set an Agent Presence policy for each NIC.

Filters

Filters can perform the following actions if the conditions associated with the filter are matched:

- Pass packets
- Discard packets

- Limit packets
- Count packets to collect statistical data

In addition to performing the packet-related actions, a filter can also cause an event to be raised.

There are two filter modes. They are the following:

- **Transmit**: Filters in this mode are applied to packets transmitted from the vPro device to the network. Such filters can be used to block all traffic from a device suspected of being infected preventing it from infecting other devices on the network. The default filter in transmit mode catches all the transmit packets that do not match any of the other policy transmit filters. Filters in this mode can be of the pass, limit, statistical, or drop type.
- **Receive**: Filters in this mode are applied to packets received from the network to the vPro device. Such filters can be used to block all packets received by the device after boot until a OOBM agent starts such as an antivirus agent. The default filter in receive mode catches all the receive packets that do not match any of the other policy receive filters. Filters in this mode can be either of the pass or drop type.

There are several filter types. They are the following:

- **Default Else**: This is the default Else filter for both the Receive and Transmit directional modes. It is used for catching all packets that do not match the condition of any of the policy filters. If the Else filter is matched (that is the packets do not match the conditions of any other filter), a filter action can be created.
- **Drop**: This is the drop filter for both the Receive and Transmit directional modes. It discards all packets matching the conditions of the filter.
- **Pass**: This is the pass filter for both the Receive and Transmit directional modes. It passes all packets matching the conditions of the filter.
- **Statistical Drop/Pass**: This is the statistical filter for both the Receive and Transmit directional modes. They count the number of packets that match the conditions of the filter. They are used for collecting statistical data. They can either pass or discard packets based on whether they are statistical pass or statistical drop filters.
- **Rate Limit**: This is the rate limit filter for both the Receive and Transmit directional modes. They limit the number of specific types of packets per second that are received or transmitted matching the conditions of the filter. This filter has a threshold and when the threshold is reached, it cuts off any additional traffic.

In addition to filter types, Transmit filters can have anti spoofing enabled. When this property is enabled, all outgoing packets are checked and the source IP is compared to the network interface IP address. If the IP addresses do not match, the packets are dropped. If this filter is enabled, it prevents a host from falsifying its identity by sending IP packets with a source IP address that is different from its assigned IP address.

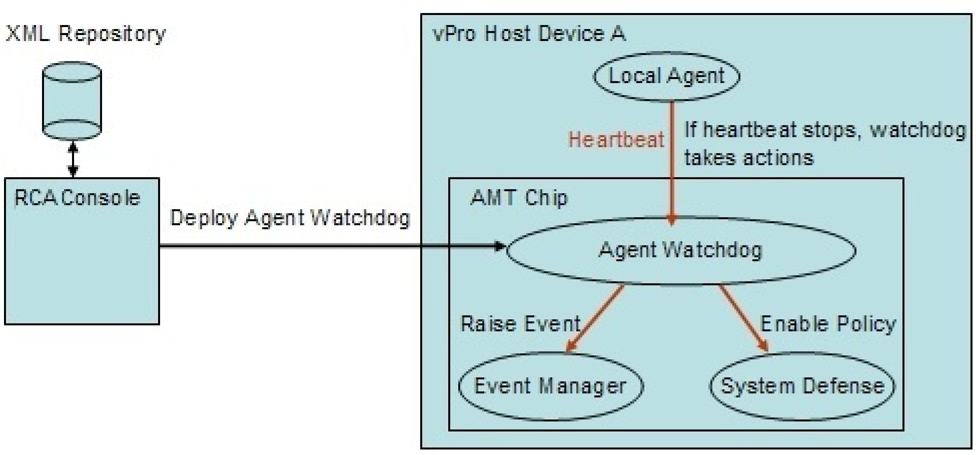
Intel vPro supports 32 filters in Receive (Rx) mode and 32 filters in Transmit (Tx) mode. One each of the filters in 32 Tx and Rx modes is used as the Else (non-matching) filter. If anti spoofing is enabled, it utilizes one of the filters in Tx mode. This reduces the available filters for a vPro device to 31 in-bound and 30 out-bound.

> **Note:** If this limit is reached, you cannot deploy additional policies containing filters to the vPro device until you delete some of the existing filters on that device.

Agent Presence

The following figure illustrates the components involved when monitoring for the presence of a OOBM agent on a vPro host device.

Agent Presence Overview



The Agent Presence capability enables the RCA Console to create an watchdog to monitor the state of a OOBM agent running on the host CPU of the vPro device. The OOBM agent is typically software that secures the vPro device by monitoring security applications related to anti-virus or firewall protection. After the OOBM agent starts, it sends heartbeats to the watchdog at regular intervals. If the heartbeat stops, the watchdog will take actions to protect the device.

OOBM Agents

As indicated, the OOBM agent secures the vPro device by monitoring the state of any critical applications running on the device. The list of applications that the OOBM agent monitors is user-defined. If a monitored application stops running, the OOBM agent stops sending a heartbeat to the watchdog. If the watchdog enables the Agent Presence policy and it becomes the active policy, a system message is displayed to the console on the vPro device. The system message is also user-defined although a default message is provided. The application list and system message are stored in the 3PDS of the vPro device.

When the OOBM agent is installed (and the software list of applications has been created and deployed to the device), it is automatically started as an NT service. After the OOBM agent starts, it does the following:

1. Registers with the watchdog.
2. Gets the heartbeat interval from the vPro chip and starts sending heartbeats to the watchdog.

3. Reads the 3PDS to get the list of applications to monitor and starts monitoring the applications. The same heartbeat interval is used for monitoring the applications list.
4. Stops sending the heartbeat, if an application on the application list stops running.
5. Shuts down the watchdog and displays the user-defined system message that it reads from the 3PDS.

Watchdogs

The actions an watchdog can perform are as follows:

- Enable the Agent Presence policy if it has been set. If it has a higher priority than the default System Defense policy, it will become the active policy, and the filters associated with this policy will be activated to protect the network.
- Raise an event. Depending on what the Event Manager finds in the Event Filter, the event will be written to the event log on the vPro chip, and/or an event alert will be sent to the RCA Console if it has been subscribed to.

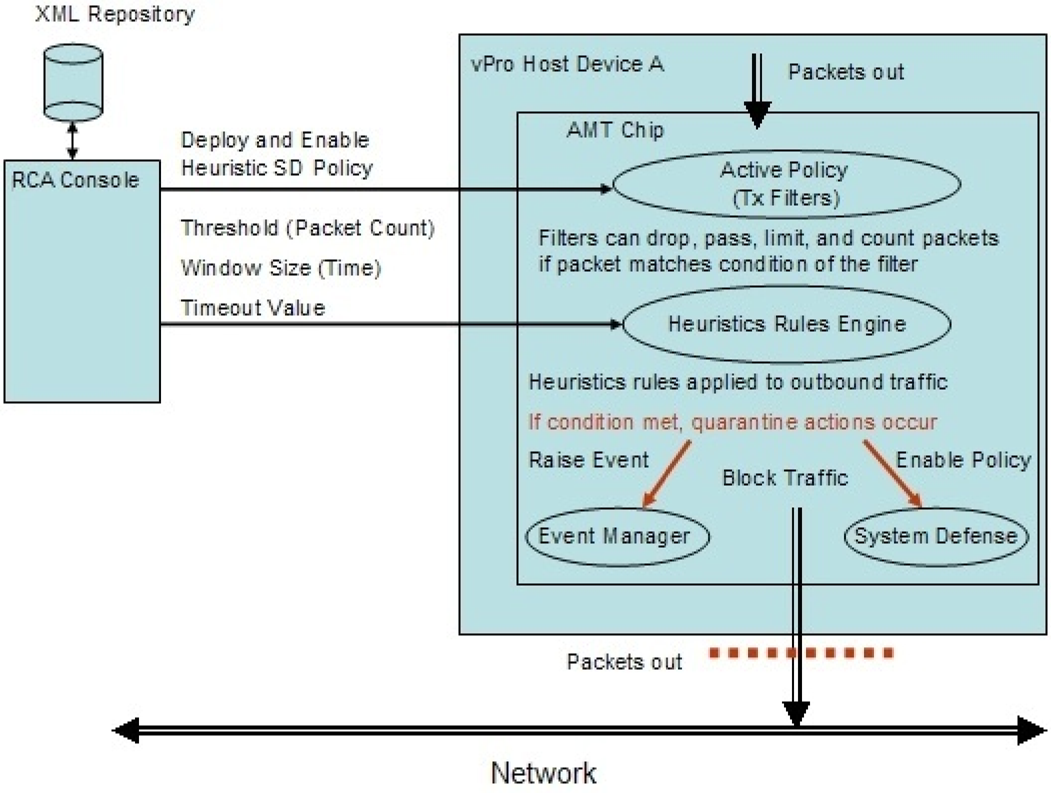
You can use the RCA Console to do the following:

- Create an watchdog.
- Specify timers to detect when the OOBM agent initializes and periodically transmits “heartbeat” signals to its watchdog.
- Specify transition states for the OOBM agent that will trigger the watchdog actions. Valid states include the following:
  - not started
  - stopped
  - running
  - expired
  - suspended
- Set the actions for the watchdog to take if the transition criteria are met (namely, enable Agent Presence policy and/or enable event logging).
- Deploy (and undeploy) the watchdog to multiple vPro devices.
- Create the list of applications to be monitored by the OOBM agent.
- Create the message that will be displayed on activation of the Agent Presence policy.

Network Outbreak Containment Heuristics

The following figure illustrates the architectural overview of a worm-containment system.

Worm-containment Architecture



The worm-containment heuristics mechanism provides additional value to a network even when there are firewalls and intrusion detection systems in place on that network. Firewalls and intrusion detection systems can be used effectively only against known worms, but they are not effective against zero-day worm outbreaks.

The vPro worm-containment system works by applying heuristic rules to the outbound traffic from the host vPro device. If the Heuristic Rules Engine detects an anomaly, the worm-containment system quarantines the host from the network. The Active Policy filters operate on the IP and TCP/UDP protocol header fields of the host traffic. As a result of this filtering, the vPro chip may take specific actions, such as, dropping the packets.

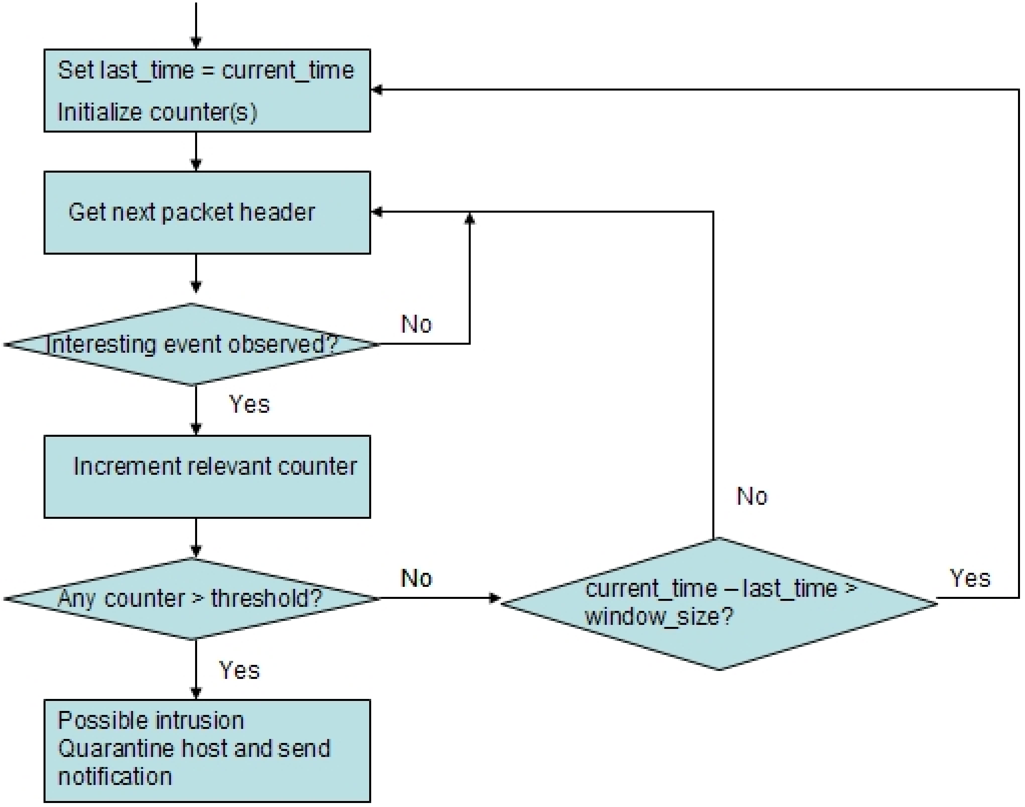
The Heuristics Rules Engine analyzes the traffic. If the Heuristics Rules Engine detects evidence of anomalous traffic, it can perform any of the following actions:

- Raise an event alert.
- Raise an event alert and block all outbound packets from the offending port.
- Raise an event alert and block all outbound packets from all ports.
- Raise an event and enable a vPro System Defense policy.

The worm-containment system relies on heuristic rules to detect traffic anomalies that could indicate scanning activity by a worm. The heuristic rules are based on the fundamental property of all self-propagating worms, namely, a worm has to contact new hosts to spread into the network. As a result, all heuristic rules identify events that suggest contact with a new host and monitor such events for anomalous patterns.

The following figure illustrates the basic mechanism employed by all heuristics.

Basic Operation of Heuristics


Set last_time = current_time
Initialize counter(s)
Get next packet header
Interesting event observed?
No
Yes
Increment relevant counter
No
Any counter > threshold?
No
current_time – last_time > window_size?
Yes
Yes
Possible intrusion
Quarantine host and send notification

For additional information, see the Intel study on a heuristics-based worm-containment system.

Window Size and Threshold Values

All heuristics examine packet headers and count the number of “interesting events” in a given time interval. As a result, all heuristics expose two configurable parameters, namely, a window size and a threshold. The window size (time count) indicates the period at which the heuristic resets its counters. The threshold (packet count) represents a limit value, which when exceeded by the counter, indicates an anomalous event.

The RCA Console enables you to configure these two parameters. When specifying these parameters, you must take into consideration two types of worms, which require different heuristic values. They are the fast spreading worm and the slow spreading worm. Different window sizes and threshold values should be used for the fast and slow spreading worms to successfully detect worm infections. Using a combined heuristic (different window sizes with appropriate threshold values) is more effective across a wider range of worms. The heuristic with the smaller window size is more effective for the fast worm, where the heuristic with the larger window size is effective for slower worms.

The configurable time window size ranges for fast and slow worms are the following:

- Fast: 10 milliseconds to one second (1000 milliseconds)
- Slow: one second (1000 milliseconds) to 50 seconds (50000 milliseconds)

The configurable threshold range for both heuristics is 8 to 64 packet count.

It is recommended the following configurations for window sizes and threshold combinations:

- Fast: 8 packets in 10 milliseconds
- Slow: 64 packets in 50 seconds

Containment Actions and Timeout Values

The RCA Console also enables you to specify the autonomous actions the system should take if the thresholds are exceeded. As indicated here, you can chose to raise an event only or raise an event in combination with blocking outbound host traffic or enabling a heuristics System Defense policy. The Heuristics Rules Engine is disabled after the action is taken.

You can specify how long the containment actions should be applied to the vPro device through the RCA Console. If you indicate a non-zero timeout value (greater than or equal to 20 seconds), the Heuristics Rules Engine stops scanning packets and applies the specified actions for that period of time. When the period of time has elapsed, the actions will automatically be removed and the chip will start scanning packets again. If you specify a zero timeout value, the Heuristics Rules Engine stops scanning packets and the actions are applied permanently. To remove the containment actions and start scanning packets again, you must manually trigger this to occur through the RCA Console.

Appendix B

Delayed Remote Configuration of the vPro Device

Delayed configuration is performed when the vPro device could not be provisioned within the Limited Network Access time interval that the network interface is opened after the device is connected to the network.

This section covers the following topics:

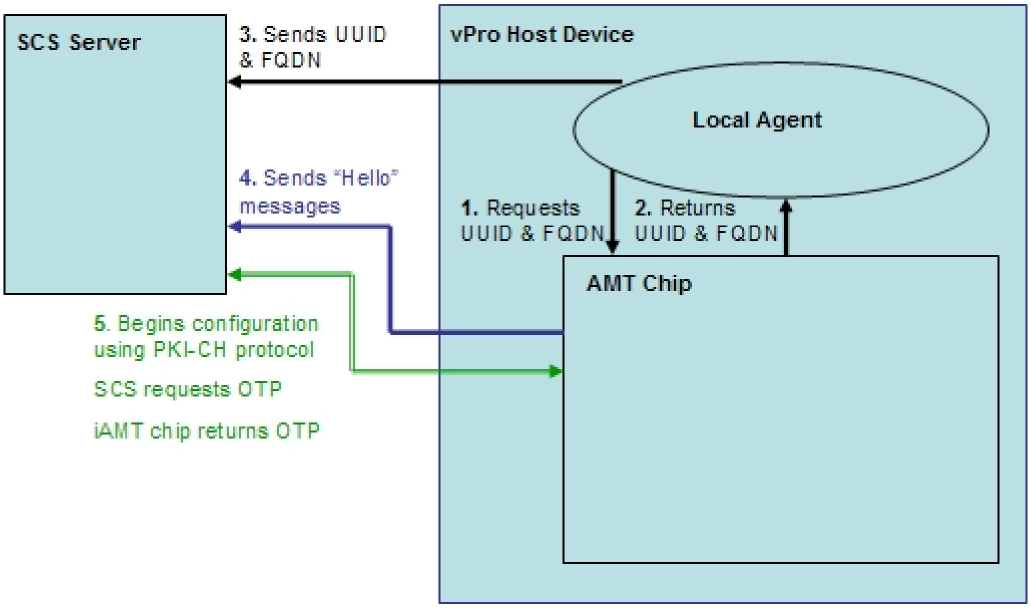
- "Transitioning to Setup Mode" below
- "Remote Configuration Provisioning Process " on next page
- "Delayed Remote Configuration through RCA Console" on page 158

Transitioning to Setup Mode

The following diagram shows the steps involved in transitioning the vPro device to Setup mode when using the OOBM agent for Remote Configuration. This is referred to as *delayed* configuration because the device was not provisioned immediately after being connected to the network. For an explanation of this alternative (immediate) configuration, see the section .

After the vPro device transitions to Setup mode, it starts sending “Hello” messages to the SCS Server indicating that it is ready to be provisioned.

Transitioning to Setup Mode in Delayed Configuration



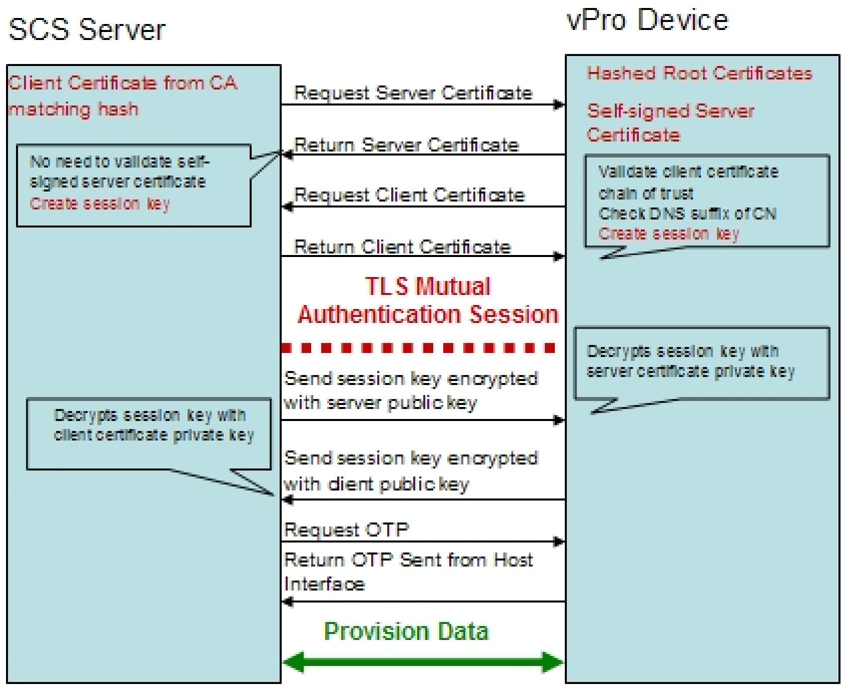
The OOBM agent must be installed on the vPro host device. The OOBM agent detects the vPro device and the following occurs:

1. The OOBM agent requests the UUID and FQDN from the vPro device.
2. The vPro device returns these values to the OOBM agent.
3. The OOBM agent sends these values to the SCS Server.
4. The vPro device starts sending “Hello” messages to the SCS Server.
5. The SCS Server starts the provisioning process using the PKI-CH protocol. The OTP is exchanged between the SCS Server and the vPro device.

Remote Configuration Provisioning Process

During the Remote Configuration provisioning process, a secure channel is created by using TLS mutual authentication. The following diagram illustrates the provisioning process flow.

Remote Configuration Provisioning Process


SCS Server
vPro Device
Client Certificate from CA matching hash
No need to validate self-signed server certificate
Create session key
Hashed Root Certificates
Self-signed Server Certificate
Validate client certificate chain of trust
Check DNS suffix of CN
Create session key
Request Server Certificate
Return Server Certificate
Request Client Certificate
Return Client Certificate
TLS Mutual Authentication Session
Decrypts session key with server certificate private key
Send session key encrypted with server public key
Decrypts session key with client certificate private key
Send session key encrypted with client public key
Request OTP
Return OTP Sent from Host Interface
Provision Data

The provisioning process includes the following steps:

1. The OOBM agent requests that the vPro device start the configuration process. The device opens its network interface for a limited period of time (24 hours on Intel machines and 255 hours on HP desktops) and starts sending “Hello” messages. The interface is opened for the specified hours the first time OOBM is enabled. If the time runs out before setup and configuration completes, any subsequent calls from the OOBM agent to start configuration opens the interface for only six hours.

2. The SCS Server does the following:
   - Extracts the root certificates hashes from the “Hello” message to know what client certificate to send the vPro device for validation.
   - Sends a certificate chain that includes a trusted root certificate matching one of the received hashes.
3. The vPro device does the following:
   - Validates the SCS client certificate. It checks that the OID or the OU is correct and that the certificate is derived from a CA that matches one of the root certificate hashes.
   - Verifies that the domain suffix matches the DNS suffix on the SCS certificate.
4. The SCS Server and the vPro device perform a complete mutual authentication session key exchange.
   - The vPro device uses a self-signed certificate, sending its public key.
   - The SCS creates a TLS session key, encrypts it with the vPro device public key, and sends it to the vPro device.
   - The vPro device decrypts the session key with its private key. The vPro device creates another session key and encrypts the session key with the client public key that the SCS Server sent to the vPro device for validation. The session key pair is used for the symmetric encryption of traffic during the setup and configuration TLS session.
5. One-time password (OTP) verification takes place between the SCS Server and the vPro device. The SCS server requests the OTP from the vPro device. The device sends the OTP securely, and the SCS Server checks it for correctness.
6. The setup and configuration process continues until the device is provisioned. Since the vPro device network interface is opened for a limited period after sending the first “Hello” message, the SCS Server can specify to the vPro device to extend this period by up to an additional 24 hours to complete the configuration process.

Delayed Remote Configuration through RCA Console

Through the RCA Console, you can provision vPro devices that were not provisioned during the initial Setup and Configuration Service (SCS) provisioning process.

The type of provisioning performed through the RCA Console is referred to as delayed Remote Configuration provisioning. It is considered *remote* configuration because you do not have to manually install a PID/PPS pair or enter information about the SCS server address, the domain name, and so on for each device to enable setup. Instead, this provisioning is done automatically and remotely from a management console. It is considered *delayed* configuration because the device was not provisioned in the time interval enabled for that device when it was initially connected to the network.

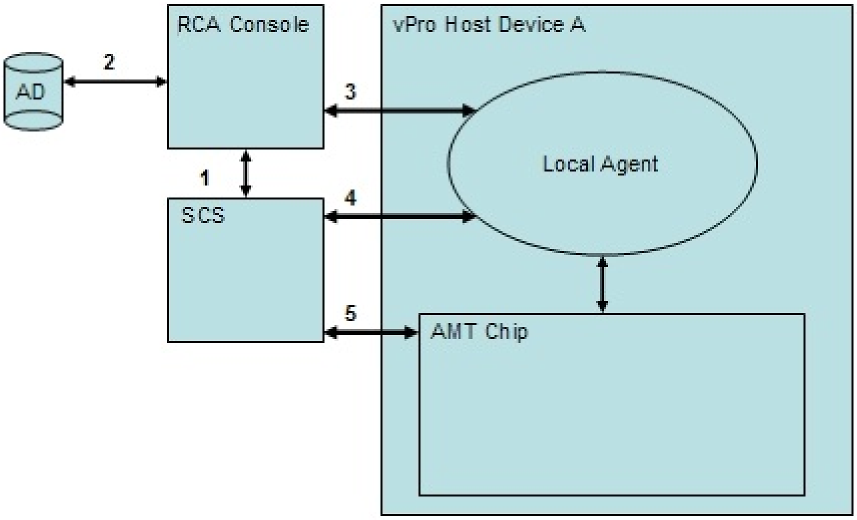
To use Remote Configuration, you must follow all of the requirements discussed in "Configuring the vPro Device Using Remote Configuration" on page 29.

> **Note:** You can use Remote Configuration to provision a vPro device only if the vPro device is in the un-provisioned or in-provisioning state. A vPro device, which has already been

provisioned, cannot be provisioned again using Remote Configuration. You must re-provision the vPro device manually.

To get the necessary information to provision the vPro devices, the RCA Console communicates with the OOBM agent running on the vPro device, the SCS server, and the Active Directory.

Delayed Remote Configuration through RCA Console



The communication exchange is the following:

1. RCA Console communicates with SCS to get a list of already provisioned devices and devices that are currently being provisioned.
2. RCA Console communicates with Active Directory (AD) to get a list of devices in that specific domain. The management console lists all of the devices with their respective provisioning state.
3. RCA Console tries to communicate with the OOBM agent on the default port. If the agent is installed, the devices are displayed with a status of unprovisioned in the RCA Console. After the communication is established with the OOBM agent, the RCA Console requests that the OOBM agent start the delayed configuration process.
4. If the device is not provisioned or in the in-provisioning state, the OOBM agent tries to contact SCS server to store the FQDN, UUID and Profile ID of the device. The hello packets are then created.
5. SCS server provisions the vPro device using the PKI-CH protocol.

Appendix C

Trusted Certificates

Trusted Certificates

A secure sockets layer (SSL) connection is secured by using the public key infrastructure (PKI). In PKI, certificates with asymmetric key pairs (public and private) are used to secure communications. The key pair is used to encrypt and decrypt data exchanged between clients and servers when they communicate with each other. The public key is shared and is used to encrypt data. The private key is kept private by the owner of the certificate and is used to decrypt data that was encrypted with the certificate's public key.

When using PKI in server authentication, the client uses the public key of the server certificate to encrypt messages, and the server uses its private key to decrypt messages. Conversely, in client authentication, the server uses the public key of the client certificate to encrypt messages, and the client uses its private key to decrypt messages.

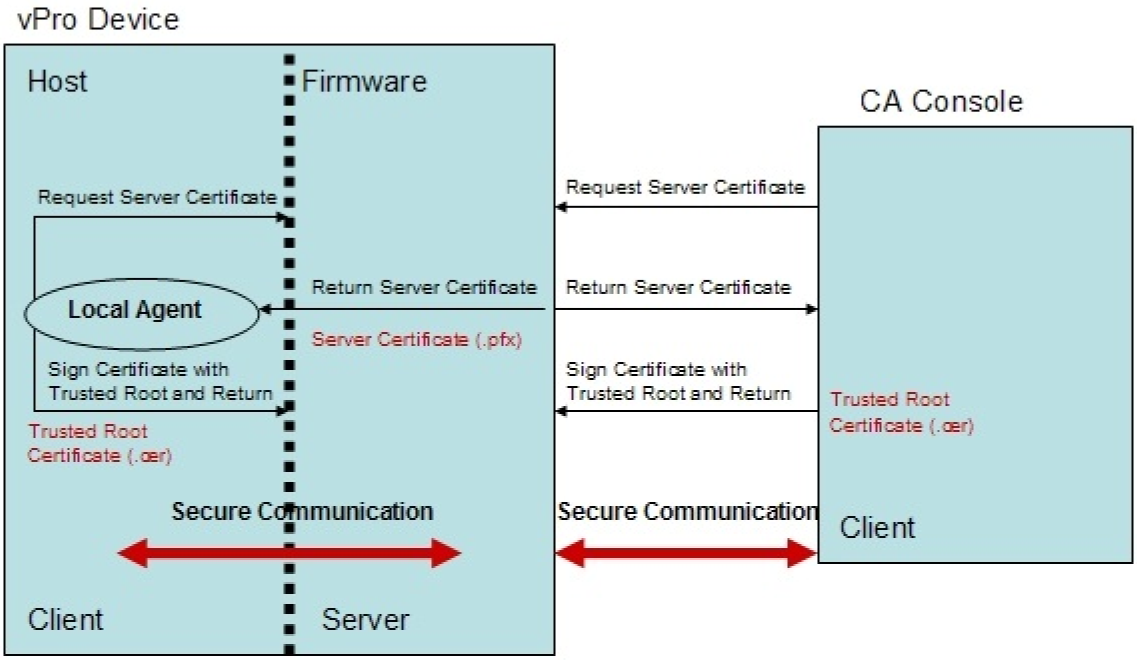
The Transport Layer Security (TLS) protocol has two kinds of authentication, "TLS Server Authentication" below (one way authentication and "TLS Mutual Authentication" on next page (two-way authentication). In the TLS protocol, the firmware on the vPro device is the SSL server. The RCA Console and/or the OOBM agent running on the host vPro device act as the client.

TLS Server Authentication

When establishing a TLS session in TLS server authentication, the client attempts to verify the validity of the SSL certificate it receives from the firmware on the vPro device. To perform this verification, the client must have the public key of the Certification Authority (CA) that signed the certificate. The public key is available in the trusted root certificate created by the same CA that created the server certificate. The trusted root certificate is already populated on all the vPro systems that are connected to the Active Directory of the domain. The client signs the certificate with the trusted root certificate verifying the identity of the server and sends it back to the server. This secures communications between the components acting as the client and the firmware on the vPro device when the client sends application data to the firmware.

In the following diagram, the OOBM agent running on the host device and the RCA Console are both clients to the vPro firmware. The functions of the OOBM agent are discussed in greater detail later in this chapter and throughout this guide.

TLS Server Authentication


vPro Device
Host
Firmware
CA Console
Request Server Certificate
Request Server Certificate
Local Agent
Return Server Certificate
Return Server Certificate
Server Certificate (.pfx)
Sign Certificate with Trusted Root and Return
Sign Certificate with Trusted Root and Return
Trusted Root Certificate (.cer)
Trusted Root Certificate (.cer)
Secure Communication
Secure Communication
Client
Client
Server

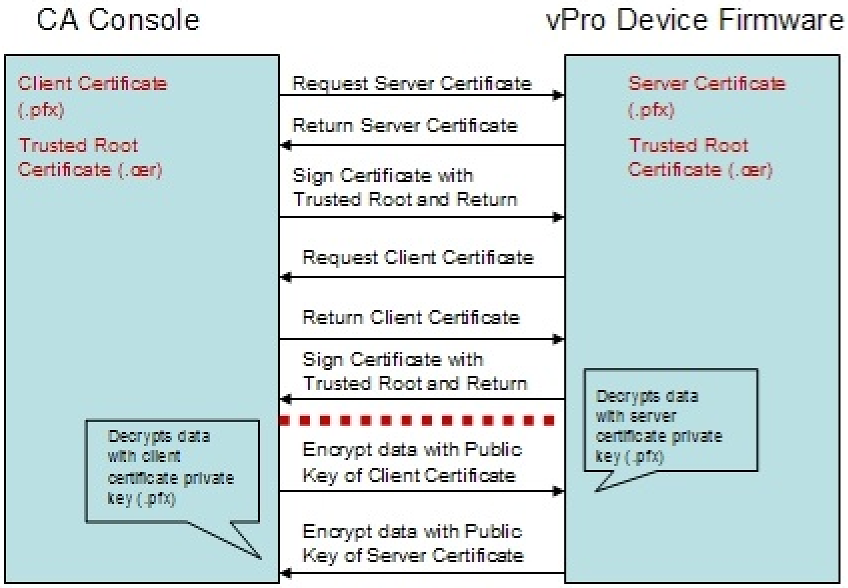
TLS Mutual Authentication

In addition to TLS server authentication where only one certificate is passed between the client and server, TLS mutual authentication provides greater security because two certificates are passed authenticating both ends of the communication. In mutual authentication, the client sends a certificate that must be signed by the server, as well as the server sending a certificate that is signed by the client. The public and private keys of the certificates are used for data encryption and decryption as described earlier.

Again in this model, the RCA Console and/or the OOBM agent act as the SSL client. The client must send its own SSL client certificate to the vPro device for client authentication, and the vPro device must have the trusted root certificate (public key) imported into its firmware to perform the verification (signing the client certificate).

When the RCA Console is the client, the trusted root certificate must also be imported into the trusted key store on the RCA Console machine. This enables the RCA Console to sign the server certificate that the vPro device sends it authenticating the server. The client certificate installed on the RCA Console must contain the complete certificate chain and the private key for the certificate. This feature provides mutual authentication for both the client and the server increasing the security level of TLS sessions. In the following diagram, the RCA Console is acting as the client to the vPro firmware.

TLS Mutual Authentication between RCA Console and vPro Device Firmware


CA Console
vPro Device Firmware
Client Certificate (.pfx)
Trusted Root Certificate (.cer)
Server Certificate (.pfx)
Trusted Root Certificate (.cer)
Request Server Certificate
Return Server Certificate
Sign Certificate with Trusted Root and Return
Request Client Certificate
Return Client Certificate
Sign Certificate with Trusted Root and Return
Encrypt data with Public Key of Client Certificate
Encrypt data with Public Key of Server Certificate
Decrypts data with client certificate private key (.pfx)
Decrypts data with server certificate private key (.pfx)

There are certain requirements when specifying vPro client certificates. They include the following:

- The certificate must contain the 1.3.6.1.5.5.7.3.2 OID, which marks it as a TLS certificate.
- The Enhanced Key Usage OID list field of the leaf certificate must contain the 2.16.840.1.113741.1.2.1 OID. This OID is used by the vPro device to authenticate the RCA Console.

You will use these values in the procedure for creating server and client certificate templates. To use the mutual authentication capability, the vPro device must have the root certificate that signed the SSL client certificate in its trust list. The root certificate is provided to the vPro device during the setup and configuration process. This is described in "Creating and Configuring the Profile" on page 27.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click here.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to radiadocfeedback@persistent.co.in.

Product name and version: Radia Client Automation Enterprise Out of Band Management, 9.00

Document title: User Guide

Feedback: