HP Client Automation

Out of Band Management

for the Windows® operating system

Software Version: 7.90

User Guide

Document Release Date: May 2010
Software Release Date: May 2010

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP 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 HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Intel®, Intel® Active Management Technology, and Intel® vPro™ Technology are U.S. registered trademarks of the Intel Corporation or its subsidiaries in the United States and other countries.

Java ™ is a registered trademark of Sun Microsystems, Inc.

Linux is a registered trademark of Linus Torvalds.

Microsoft®, Windows®, and Windows® XP are U.S. registered trademarks of Microsoft Corporation.

Microsoft Windows™ Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

PREBOOT EXECUTION ENVIRONMENT (PXE) SERVER
Copyright © 1996-1999 Intel Corporation.

TFTP SERVER
Copyright © 1983, 1993
The Regents of the University of California.

OpenLDAP
Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA.
Portions Copyright © 1992-1996 Regents of the University of Michigan.

OpenSSL License
Copyright © 1998-2001 The OpenSSLProject.

Original SSLeay License
Copyright © 1995-1998 Eric Young (eay@cryptsoft.com)

DHTML Calendar

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://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

The documentation for this product is available in the distribution media. The HP Client Automation software can be downloaded from **www.hp.com/go/clientautomation**.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

The following table indicates changes made to this document since the last released edition.

Document Changes

Chapter	Version	Changes
Chapter 3, Out of Band Management Configuration	7.80	Added configuration parameters for IDE-R/SOL time-out sessions in Configuring the IDE-R and SOL Time-out Values on page 48.
Chapter 3, Out of Band Management Configuration	7.80	Added configuration parameter for DASH text redirection time delay in Setting Configuration Parameters on page 50.
Chapter 8, Device Management	7.80	Added incremental vPro device discovery in Device Discovery on page 128.
Chapter 8, Device Management	7.80	Added Refreshing Device Information on page 131 to explain when SD columns are refreshed in the multi-device summary table.

Document Changes

Chapter	Version	Changes
Chapter 8, Device Management	7.80	Added more information for the DASH configuration boot settings in Configuring the Boot Settings on the DASH Device on page 161.
Chapter 11, Troubleshooting	7.80	Replaced domain name not validate item with Can not save SCS properties when managing vPro devices in device type selection window on page 175.
Chapter 8, Device Management	7.90	Added KVM Redirection functionality for vPro devices as discussed in KVM Redirection on vPro Devices on page 154.

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online 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 using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1 Introduction

The Out of Band Management (OOBM) features available in the HPCA Console allow you to perform out of band management operations regardless of system power or operating system state.

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

The HPCA Console supports Out of Band Management of Intel vPro devices and DASH-enabled devices.

Intel vPro 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.

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.

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 allows you to automatically provision remote vPro devices. In addition, it provides System Defense and Agent Presence capabilities, which serve to protect vPro devices from mal-ware attacks and the removal of local 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 TLS. Currently, for Dash-enabled device, the only supported mechanism is through Digest authentication.

This guide introduces OOBM features, shows you how to configure OOBM, and provides detailed information and instructions for using its management console.

Features

The OOBM in the HPCA Console provides the following:

- 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, rebooted, and reimaged.
- Provides System Defense capabilities for vPro devices that allow for selective network isolation of Ethernet and IP protocol packet flows based on policies and filters created through the HPCA Console.
- Provides Agent Presence capabilities that allow for the monitoring of local agents running on vPro systems by agent watchdogs that are created through the HPCA Console. 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 HPCA Console.
- 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.

Audience

This guide is intended for administrators and operators who will be configuring and using the OOBM features in the HPCA Console to manage vPro and DASH-enabled devices.

Chapter Summaries

Introduction

This chapter contains an overview of Out of Band Management features.

SCS and vPro Setup

This chapter provides detailed steps for setting up and configuring the SCS Provisioning Server and the Intel vPro device.

Out of Band Management Configuration

This chapter tells you how to configure Out of Band Management.

Getting Started Managing OOB Devices

This chapter provides getting started instructions on how to login to the HPCA Console and start using the Out of Band Management features.

Out of Band Management Use Case Scenarios

This chapter provides typical use case scenarios that you can perform when using the HPCA Console to discover, heal, and protect OOB devices on your network.

Administrative Tasks

This chapter describes the basic configuration and operational tasks that the user in the Administrator role performs.

Provisioning vPro Devices

This chapter explains how to provision vPro devices through the HPCA Console.

Device Management

This chapter describes how to manage vPro and DASH-enabled devices on your network. It provides detailed descriptions on how to use every aspect of the Device Management window to manage these devices.

Group Management

This chapter describes how to use the Group Management functionality to manage groups of vPro devices on your network. It provides detailed descriptions on how to use every aspect of the Group Management window to manage these device groups.

Alert Notifications

This chapter describes how to view alerts generated by provisioned vPro devices when an event occurs.

Troubleshooting

This chapter provides troubleshooting information for the most common problems that can occur when using the HPCA Console to manage remote OOB devices.

2 SCS and vPro Setup

For the SCS Provisioning 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.

SCS is the Intel AMT Setup and Configuration Service. It is relevant to vPro devices only. It is assumed that you have already configured DASH-enabled devices according to the documentation for that device. Refer to DASH Configuration Documentation in the Getting Started Managing OOB Devices chapter. Further details can be obtained from the product documentation and from the HP support website.

Be sure to use the version of the SCS software that is bundled with the HPCA Core distribution media located in the `Media\OOBM\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.

Overview

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 allows for 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 HPCA Console will establish a TLS session with it before opening SOL or IDE-R sessions, thus ensuring that all relevant network communications are secure.

If you do not require TLS, skip to SCS Provisioning Server on page 20.

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.

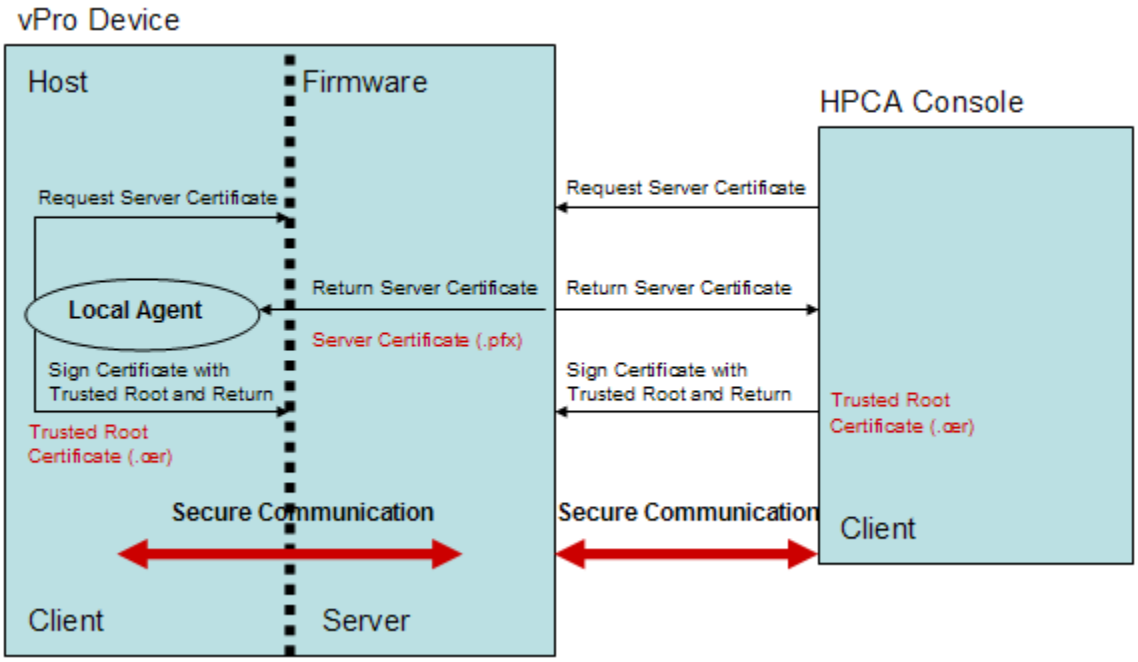
The Transport Layer Security (TLS) protocol has two kinds of authentication, TLS Server Authentication (one way authentication and TLS Mutual Authentication (two-way authentication). In the TLS protocol, the firmware on the vPro device is the SSL server. The HPCA Console and/or the local agent running 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 Certificate 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 local agent running on the host device and the HPCA Console are both clients to the vPro firmware. The functions of the local agent are discussed in greater detail later in this chapter and throughout this guide.

Figure 1 TLS Server Authentication



TLS Mutual Authentication

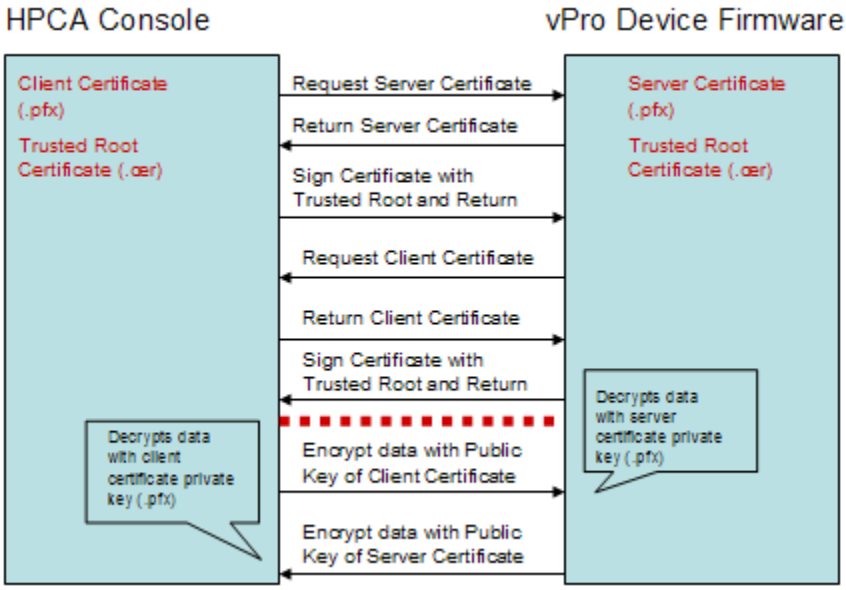
In addition to TLS server authentication where only one certificate is passed between the client and server, TLS mutual authentication provides greater security because two certificates are passed authenticating both ends of the communication. In mutual

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 HPCA Console and/or the local 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 HPCA Console is the client, the trusted root certificate must also be imported into the trusted key store on the HPCA Console machine. This allows the HPCA Console to sign the server certificate that the vPro device sends it authenticating the server. The client certificate installed on the HPCA 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 HPCA Console is acting as the client to the vPro firmware.

Figure 2 TLS Mutual Authentication between HPCA Console and vPro Device Firmware



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 HPCA Console.

You will use these values in the procedure for creating server and client certificate templates as described in To create the client authentication template on page 26. 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 Configuring the Profile on page 33.

SCS Provisioning Server

The Provisioning Server (also referred to as the Setup and Configuration Server) is the machine that runs the Intel Setup and Configuration Service (SCS). The SCS Provisioning Server performs all of the necessary steps to make a vPro device operational.

SCS Components

The major components of the SCS Provisioning Server are:

- Windows service (the SCS Main Service) for starting the server
- Secure database for storing root certificates and PID/PPS key pairs
- SOAP API
- AMT SCS console for provisioning vPro devices

SCS Provisioning of vPro Devices

The SCS Provisioning Server and the vPro device communicate securely. The SCS generates and sends the vPro device security-related configuration information that includes the following:

- Certificates from a public key infrastructure (PKI)
- Access Control Lists (ACLs)
- Setup parameters as defined in a profile of setup and configuration information specific to the platform or to a family of platforms
- Authentication Types TLS (Server Authentication or Mutual Authentication) or TCP
- Un-Provision and Re-Provision options

SCS provides initial values to vPro devices. Setup and configuration include setting the following parameters that are either included in profiles or generated automatically:

- Administrator account credentials (Username and password)
- Access control list (ACL) entries for Digest account types.

  The HPCA Console does not support Kerberos authentication. It supports Digest authentication only.

- Networking settings (host name and domain name)
- RSA key pair and X.509 certificate for TLS (TLS Certificate and RSA private key) (automatic)
- Pseudo Random Number Generator (PRNG) value
- Time and date (automatic)
- Trusted root certificates (Mutual TLS)
- Trusted domain name suffixes (Mutual TLS)
- Certificate Revocation Lists (CRLs)
- Power-policy options
- Replacement PID/PPS

SCS Configuration Scenarios

There are two ways to configure the SCS Provisioning Server with regard to Public Key Infrastructure (PKI).

You can install all of the software components required by the OOBM feature in the HPCA Console (including the Enterprise Root CA) on a single machine, namely, the Provisioning Server. This is referred to as Setup 1: Enterprise Root CA on Provisioning Server.

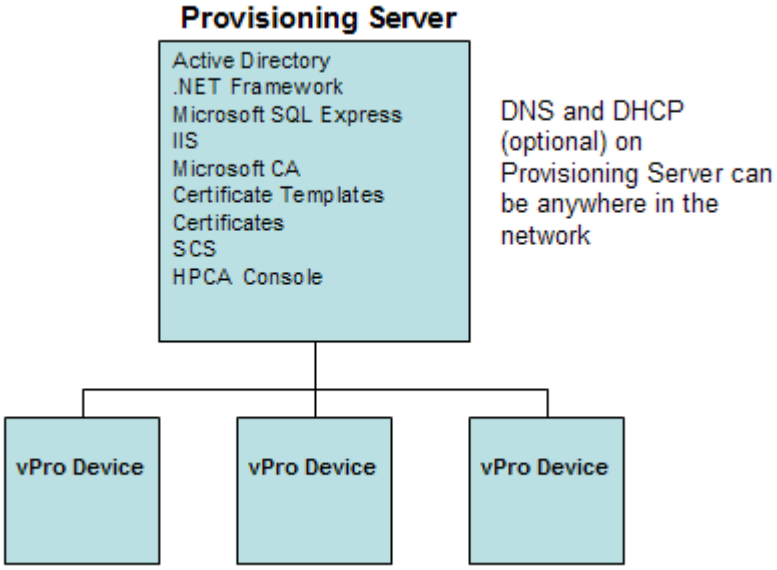
Alternatively, you can use two machines, an Enterprise Root CA Server and a Provisioning Server. This is referred to as Setup 2: Enterprise Root CA not on Provisioning Server. This configuration separates certificate-related components from SCS-related software components thus enhancing security.

In both configurations, all of the vPro devices, the Provisioning, and the Enterprise Root CA Server (if applicable) must be in the same domain with DHCP enabled.

These two configurations are discussed in greater detail in the following sections.

Setup 1: Enterprise Root CA on Provisioning Server

Figure 3 Setup 1: Root CA on Provisioning Server



In this configuration, all of the software components reside on a single machine. These components include the following:

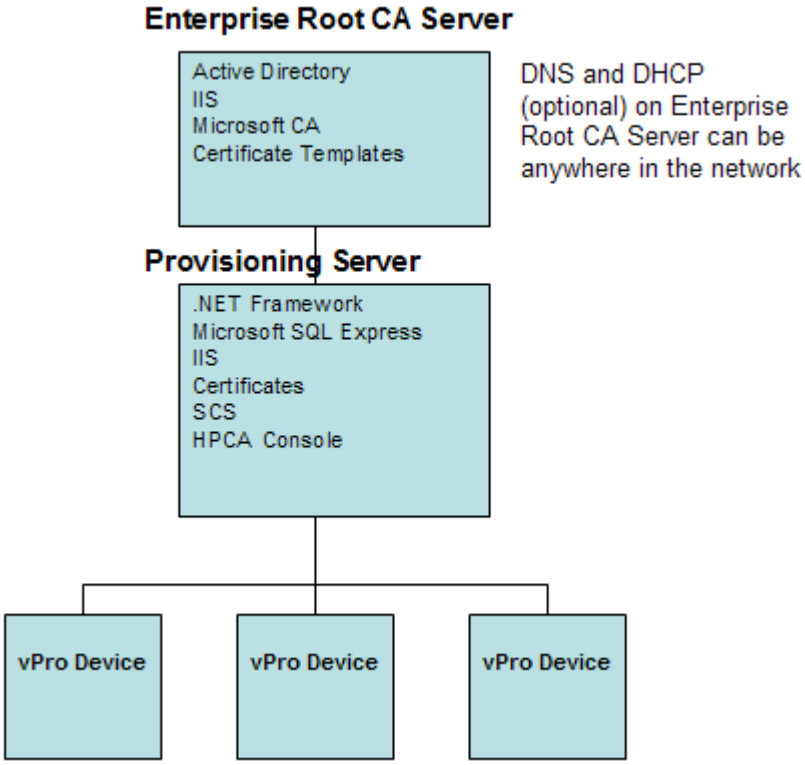
- Active Directory
- .NET Framework
- Microsoft SQL Server Express
- Internet Information Services (IIS)
- Microsoft CA and TLS certificate templates and certificates
- SCS software
- HPCA Console

In Setup 1, with the Enterprise Root CA on the Provisioning Server, the certificate templates are created, issued, installed, and exported on the Provisioning Server. This setup is not practical in a production environment because installation of management applications on the Active Directory Service Server is not recommended for security reasons. The Enterprise Root CA has the private key of the Root certificate and as such should be kept secure.

In Setup 2, this security is provided since a separate Enterprise Root CA Server is used to get the trusted root certificate and to create client and server certificates that are used in TLS authentication.

Setup 2: Enterprise Root CA not on Provisioning Server

Figure 4 Setup 2: Root CA on Enterprise Root CA Server



In this configuration, the Active Directory Service and the Enterprise Root CA services are installed on the Enterprise Root CA Server and the management applications are installed on the Provisioning Server. This configuration is recommended because it better secures the Root CA Server where the private key of the root certificate resides.

The Microsoft EnterpriseRoot CA Server is used to get the trusted root certificate and create the server and client certificates that are used in TLS authentication. The certificate templates are created, issued, installed, and exported on the Enterprise Root CA Server.

HPCA and SCS on Different Machines

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

Review the latest support matrix in the SCS documentation to be aware of the platforms upon which you can successfully install SCS. These may be a subset of the supported platforms for HPCA installation.

Non TLS Mode

If you are not using TLS authentication, there are no special configuration considerations if you use separate machines for the SCS and the HPCA Console software. Install all of the SCS-related software (except for HPCA) on the Provisioning Server as shown in Setup 1: Root CA on Provisioning Server on page 21. Install the HPCA software on a different machine.

From the HPCA Console, you enter the SCS login credentials and the URL for the SCS Service, which allows you to access vPro devices. The URL is usually specified as a fully qualified domain name (FQDN).

TLS Mode

If you are using TLS authentication, you must consider where to install the security certificates to ensure secure communication between the HPCA Console and the Provisioning Server.

If you are using Setup 1: Enterprise Root CA on Provisioning Server for your TLS configuration, install all SCS-related software (except for HPCA), as you did before, on the Provisioning Server as shown in Setup 1: Root CA on Provisioning Server on page 21. Install the HPCA software on a different machine. You must issue and install the client certificate on the machine on which you installed the HPCA software. Both the client and server certificates must be installed on the Provisioning Server.

If you are using Setup 2: Enterprise Root CA not on Provisioning Server for your TLS configuration, install the Active Directory Service and the Enterprise Root CA services, as you did before, on the Enterprise Root CA Server as shown in Setup 2: Root CA on Enterprise Root CA Server on page 22. Install all other SCS-related software (except for HPCA) on the Provisioning Server as shown in Setup 2: Root CA on Enterprise Root CA Server on page 22. Install the HPCA software on a different machine. You must issue and install the client certificate on the machine on which you installed the HPCA software. Both the client and server certificates must be installed on the Provisioning Server.

From the HPCA Console, you must still enter the SCS login credentials and the URL for the SCS Service. This is a secure communication because of the presence of the security certificates.

General Requirements

The operating system requirement on the server is Windows Server 2003 Standard Edition or Windows Server 2003 Enterprise Edition (32 bit only).

Integrating with Active Directory

Make sure that the vPro devices, the Provisioning Server, and the Enterprise Root CA Server (if using Setup 2), are all in the same domain. Intel vPro devices must be in the Computers (CN) domain of the Active Directory.

The DHCP and Domain Name servers must be running. This assumes that DHCP and DNS have already been installed although they need not be installed on the same machine as the Enterprise Root CA Server.

Installing .NET Framework 2.0

On the Provisioning Server, install .NET Framework 2.0. Refer to the *Intel AMT SCS Version 5.0 Installation Guide* located in the `Media\oobm\win32\AMT Config Server` directory of the HPCA Core distribution media.

Installing Microsoft SQL Server Express

On the Provisioning Server, install Microsoft SQL Server Express. Refer to the *Intel AMT SCS Version 5.0 Installation Guide*.

Installing Internet Information Services (IIS) 6.0

On the Provisioning Server and the Enterprise Root CA Server (if using Setup 2), install Internet Information Services (IIS) 6.0. Refer to the *Intel AMT SCS Version 5.0 Installation Guide*.

A server certificate must be imported into the IIS Web server environment. This server certificate is necessary because SCS is an IIS application, which requires the HTTPS protocol to communicate securely with its SCS console. The procedures to create, issue, install, export, and import a server certificate are discussed in Setting up the IIS Server Certificate on page 31.

Setting up Certificates for TLS

If you set up TLS authentication on the HPCA Console, it will be able to manage only those vPro devices that have been configured to use TLS. Conversely, if you have not set up TLS authentication on the HPCA Console, it will be able to manage only those vPro devices that have not been configured to use TLS.

This section is relevant only if you want to set up TLS mutual authentication between the HPCA Console and the vPro devices. If you do not require TLS, skip to Setting up SCS on page 30.

Installing the Microsoft CA

The Microsoft CA allows you to create the client certificate and to export it and the trusted root certificate so that they can be used for TLS authentication.

The trusted root certificate exported by the Microsoft CA is the public key of the CA, which is used to sign any client or server certificate created with the Microsoft CA. The trusted root certificate must be installed locally on any machine that must authenticate a certificate from this CA. As such, the root certificate is needed on both the HPCA Console and the vPro device.

Client Certificate

As indicated, the Microsoft CA is used to create the client certificate. Its private key will be exported and then converted to a format where it can be used on the HPCA Console to secure IDE-R/SOL operations with vPro devices.

Server Certificate

The server certificate for the vPro device is automatically imported into its firmware when it is provisioned by the SCS server if you select TLS when setting up the profile for the device.

Root Certificate

The trusted root certificate is the public key of the CA used by both the server and client to verify the digital signatures on the server and client certificates exchanged during TLS mutual authentication.

If you are using Setup 1 (single machine setup), perform these steps on the Provisioning Server. If you are using Setup 2 (dual machine setup), perform these steps on the Enterprise Root CA Server.

To install the Microsoft CA

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 CA must be the same as the Computer Name on which you are installing the 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 allows 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 Exporting the Root Certificate on page 29.

Creating the Client Certificate Template

Now you must create a client certificate for TLS mutual authentication. The client certificate will be installed on the HPCA Console and converted to PEM format to secure redirection operations as described in To convert the client certificate to PEM format on page 61 in the Out of Band Management Configuration chapter.

Certificate templates are used to help simplify the choices a certificate requester has to make when requesting a certificate, depending on the policy used by the CA. So the first step in creating a certificate is to create a template for that certificate.

If you are using Setup 1 (single machine setup), perform these steps on the Provisioning Server. If you are using Setup 2 (dual machine setup), perform these steps on the Enterprise Root CA Server.

To create the client authentication template

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 on 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 allows the private key for the server certificate to be exported.

> If the policy already exists with the same Object identifier, you can select it from the list. You will not be allowed to create it again.

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.

Issuing the Client Certificate Template

Before you can install the certificate, you must issue the certificate template. This step enables the template to become a certificate.

If you are using Setup 1 (single machine setup), perform these steps on the Provisioning Server. If you are using Setup 2 (dual machine setup), perform these steps on the Enterprise Root CA Server.

To issue the client certificate template

1 Click the Windows **Start** button and select **Administrative Tools** > **Certificate Authority**.

2 Expand the installed CA. Right-click on Certificate Templates and select **New** > **Certificate Templates to Issue**. The Enable Certificate Templates window opens.

3 Select the client authentication template you created in Creating the Client Certificate Template on page 26. 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.

Installing the Client Certificate

Now you are ready to use the template to install the client certificate in the Windows certificate store on the Provisioning (SCS) server. It will eventually be exported from this store and copied over to the HPCA Console and converted to PEM format where it can be used for client authentication to secure redirection operations on vPro devices.

To install the client certificate

1. On the Provisioning Server, go to one of the following URLs depending on the configuration you used:
   - Setup 1 (single machine configuration): **http://***FQDN_ProvisioningServer***/certsrv**
   - Setup 2 (dual machine configuration): **http://***FQDN_EnterpriseCARootServer***/certsrv**

   You can find the fully qualified domain name (FQDN) of a machine from the Windows desktop on that machine. Right-click **My Computer**, select **Properties**, and select the **Computer Name** tab.

   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. Click **Add**.

   e. Unselect the **Require Server Verification (https :) for all sites in this zone** checkbox.

   f. Click **OK**.
2. Click **Request a certificate**. Click **Advanced certificate request**. Click **Create and submit a request to this CA**.
3. Select the client certificate template in **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 Provisioning Server.
5. Select the **Mark keys as exportable** checkbox.
6. Click **Submit**. Select **Yes** in the subsequent window and install the certificate.

Exporting the Client Certificate

In this procedure, you export the private key file (`.pfx`) for the client certificate that you installed in the Windows certificate store in the previous procedure. The client private key will be installed on the HPCA Console 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 To convert the client certificate to PEM format on page 61 in the Out of Band Management Configurationchapter.

To export the client certificate

1. On the Provisioning 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 on 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** and click **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 a name for the file. Fully specify its path. The suffix for the file indicating its file type (`.pfx`) is automatically generated. 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.

21 Copy the certificate file to a location on the HPCA Console machine if this machine is different from the Provisioning Server.

Exporting the Root Certificate

In this procedure, you export the trusted root certificate in the Windows certificate store as a `.cer` file so that it can be used in the TLS mutual authentication process. The root certificate is needed on both the vPro device and the HPCA Console to verify the digital signature on the server and client certificates.

- On the vPro device, the SCS provisions the device with the root certificate when it configures the profile for the device as described in Configuring the Profile on page 33. The root certificate is needed on the vPro device so that it can authenticate the identity of the HPCA Console client when the management console sends the device its client certificate.
- On the HPCA Console, the root certificate is added to the Java key store (as described in the To import the root certificate into the Java key store procedure in the Out of Band Management Configuration chapter) so that it can be used to authenticate the identity of the vPro device server when the device sends the management console its server certificate. The trusted root certificate is used for signing with vPro devices to

authenticate hardware and software queries and remote control capabilities. It is also converted to PEM format (as described in To convert the root certificate to PEM format on page 61 in the Out of Band Management Configuration chapter) so that it can be used to secure IDE-R/SOL operations when TLS mutual authentication is turned on.

If you are using Setup 1 (single machine setup), perform these steps on the Provisioning Server. If you are using Setup 2 (dual machine setup), perform these steps on the Enterprise Root CA Server.

To export the root certificate

1. Click the Windows **Start** button and select **Administrative Tools** > **Certificate Authority**.
2. On the left-side of the window, right-click on the installed CA. A popup menu opens.
3. Click **Properties** and select the **General** tab.
4. Select the certificate and click **View Certificate**.
5. Select the **Details** tab
6. Click **Copy to file**. Enter a name for the file. Fully specify its path. The suffix for the file indicating its file type (`.cer`) is automatically generated. Make note of the location since you will have to access it in subsequent procedures.
7. Complete the remaining steps in the Wizard. A message displays indicating that the export was successful. Click **OK**. You are returned to the **Details** tab.
8. Click **OK** three times. You are returned to the Certificate Authority Management Console. Close the console.
9. Copy the certificate file to a location on the Provisioning Server if you are using the dual machine setup.

Setting up SCS

The Setup and Configuration Service (SCS) must be configured so that all communications with the vPro device are secure.

Installing SCS

This software is installed on the Provisioning Server. See the SCS Configuration Scenarios on page 21.

To install SCS

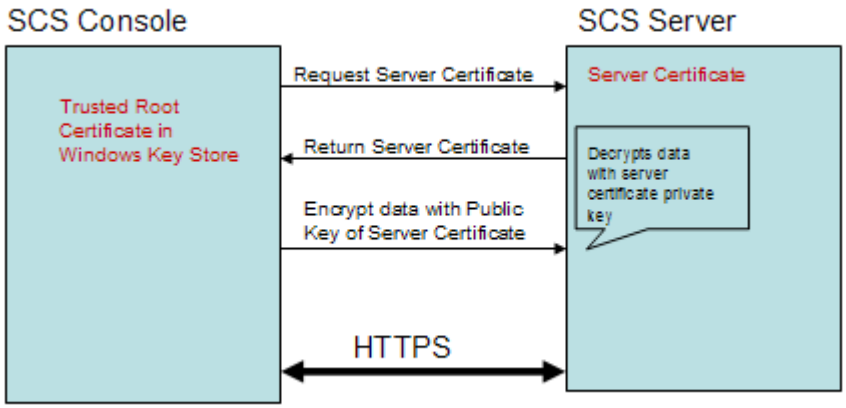
To install the components of the SCS, refer to the “Installation” chapter in the *Intel AMT SCS Version 5.0 Installation Guide* located in the `Media\oobm\win32\AMT Config Server` directory on the HPCA Core distribution media.

➤ Review the latest support matrix in the SCS documentation to be aware of the platforms upon which you can successfully install SCS. These may be a subset of the supported platforms for HPCA installation.

Setting up the IIS Server Certificate

You will need a server certificate to provide secure communication between the SCS server and the SCS console. The following figure illustrates the authentication that takes place between these two components.

Figure 5 SCS Authentication



One way to provide such a certificate is through the Microsoft Certificate Authority.

Refer to the "Securing the Connection to IIS Using SSL" section under the "Installing Microsoft's Certificate Authority" section in the *Intel AMT SCS Version 5.0 Installation Guide*.

You must install the server certificate on the SCS Provisioning Server as illustrated in SCS Authentication on page 32.

Logging in to the AMT SCS Console

To log in to the AMT SCS console

1. On the Provisioning 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 Intel AMT SCS Console opens.

Configuring SCS Service Settings

To configure SCS Service settings

1. Open the Intel AMT SCS Console.
2. Navigate to **Tools** > **Console Settings**. The SCS Service Settings window opens.
3. In the SCS Service Settings window specify the following:
   - **Active Directory Integration**: Select **None** from the pull-down list.
   - **First common name (CN) in certificate subject name**: Select **Fully Qualified Domain Name** from the pull-down list.
   - **TCP Listener Port**: Select **9971** from the pull-down list.
   - **AMT requires authorization before performing configuration**: Do *not* select this checkbox.
   - **Allow Remote Configuration**: Select this checkbox.

— **One Time Password required**: Select this checkbox if you need additional security when performing delayed Remote Configuration. If this checkbox is checked, bare metal Remote Configuration will not be successful. See Configuring the vPro Device through Remote Configuration on page 38 for details.

4 Click **Apply**.

5 Select the **Logging** tab. Select the **Log Level** as **Verbose** (optional, but a good idea).

6 Click **Apply**.

7 Select the **Intel AMT Configuration** tab. Select the **Retrieve configuration parameters from database** option.

8 Click **Apply**.

9 You can accept all the other default settings.

For additional information, refer to the "Viewing and Configuring SCS Services" section in the *Intel AMT SCS Version 5.0 Console User's Guide*.

Configuring Security Keys

This procedure is required only if you are going to manually set up your vPro devices through the Management Engine BIOS Extension (MEBx) in pre-shared key (PSK) mode. See Configuring the vPro Device through the MEBx on page 37.

If you plan to automatically set up your vPro devices through Remote Configuration in Public Key Infrastructure (PKI) mode, you do not have to perform this procedure. See the Configuring the vPro Device through Remote Configuration on page 38.

To configure security keys

1 Open the Intel AMT SCS Console.

2 Navigate to **Advanced** > **TLS-PSK Security Keys**.

3 In the Result Area, right-click and select **Add Security Keys** from the context menu. The Create TLS-PSK keys window opens.

4 In the Create TLS-PSK keys window specify the following:

— **Number of keys to store (one key per platform)**: This option determines the number of PID/PPS key pairs that will be generated. In our example, we have set this value to 2.

— **Manufacturing default MEBx Password**: This field displays the factory default password.

— **New MEBx Password**: This field displays the new password. It is recommended that you select **Fixed Password** and supply the new password.

5 Click **OK**.

For additional information, refer to the "Configuring Pre-Setup and Configuration Security Keys" section under the "Using USB Drives for TLS-PSK Keys" section in the *Intel AMT SCS Version 5.0 Console User's Guide.*

Configuring the Profile

This profile is associated with a vPro device as described in Creating New vPro Systems on page 36. The profile provides initial values to the vPro device during the provisioning process.

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 will need to refer to the documentation that comes with your wireless router.

When configuring the WPA-TKIP profile through the Wireless Access Point of your router, you must make the following selections:

- Set the wireless mode to WPA – Personal (Wi-Fi Protected Access).
- Set the encryption algorithm to TKIP (Temporal Key Integrity Protocol).

When creating a profile, use the following guidelines:

- Select the **Digest User** as the user type for ACL since it is the only supported user type in HPCA Console.
- For TLS, enable **Use mutual authentication** for the remote interface between the HPCA Console and the vPro device.

To configure the profile

1. Open the Intel AMT Console.
2. Navigate to **Profiles** > **All Profiles**.
3. In the Result Area, right-click and select **Add Profile** from the context menu. The Add Profile Wizard opens.
4. Click **Next** to continue. The General Settings window opens.
5. In the General Settings window, specify the following:
   - **Profile Name**: Enter a name for the profile, for example, **PSGProfile**.
   - **Description**: Enter a description for the profile, for example, **Profile for PSG**.
6. Click **Next**. The Advanced Settings window opens.
7. In the Advanced Settings window, specify the following:
   - Under Platform Interface Settings: Enable the **Web UI**, **Serial Over LAN**, and **IDE Redirection** interfaces.
   - Under Power Management Settings: Accept the default settings.
   - Under Additional Settings: Click **Set**. The Advanced profile settings window opens.
8. In the Advanced profile settings window, specify the following:
   - Under New MEBx password: For **New password for certificate based configuration**, enter the MEBx password of the PSK, which is going to be used to provision the vPro device. This is the password you created in step 4 of To configure security keys on page 33.
   - Under Configuration encryption mode: Accept the default settings.
   - Under Kerberos: Accept the default settings.
   - Under Network Settings; Select **Enable ping responses**.
9. Click **OK**.
10. Click **Next**. The Optional Settings window opens.
11. 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.)

12 Click **Next**. The ACL Details window opens.

13 Click **Add**.

14 In the ACL Details window, specify the following:

- **User Type**: Select the **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 pull-down list.
- **Realms**: Check the appropriate realms in the list. Realms determine the type of operations the user account can perform when managing a vPro device with the HPCA Console. It is recommended that you select all realms except the Security Audit Log Realm for the first account that you create.

15 Click **OK**.

- If you have enabled only the ACL and TLS options in Optional Settings, click **Next** and go to step 16.
- If you have enabled only the ACL and WiFi network options in Optional Settings, click **Next** and go to step 18.
- If you have enabled the ACL, TLS and WiFi network options in Optional Settings, Click **Next** and follow all steps from 16 on.
- If you have not enabled both the TLS and WiFi network options in Optional Settings, click **Next** and click **Finish** (last step of the procedure).

16 In the TLS window, specify the following:

- Under Basic TLS Configuration: For **TLS Server Certification Authority**, select the CA from the pull-down list. For **Server Certificate Template**, select **WebServer** from the pull-down list.
- Under Advanced TLS Configuration: Enable **Use mutual authentication**. Check the desired TLS trusted root certificates in the list.
- Click **Add**. The Add Trusted Root Certificate window opens. In this window, select **From File** and browse to the root certificate exported in Exporting the Root Certificate on page 29. You can view the certificate. Click **OK** to complete the task.

17 Click **Next** in the Optional Settings window. If you are in the Finish window, click **Finish** (last step of the procedure). Otherwise, if you have chosen the WiFi network option, the Optional Settings: WiFi window opens.

18 Click **Add**. The WiFi Profile window opens.

19 In the WiFi Profile window, specify the following:

- **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. Refer to the wireless router documentation.
- **Key Management Protocol**: Select WiFi Protected Access (WPA) from the pull-down list.
- **Encryption Algorithm**: Select Temporal Key Integrity Protocol (TKIP) from the pull-down list.

— **Passphrase**: Enter the pass phrase value that you used when you set up the WPA-TKIP profile in the router Wireless Access Point. Refer to the wireless router documentation.

20 Click **Apply** and **OK**.

21 Check the Wireless Profile created and click **Next**. The Finish window opens.

22 Click **Finish**. The profile is created.

For additional information, refer to the "Creating a Profile" section under the "Creating and Changing Profiles" section in the *Intel AMT SCS Version 5.0 Console User's Guide.*

Creating New vPro Systems

In order to provision a vPro device in PSK mode, information about that device must be entered into SCS. The following procedure explains how to enter this provisioning information.

This procedure is required only if you are going to manually set up your vPro devices through the Management Engine BIOS Extension (MEBx) in pre-shared key (PSK) mode. See Configuring the vPro Device through the MEBx on page 37.

If you plan to automatically set up your vPro devices through Remote Configuration in Public Key Infrastructure (PKI) mode, you do not have to perform this procedure. See Configuring the vPro Device through Remote Configuration on page 38.

To create new vPro systems

1 Open the Intel AMT SCS Console.

2 Navigate to **Platform Collections** > **All Platforms**.

3 In the Result Area, right-click and select **New Platform** from the context menu. The Platform Settings window opens.

4 In the Platform Setting window, specify the following:

— **FQDN**: Enter the fully qualified domain name of the target vPro device.

— **UUID**: Enter the UUID of the target vPro device. The UUID can be obtained from the BIOS.

— **Active Directory OU**: Enter the LDAP name in distinguished name format. In our example, it is **CN=Computers,DC=AMT,DC=HP,DC=COM**.

— **Profile**: Select the profile you created in Configuring the Profile on page 33 from the pull-down list. In our example, it is PSGProfile.

5 Click **Apply** and then **OK**.

Now it is possible to set up the vPro device as described in the next section.

For additional information, refer to the "Adding a Platform Definition" section under the "Preparing and Managing Platforms" section in the *Intel AMT SCS Version 5.0 Console User's Guide.*

Setting up the vPro Device

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 and the vPro device.

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.

Both methods are described in the next sections.

Configuring the vPro Device through the MEBx

To configure the vPro device through MEBx

1. Restart the system. As the system restarts, press **Ctrl-P** to enter the Management Engine BIOS Extension (MEBx) window.
2. Enter **admin** for the ME password. This password will be accepted once.
3. Select **Change Intel ® ME Password** and set the password to the value specified in step 4 of To configure security keys on page 33.
4. Select **Intel ME Configuration**. Press **Y** to reset system configuration. This opens the Intel ME platform configuration window. Select **Intel ME State Control** and choose **Enable**.
5. Select **Intel ® ME Firmware Local Update Qualifier** and choose **Always Open**.
6. Select **Intel ® ME Features Control**. Then select **Manageability Feature Selection** and choose **Intel ® AMT**.
7. Select **Intel ® Quiet System Technology** and choose **Enabled**. Then return to the previous menu.
8. Select **Intel ® ME Power Control**. Then select **Intel ® ME State Upon Initial Power On** and choose **ON**.
9. Select **Intel ® ME ON in Host Sleep States** and choose **Always**.
10. Select **LAN Power Well** and ensure that **WOL EN Pin** is selected.
11. Select **Intel ® ME Visual LED Indicator** and ensure that **ON** is selected. Then return to the previous menu. Return to the previous menu again. Select **Exit**. Press **Y** to confirm. This saves the configuration and the system reboots automatically. If the system does not reboot, reboot it manually.
12. As the system reboots, pull out the power and LAN cable. Wait ten seconds.
13. Restart the system. As the system restarts, press **Ctrl-P** to enter the MBEx window again.
14. Enter the new password that you specified in step 3 of this procedure.
15. Select **Intel ® AMT Configuration**.
16. Select **Hostname** and enter the hostname of the vPro device.

17 Select **TCP/IP**. Press **N** when asked to disable the Network Interface. Press **N** when asked to disable the DHCP. You want to keep them in the enabled state.

18 Select **Provisioning Server**. Enter the IP address of the machine you are using to run Intel SCS. Set the port to 9971.

19 Select **Provisioning Model** and ensure that **Intel ® AMT 2.0** mode is selected by pressing **N**.

20 Ensure that **Enterprise Mode** is selected by pressing the appropriate key (**Y/N**).

21 Select **Set PID and PPS**.

22 Set the PID and PPS to the values specified in step 7 of To configure security keys on page 33.

23 Select **Return to Previous Menu**, select **Exit**, and press **Y** to confirm.

You should now be able to see the setup and configuration process occurring and completing with success by viewing the Provisioning Server's console.

The preceding steps may not represent the exact procedural steps for your vPro device. Refer to the vendor documentation for the device to see the definitive steps.

Configuring the vPro Device through 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:

- Purchase a security certificate from a trusted Certificate Authority (CA). The CA vendor must match one of the vendors whose root certificate hashes are built into the vPro firmware. You must install the certificate in the System Certificate Store on the system where the SCS Server is installed. See sections starting with Getting a Certificate for Remote Configuration on page 40.
- Install the local agent on the host vPro device. The local agent will start the delayed configuration process if the vPro device was not successfully provisioned when it was first connected to the network.

  Delayed configuration is performed when the vPro device could not be provisioned within the time window that the network interface is opened after the device is connected to the network. See Limited network access on page 39. Delayed Remote Configuration is discussed in To manually install the local agent on the vPro device on page 43 of this chapter and Delayed Remote Configuration of the vPro Device on page 120 of the Provisioning vPro Devices chapter.

  Typically, immediate setup of the vPro device occurs (if you have performed the Remote Configuration Requirements correctly) when you connect the device to the network. This is referred to as *bare metal configuration*. The device will start sending out "Hello" messages to the SCS server indicating that it has transitioned to setup mode. If the device can be successfully provisioned in the time window that the network interface is opened for that device, no further provisioning tasks need to be performed. See Bare Metal Remote Configuration of the vPro Device on page 40.

These concepts and procedures are developed in greater detail in the following sections.

Remote Configuration Features

Remote Configuration is possible because of the following vPro features:

- Embedded hashed root certificates

  The vPro device contains one or more root certificate hashes from worldwide SSL certificate providers in its firmware image. As part of the “Hello” message, the vPro device sends all of the hashes to the SCS. When the SCS authenticates to the vPro device, it must do so with a certificate compatible with one of the hashed root certificates. The vPro device checks the list of embedded root certificate hashes to verify that the TLS Client Certificate sent by SCS is a valid certificate signed by one of the CA root certificates in the list.

- Self-signed certificate

  The vPro device produces a self-signed certificate that it uses as a TLS Server Certificate to authenticate to the SCS for configuration purposes only. The SCS must be configured to accept a self-signed certificate.

- One-time password

  When performing delayed configuration, the security policy may require use of a one-time password (OTP) to improve security. The local agent running on the local host requests the OTP from the SCS and sends it to the firmware on the vPro device. The SCS saves the OTP in the database entry associated with the specific vPro device, and uses it to validate the connection to the device. The OTP is used in delayed configuration only; it cannot be used in bare metal. See Remote Configuration Provisioning Process on page 41.

- Limited network access

  The network interface opens for a limited time interval to send “Hello” messages and to complete the setup and configuration process. For Intel machines, this time interval is 24 hours. For HP desktops, it 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.

Remote Configuration Requirements

Before you can begin the Remote Configuration process, the following requirements must be met:

- The vPro device must be configured to receive its IP address from a DHCP server. The DHCP must support option 15, which allows it to return the local domain suffix to the vPro device for inspection.
- The vPro device has been pre-programmed with at least one active root certificate hash.
- For the delayed configuration process, the local agent must be installed and running on the vPro host machine. See To manually install the local agent on the vPro device on page 43.
- The SCS Server must be registered with a DNS server that is accessible to the vPro device with the name `Provisionserver`, and it must be in either the same domain as the device or in a domain with the same suffix.
- The SCS Server must have a certificate with an Organizational Unit (OU) or Organizational ID (OID) that traces to a CA, which has a root certificate hash stored in the vPro device. See Acquiring and Configuring a Certificate for Remote Configuration on page 40 for more details.
- The SCS Server must be configured to allow Remote Configuration. See Configuring SCS Service Settings on page 32.

The OTP option must not be enabled for bare metal configuration.

Getting a Certificate for Remote Configuration

In order to configure vPro devices through the Remote Configuration process, you must purchase a trusted certificate from one of the following Certificate Authorities (CAs):

- VeriSign Class 3 Primary CA-G1
- VeriSign Class 3 Primary CA-G3
- Go Daddy Class 2 CA
- Comodo AAA CA

These are the vendors whose root certificate hashes are built into the Intel 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.

Acquiring and Configuring a Certificate for Remote Configuration

To acquire and configure a certificate for remote configuration, refer to the "Acquiring and Configuring a Certificate that Supports Remote Configuration" section in the "Remote Configuration" Appendix of the *Intel AMT SCS Version 5.0 Console User's Guide.* This document is located in the `Media\oobm\win32\AMT Config Server` directory on the HPCA Core distribution media.

Creating and Installing Your Own Certificate

It is also possible to create and install your own certificate to allow remote configuration. To create and install your own certificate for remote configuration, refer to "Creating and Installing Your Own Certificate" section in the "Remote Configuration" Appendix of the *Intel AMT SCS Version 5.0 Console User's Guide*. This document is located in the `Media\oobm\win32\AMT Config Server` directory on the HPCA Core distribution media.

Selecting the SCS Certificate for Remote Configuration

The information in this section is required only if you have created a multipurpose certificate template and want to import it into the user's personal certificate store. To create a multipurpose certificate template, refer to the" Creating a Multipurpose Certificate Template" section in the "Remote Configuration" Appendix of the *Intel AMT SCS Version 5.0 Console User's Guide*.

To select the SCS certificate for remote configuration, refer to the "Selecting the Certificate Used by the SCS for Remote Configuration" section in the "Remote Configuration" Appendix of the *Intel AMT SCS Version 5.0 Console User's Guide.* This document is located in the `Media\oobm\win32\AMT Config Server` directory on the HPCA Core distribution media.

Bare Metal Remote Configuration of the vPro Device

Transitioning to Setup Mode

A vPro device starts sending "Hello" messages as soon as the device is connected to AC power and to the network. Intel uses "bare metal configuration" to describe a device that has been connected to the network and has its limited access network window still open for provisioning.

However, the term “bare metal” usually refers to a system with no operating system installed. Specifically, in the case of a vPro device, it is a system that does not have an operating system installed on the vPro host machine.

With no operating system, there is no way to run the local agent to install a one-time password (OTP) to provide additional security. These concepts are explained in Delayed Remote Configuration of the vPro Device on page 120 in the Provisioning vPro Devices chapter.

Simplified One-Touch Configuration

Although it is not possible to use the OTP in the bare metal setup, you can provide additional security if the FQDN of the SCS Server is entered on a bare metal vPro system. This is referred to as *Simplified One-Touch* configuration.

Remote Configuration Provisioning Process

Except for the fact that there is no OTP exchange, the setup and configuration flow is the same as the delayed configuration that employs the local agent as described in Remote Configuration Provisioning Process on page 41. .

The SCS cannot setup bare metal systems when an OTP is required. As a result, the OTP option in the SCS server must not be enabled for bare metal configuration to succeed.

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 will automatically send 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 allowing for 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

If bare metal configuration fails, you can provision the device by using delayed configuration. There are two ways a vPro device can be provisioned through delayed configuration. They are the following:

- Local Agent as described in the next section of this chapter.
- HPCA Console as described in Delayed Remote Configuration of the vPro Device on page 120 in the Provisioning vPro Devices chapter.

Installing the OOBM Local Agent

It is recommended that you install the HP CA Out Of Band Management local 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 local agent will invoke delayed configuration as part of its installation process on unprovisioned devices.

To understand what occurs during the transition to Setup mode and the provisioning process in delayed configuration, see Delayed Remote Configuration of the vPro Device on page 120 in the Provisioning vPro Devices chapter.

One-time Password Setting

It is also recommended that you go back into the SCS setup and enable one-time password (OTP) if this additional security is required as part of your network security policy. See Configuring SCS Service Settings on page 32.

Methods for Installing the Local Agent

There are two ways to install the local agent on vPro devices. One way is to install the local agent manually on each vPro device. Alternatively, you can install the local agent automatically to multiple vPro devices through the Client Automation Standard or Enterprise software.

Both methods are described in the following sections.

Configuration Client Role

To be able to provision vPro devices through the local 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 local agent installation. The user credentials of the SCS configuration client must be provided correctly, otherwise the local agent will not be able to start the provisioning of the device through delayed setup.

When installing the local 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 will fail with error code 1920.

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

Manual Install on Individual vPro Device

To manually install the local agent on the vPro device

1. Copy the `oobmclocalagent.msi` file located in the `\Media\client\default\win32\oobm\LocalAgent` directory on the HPCA 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. 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 allows 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.
   - Check 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 local agent is an NT service and starts as soon as it is installed.

Automatic Install on Multiple vPro Devices through Client Automation

As indicated, you can automatically install the local agent on multiple devices through the Client Automation Standard or Enterprise software.

You cannot use this method to install the local agent if you have the Starter edition of the Cleint Automation software.

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

- You must publish the HP CA Out Of Band Management local agent software to the Client Automation database by using the Client Automation Publisher.
- You must deploy the local agent to the vPro target devices by using the Client Automation management console.

To publish the local agent to the Client Automation database

1. Select **Start** > **Programs** > **HP Client Automation Administrator** > **Client Automation Publisher** to invoke the Client Automation Publisher. The Logon window opens.
2. Log in to the Publisher using the Client Automation user name and password. By default, the user name is `admin` and the password is `secret`. The Publisher dialog window opens.
3. From the pull-down list, select **Windows Installer**.
4. Click **OK**. The Select wizard in the Publisher opens.
5. Select the local 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 in the Publisher 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 in the Publisher opens.
10. In this window, specify the following (fields not listed are optional):
    - **Service ID**: Enter a text string to identify the service, for example, **HP_CA_OOB_LOCAL_AGENT**.
    - **Description**: Enter a description for the software, for example, **HP CA OOB Local Agent**.
    - **Software catalog**: Select **User Application** from the pull-down list.
    - **Limit package to systems with**: If you do not select any of the operating systems, the software will be deployed to all vPro devices regardless of the operating system.
11. Click **Next**. The Publish wizard of the Publisher opens. Summary and Progress information are displayed.
12. Click **Publish**. The local agent application is published to the Client Automation database.
13. Click **Finish**.
14. Click **Yes** in the pop-up window to exit the Publisher.

To automatically deploy the local agent to multiple vPro devices

For detailed instructions on the following procedures, refer to the *HP Client Automation Core and Satellite User Guide* for either the Standard of Enterprise edition.

1. Import the vPro devices into Client Automation.
2. Deploy the Client Automation Management agent to the target vPro devices.
3. Create a static group and add the target vPro devices to the group.
4. Deploy the HP CA Out Of Band Management local agent to the vPro device group.

Checking Version of the Local Agent on the vPro Device

To check the version of the local agent

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

Local Agent on 64-bit Platforms

If you install the local 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.

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 Intel AMT Systems branch and select the target vPro device. The target vPro device is displayed with its provisioned status.
3. Expand the Logs branch and select the Log node. The log information is displayed.

Changing the Authentication Mode

This section is relevant only if you have set up TLS authentication. If you have not set up TLS, skip to the Out of Band Management Configuration 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 appropriate 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. Click **OK**.
8. 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 (non-TLS)

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 appropriate profile for the vPro Device and click **Edit**.
4. Select the **Network** tab and uncheck the Use TLS option.
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. Click **OK**.
8. 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.

3 Out of Band Management Configuration

This chapter explains how to configure Out of Band Management (OOBM) after it has been installed through the HPCA Installer. For system requirements and installation information, refer to the *HP Client Automation Core and Satellite Getting Started and Concepts Guide* and the *HP Client Automation Release Notes.*

Information about Configuration Parameters

Reconfiguring the SCS Path

If necessary, you can change the SCS path currently configured through the HPCA Console. See Setting Configuration Parameters on page 50.

Reconfiguring Client Automation Web Services

If necessary, you can change the gateway URL for the HPCA 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. See Setting Configuration Parameters on page 50.

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. See Setting Configuration Parameters on page 50. 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.

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 HPCA Console server, you can point to any local bootable ISO image instead of the Floppy drive for IDE-R operations.

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 HPCA 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 in order to have multiple simultaneous SOL sessions on vPro devices. You can change these values. See Setting Configuration Parameters on page 50.

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 HPCA Console. If HyperTerminal is not already installed, refer to 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. See See Setting Configuration Parameters on page 50.

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. See Setting Configuration Parameters on page 50.

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. See Setting Configuration Parameters on page 50.

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. See Setting Configuration Parameters on page 50. Modifying this value affects performance. This value is dependent on the availability of memory resources.

Configuring Security Parameters

This step is required only if you have TLS configured.

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 allow OOBM to locate the trusted root and client certificates, to know the passwords associated with them, and the FQDN of the Certificate Authority server.

You must configure the following:

- Full pathname to the root certificate in PEM format (`root_certificate`)
- Full pathname to the client certificate in PEM format (`client_certificate_pem`)
- Full pathname 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 page 50.

For information about certificates in PEM format, see Converting Certificates to PEM Format on page 61.

In addition, you must specify the password for the PEM and PFX client certificate as shown in the following command lines:

To specify the PEM client certificate password

1. Type `amtpem_chgpwd`.
2. When prompted, enter the password.

To specify the PFX client certificate password

1. Type `amtpfx_chgpwd`.
2. When prompted, enter the password.

Configuring Agent Watchdog Settings

When you are creating an agent watchdog, two of the settings for the agent watchdog are the local agent's heartbeat interval (time between heartbeats sent to the watchdog) and the startup time before the agent starts sending heartbeats to the watchdog. You can change the default values to reflect the needs of your network. Setting Configuration Parameters on page 50.

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 allows 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 allows you to change the time-out value in case there are any socket problems on the HPCA Console server when calling on vPro web services. If there are any problems that deal with sockets, it is recommended that you increase the time-out value.

See Setting Configuration Parameters on page 50.

Setting Configuration Parameters

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

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.

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.

Table 1 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 default value	URL of the HPCA Console
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.

Table 1 Configuration Parameters in the config.properties File (cont'd)

Parameter (key)	Default Value	Description
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 pathname to root certificate in PEM format
client_certificate_pem format	No default value	Full pathname to client certificate in PEM
client_certificate_pfx	No default value	Full pathname to client certificate in PFX format
ca_server_commonname	No default value	Client certificate CN
apwatchdog_heartbeat_interval	60 seconds	Watchdog local agent heartbeat interval
apwatchdog_startup_time	300 seconds	Watchdog local 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.
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)

Table 1 Configuration Parameters in the config.properties File (cont'd)

Parameter (key)	Default Value	Description
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 HPCA Console

Additional configuration parameters can be found in the `configuration.properties` file also located in the `<HPCA_Install_DIR>\oobm\conf\` directory. All of these parameters have been assigned default values, but some may require reconfiguration depending on your setup.

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 Table 2.

The Table 2 lists the parameters contained in this file with their default settings and descriptions.

Table 2 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
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.

Table 2 Configuration Parameters in the configuration.properties File (cont'd)

Parameter	Default Value	Description
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
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)

Table 2 Configuration Parameters in the configuration.properties File (cont'd)

Parameter	Default Value	Description
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 OOBM Server, the client will shut down the IDE-R session. When an IDE-R session is open, the OOBM Server continually sends out messages to make sure that the receive time-out value for the client does not expire (the OOBM 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 OOBM 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 OOBM Server. A value of 0 means that no heartbeat messages are sent. In this case, the OOBM 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 Default value: 5000

Table 2 Configuration Parameters in the configuration.properties File (cont'd)

Parameter	Default Value	Description
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

Table 2 Configuration Parameters in the configuration.properties File (cont'd)

Parameter	Default Value	Description
SOL_CLIENT_HB_INTERVAL	5000	Client heartbeat interval in milliseconds. This is the amount of time the client waits between sending heartbeat messages to the OOBM Server indicating that the client is active. A value of 0 means that no heartbeats are sent. In this case, the OOBM 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 OOBM Server, the client shuts down the SOL session. When an SOL session is open, the OOBM Server periodically sends heartbeat messages to make sure that the receive time-out for the client does not expire (the interval between OOBM Server heartbeat messages is based on the client receive time-out). Minimum value: 10000 Maximum value: 65535 Default value: 10000

Table 2 Configuration Parameters in the configuration.properties File (cont'd)

Parameter	Default Value	Description
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 OOBM 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
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

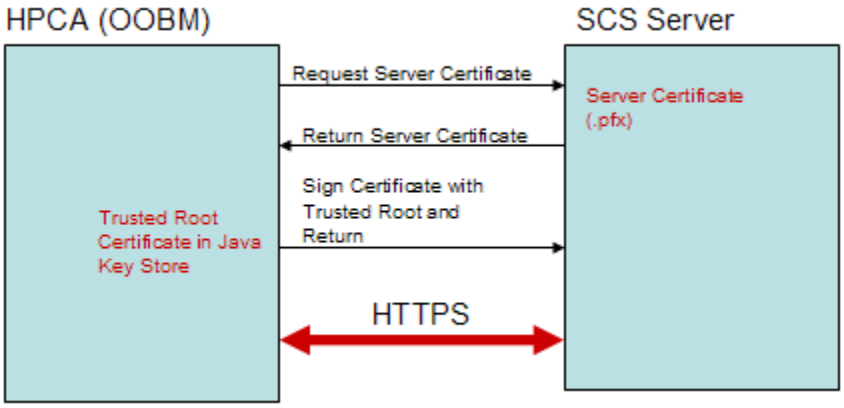
The values you give to the `*BOOT_SOURCE_VALUES` parameters are used in the HPCA Console GUI to provide user friendly names for these boot devices. If you do not provide values for these parameters, you may see some non-intuitive text strings displayed representing these boot devices. The string value 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

In Setting up the IIS Server Certificate on page 31 in the SCS and vPro Setupchapter, you created a server certificate by using the Microsoft CA. You imported this server certificate into the IIS Manager to secure SCS communication between the SCS server and the SCS console. See SCS Authentication on page 32 in the SCS and vPro Setupchapter.

You can also provide secure communication between the SCS server and the OOBM Service running on the HPCA Console 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 HPCA Console machine thus allowing the HPCA Console to sign the server certificate to authenticate the SCS server.

Figure 6 Secure Access between OOBM and SCS



To export the root certificate

If you have already exported the root certificate as part of the TLS mutual authentication setup as described in Exporting the Root Certificate on page 29 in the SCS and vPro Setupchapter, you do not have to perform this task again.

Follow the steps in To export the root certificate on page 30 in the SCS and vPro Setupchapter.

To import the root certificate into the Java key store

1. On the HPCA Console, backup the existing trusted certificate file. This is the `cacerts` file which is typically located in `C:\Program Files\Hewlett Packard\HPCA\jre\lib\security`.
2. At the command prompt, enter the following command:

   `keytool -import -noprompt -alias customcacert -keystore ..\lib\security\cacerts -storepass` *<store-password>* `-file` *<ca_file.cer>*

   — This command line assumes that you are running the command from the JRE bin directory. By default, this directory is `C:\Program Files\Hewlett Packard\HPCA\jre\bin`.

   — The *<store-password>* is the password of the certificate store. By default, this password is **changeit**.

   — The *<ca_file.cer>* is the full pathname to the root certificate you exported in Exporting the Root Certificate on page 29 in the SCS and vPro Setupchapter and copied over to the HPCA Console machine (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.

4 Restart the Tomcat Service.

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 HPCA Console is `C:\Program Files\Hewlett Packard\HPCA`.

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 HPCA Console server. See the Configuring Secure Access between OOBM Service and SCS on page 58.

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

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 on **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 Uncheck the **Require secure channel (SSL)** checkbox 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.

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 HPCA Console. This is used by OOBM to authenticate vPro devices. You exported this root certificate as a `.cer` file in the To export the root certificate on page 59.

If you have already imported the root certificate into the Java key store of the HPCA Console to secure communication between OOBM and the SCS server as described in the Configuring Secure Access between OOBM Service and SCS on page 58, you do not have to perform this procedure again.

To import the root certificate into the Java key store

Follow the steps in To import the root certificate into the Java key store on page 59.

Converting Certificates to PEM Format

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 HPCA Console. The root certificate was exported as a `.cer` file as described in To export the root certificate on page 59. The client certificate was exported as a `.pfx` file as described in the To export the client certificate on page 28 in the SCS and vPro Setupchapter. These files were copied over to the HPCA Console machine if this machine is different from the SCS server machine where the certificates were exported.

To convert the root certificate to PEM format

At the command line prompt on the HPCA Console machine, type the following:

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

Example:

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

To convert the client certificate to PEM format

At the command line prompt on the HPCA Console machine, type the following:

`Openssl pkcs12 –in <client.pfx> –out <client.pem>`

Example:

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

4 Getting Started Managing OOB Devices

This chapter gives you a quick overview of the Out of Band Management (OOBM) tasks you can perform in the HPCA Console. They include the Configuration tasks you perform as Administrator and the Operations you perform as Operator.

For best viewing results in the HPCA Console, set the screen resolution for the display console to 1280x1024.

Configuration

The following sections describe 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 HPCA Console. They include the following:

- Enabling Out of Band Management
- Selecting the Device Type
- Managing vPro System Defense Settings

Enabling Out of Band Management

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

On the **Configuration tab**, under **Out of Band Management**, click **Enablement**. The Enablement window opens.

Refer to Enablement on page 99 for complete details.

Selecting the Device Type

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

On the **Configuration tab**, 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, vPro Devices, or Both.

Depending on the device type that you chose, the HPCA Console displays an interface relevant to that selection as explained in Configuration and Operations Options Determined by Device Type Selection.

DASH Devices

If you select DASH, you can enter the common credentials for the DASH devices if the DASH administrator has configured all of the devices to have the same username and password.

You can change the credentials the next time you visit this window if you have made a mistake entering them or if they have changed.

vPro Devices

If you select vPro devices, you must enter the SCS login credentials and the URL for the SCS Service to access vPro devices.

You can change the credentials the next time you visit this window if you have made a mistake entering them or if they have changed.

Both

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.

Refer to Device Type Selection on page 102 for complete details.

Configuration and Operations Options Determined by Device Type Selection

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:

Table 3 Configuration and Operations options

	DASH	vPro
Configuration	No additional options	vPro System Defense Settings
Operations	Device Management	Provisioning vPro Devices , Device Management, Group Management, Alert Notifications

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

Managing 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.

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 agent watchdogs for the network in general when managing vPro devices.

- Managing System Defense Filters: For vPro devices, you can create, modify, and delete System Defense filters. 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. Filters are assigned to System Defense Policies that can be enabled to protect the network.
- Managing System Defense Policies: For vPro devices, you can create, modify, and delete System Defense policies and then deploy them to multiple vPro devices on the network. System Defense policies can selectively isolate the network to protect vPro devices from mal-ware attacks.
- Managing System Defense Policies: For vPro devices, you can create, modify, and delete heuristics specifications and then deploy them to multiple vPro devices on the network. 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.
- Managing Agent Watchdogs: For vPro devices, you can create, modify, and delete agent watchdogs and then deploy them to multiple vPro devices on the network. Agent watchdogs monitor the presence of local agents on the vPro device. You can specify the actions the agent watchdog must take if there is a change in state of the local agent.

Refer to vPro System Defense Settings on page 102 for complete details.

This is the last administrative task you have to perform on the **Configuration** tab to get the HPCA 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 as explained in Operations.

Operations

The following sections describe the operations you will want to perform in the Operator or Administrator role to manage OOB devices. You can perform these tasks on the **Operations** tab of the HPCA Console. They include the following:

- Provisioning and Configuration Information
- Managing Devices
- Managing Groups
- Viewing Alerts

Provisioning and Configuration Information

Your vPro and DASH devices must be provisioned before you can discover and manage them. It is possible to provision vPro devices through the HPCA console if the devices did not automatically become provisioned when originally connected to the network.

On the **Operations tab**, under **Out of Band Management**, click **vPro Provisioning**. The vPro Provisioning window opens. It allows you to discover and provision vPro devices.

This option does not appear on the **Operations** tab under **Out of Band Management** if you have selected to manage DASH devices only since it is not relevant for this type of device.

Refer to Provisioning vPro Devices on page 119 for complete details.

DASH Configuration Documentation

It is assumed that you have already provisioned DASH-enabled devices according to the documentation accompanying the device. DASH configuration information is documented in the "Broadcom NetXtreme Gigabit Ethernet Plus NIC" whitepaper. This can be found in the "Manuals (guides, supplements, addendums, etc)" section for each product that supports this NIC.

This information pertains to DASH-enabled devices from Hewlett-Packard only.

To access this documentation

1. Go to **www.hp.com**.
2. Select **Support and Drivers** > **See support and troubleshooting information**.
3. Enter a product that supports this NIC, for example, the dc5850.
4. Select one of the dc5850 models.
5. Choose Manuals (guides, supplements, addendums, etc).
6. Choose the "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 > **Download 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 NetXtreme Gigabit Ethernet Plus NIC driver.

Managing Devices

The Device Management option allows you to manage multiple and individual OOB devices.

On the **Operations tab**, under **Out of Band Management**, click **Device Management**. The Device Management window opens. From the icons on the toolbar of the device table, you can perform the following tasks on multiple devices:

- Refresh data
- Reload device information

- Discover Devices
- Power on and off and reboot devices
- Subscribe/unsubscribe to vPro alerts
- Manage common utilities on vPro devices
- Deploy System Defense policies to selected vPro devices
- Deploy heuristics worm containment information to selected vPro devices
- Deploy agent watchdogs to selected vPro devices
- Deploy agent software list and system message to selected vPro devices

Click the hostname link in the device table to manage an individual OOB device. A management window opens that has several options in its left navigation pane. The options available are dependent on the type of device you selected to manage. See Summary of Management Operations .

Refer to Device Management for complete details.

Managing Groups

The Group Management option allows 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, agent watchdogs, local agent software lists, and heuristics.

On the **Operations tab**, under **Out of Band Management**, click **Group Management**. The Group Management window opens. From the icons on the toolbar of the group table, you can perform the following tasks on multiple groups:

- Refresh data
- Reload group information
- Power on and off and reboot groups
- Subscribe/unsubscribe to vPro alerts
- Deploy agent software list and system message to selected vPro groups
- Provision vPro device groups
- Deploy and undeploy System Defense policies to selected vPro groups
- Deploy and undeploy agent watchdogs to selected vPro groups
- Deploy and undeploy heuristics worm containment information to selected vPro groups

To drill down to manage individual devices within a group, click the group name link under the Description column of the table. The Device Management window opens displaying a list of devices belonging to the selected group. You can manage multiple or individual devices within the group. See Managing Devices.

Refer to Group Management for complete details.

Viewing Alerts

For vPro devices, you can view the alerts generated by provisioned vPro devices if you have an alert subscription to the device. Monitoring alert notifications gives you a good idea of the health of the devices on your network.

On the **Operations tab**, under **Out of Band Management**, click **Alert Notification**. The Alert Notification window opens

Refer to Alert Notifications for complete details.

Summary of Management Operations

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

Table 4 Management Operations on Out of Band Devices

Management Operation	vPro	DASH	Where to Find Information
Provisioning Configuration[1]	X		Provisioning vPro Devices on page 119
Device Discovery[2]	X	X	Device Discovery on page 128
Managing Multiple Devices	X	X	Managing Multiple Devices on page 127
General Asset Discovery	X		Viewing vPro General Asset Information on page 141
Hardware Asset Discovery	X	X	Viewing Hardware Assets on page 141
Software Asset Discovery[3]	X	X	Viewing Software Assets on page 142
Power Management[4]	X	X	Changing the Power State on page 143
Rebooting[4]	X	X	Rebooting the System on page 147
Rebooting with IDE-R[4]	X		Rebooting the vPro System with IDE-R on page 148
Rebooting to BIOS[4]	X		Rebooting the vPro System to BIOS Settings on page 150
Rebooting to LAN (PXE)[4]	X	X	Rebooting the System to Preboot Execution Environment on page 152
Rebooting or powering to more discreet sleep states[4]		X	Booting to DASH-only Supported Power States on page 153
Text Console Redirection	X	X	Remote Operations on page 74
Device Group Management	X		Group Management on page 163
Event Management	X		Viewing the vPro Event Log on page 140, Viewing vPro Event Filters on page 140, Alert Notifications on page 171

Table 4 Management Operations on Out of Band Devices (cont'd)

Management Operation	vPro	DASH	Where to Find Information
System Defense	X		Managing System Defense Filters on page 103, Managing System Defense Policies on page 106
Agent Presence	X		Managing Agent Watchdogs on page 114
Heuristics Worm Containment	X		Managing Heuristics Information on page 110
Front Panel Settings Configuration	X		Configuring Front Panel Settings on the vPro Device on page 160
Flash Limit Reset	X		Resetting the Flash Limit on the vPro Device on page 160
Boot Settings Configuration		X	Configuring the Boot Settings on the DASH Device on page 161

1. Provisioning Configuration: There are multiple ways to provision vPro devices. The HPCA Console 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.
2. 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).
3. 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.
4. Power and Reboot Operations: Refer to the Mapping Power Operations to Power States on page 137.

5 Out of Band Management Use Case Scenarios

This chapter explains how you can use the HPCA 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 mal-ware attacks. You can use the HPCA 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 HPCA Console in your enterprise but rather serve as illustrative examples.

This chapter is divided into two major sections:

- Conceptual Overview: Before describing the use cases, some conceptual information is presented to provide some context for these tasks.
- Use Cases: The procedures necessary to perform end-to-end use case scenarios are presented.

Conceptual Overview

As a result of your configuration and installation activities, you have:

- Provisioned the vPro devices by using the SCS console to access the SCS server
- Provisioned the DASH devices according to the documentation for that device
- Installed and configured the HPCA Console so that it can communicate with the SCS to obtain a device list of all the provisioned vPro devices.

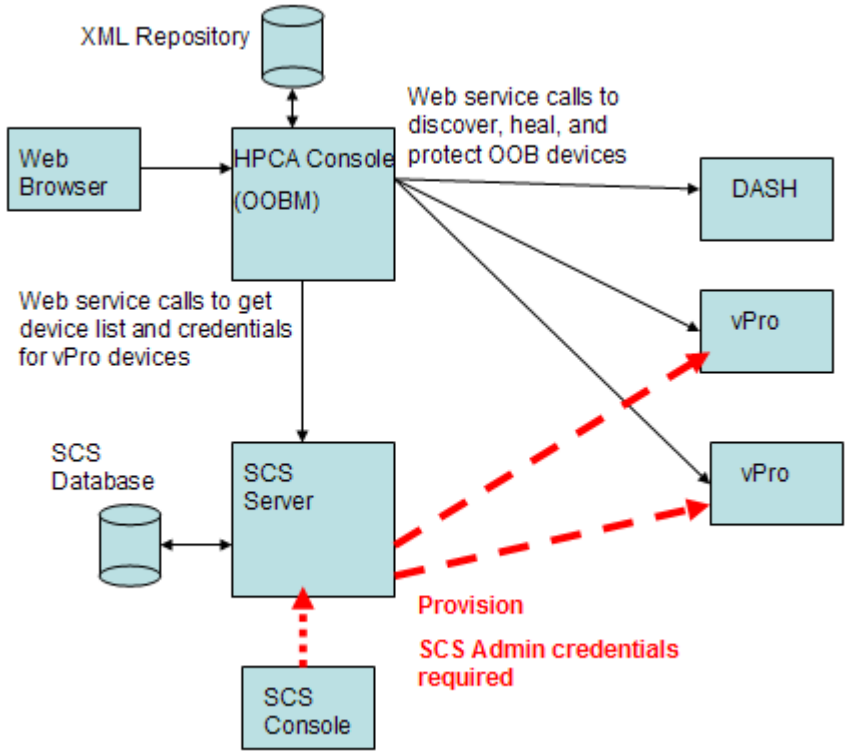
DASH devices are discovered through HPCA Console by specifying IP or Active Directory information.

It is now possible for you to do the following:

- Log into the HPCA Console through a web browser interface
- Perform supported discover, heal, and protect operations (based on device type) on the provisioned devices in your network through the OOBM options in the console.

The following diagram highlights the main components in this management solution and shows how they communicate with each other.

Figure 7 Overview of Out of Band Management Components



The following sections describe in greater detail the OOBM features that allow you to Discover, Heal, and Protect the OOB devices on your network.

Protect scenarios are relevant to vPro devices only.

Discover

You can discover the Hardware Assets and Software Assets 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 HPCA 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 allows 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 HPCA 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 local agent running on the vPro device to monitor.
- View the system message that the local agent will display to the console of the vPro device if the Agent Presence policy is activated.

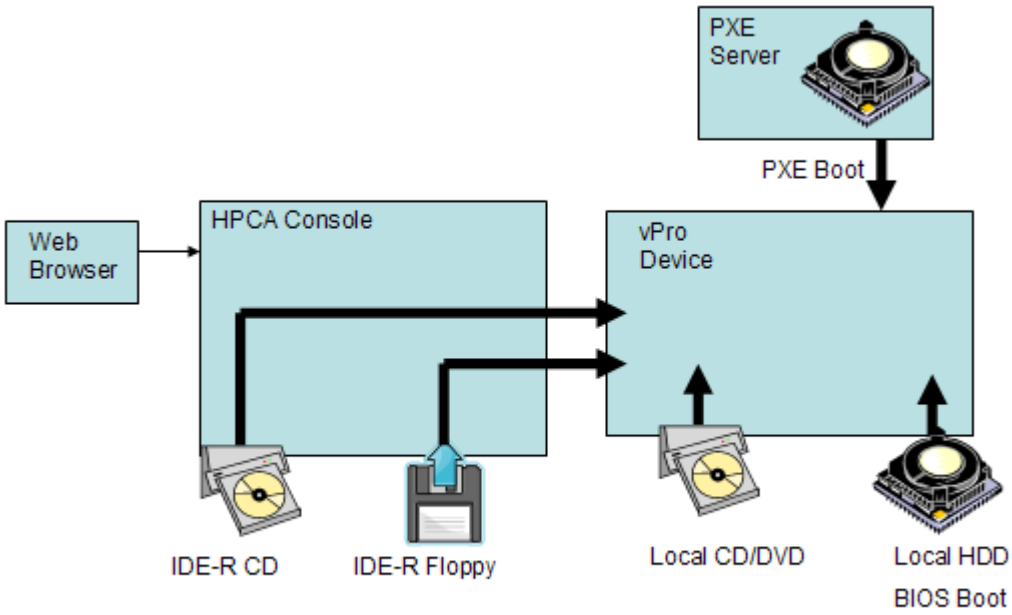
Heal

Heal operations include Remote Operations and Event Management.

Event Management is relevant to vPro devices only.

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

Figure 8 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 HPCA 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
- Rebooting OOB devices using console text redirection and IDE-R

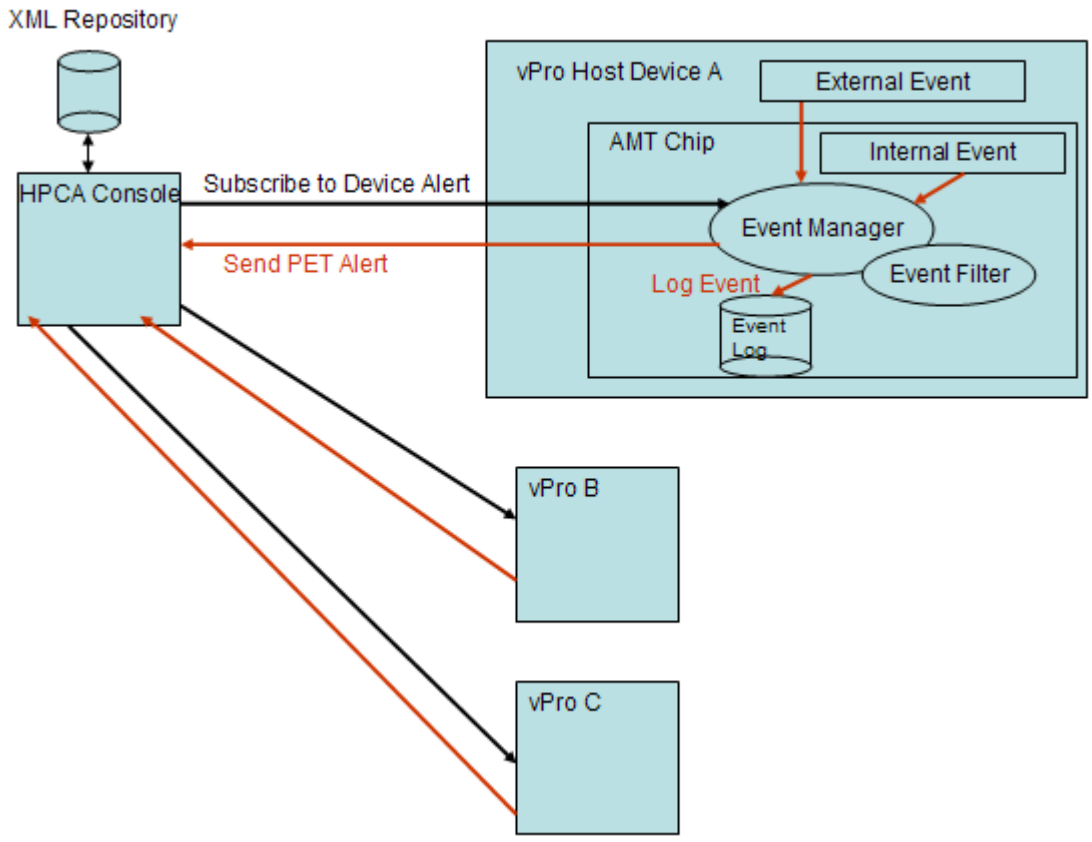
Integrated drive electronic redirect (IDE-R) is available on vPro devices only.

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

Event Management

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

Figure 9 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 generated from external sources such as the System Management (SM) bus and hardware sensors. There are also internal, vPro-self generated

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 HPCA Console, logging the event in the vPro log, or both.

You must subscribe to a vPro device for event alerts generated by that device to be sent to the HPCA 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 HPCA Console.

Intel vPro devices come with a set of default event filters built in to their firmware chip. The HPCA Console also allows 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 allow 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 local agents running on the devices in your network. It also allows you to quarantine worm-infected devices by providing a mechanism that continuously observes outgoing traffic to detect and impede the proliferation of worms.

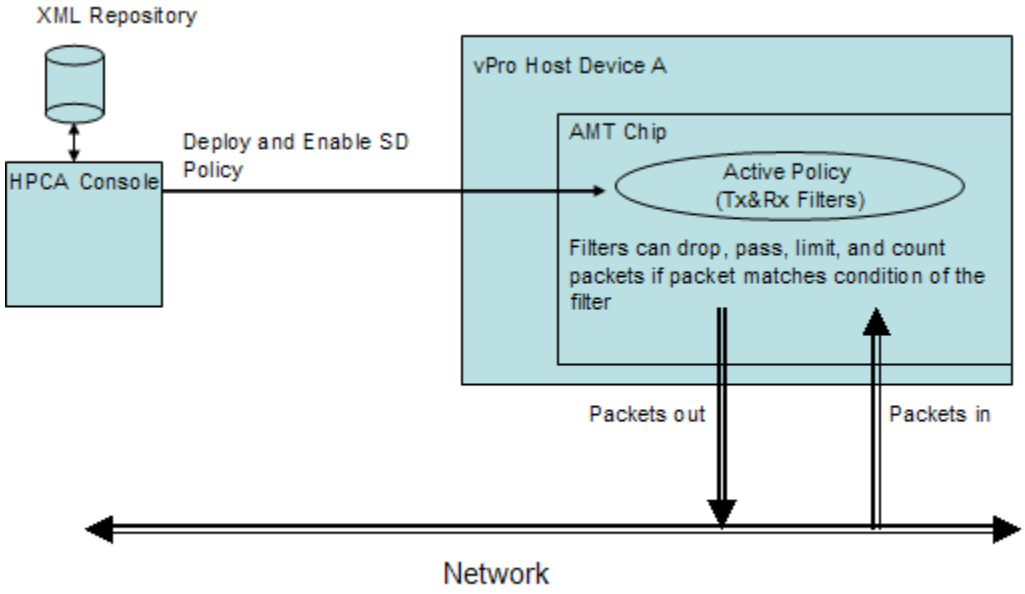
These topics are discussed in the following sections:

- System Defense
- Agent Presence
- Network Outbreak Containment Heuristics

System Defense

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

Figure 10 System Defense Overview



Policies

The System Defense vPro capability allows the HPCA 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 allows for selective network isolation of Ethernet and IP protocol flows based on the filters associated with a policy. These filters allow 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 HPCA 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 HPCA 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 agent watchdog action. This is discussed in greater detail in Agent Presence on page 77. The enabled policy with the higher priority becomes the active policy for the device. Once 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 local 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 generated.
- **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.

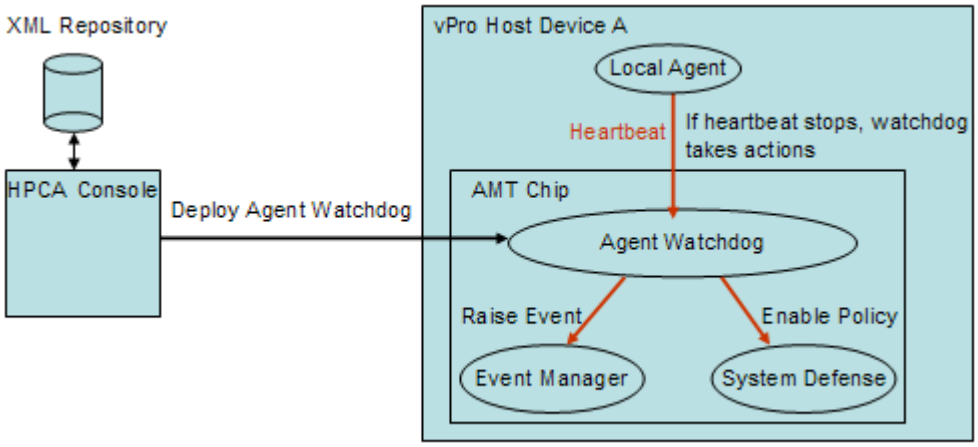
Intel vPro supports 32 filters in Receive (Rx) mode and 32 filters in Transmit (Tx) mode. One each of the filters in 32 Tx and Rx modes is used as the Else (non-matching) filter. If anti spoofing is enabled, it utilizes one of the filters in Tx mode. This reduces the available filters for a vPro device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

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 diagram shows the components involved when monitoring for the presence of a local agent on a vPro host device.

Figure 11 Agent Presence Overview



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

Local agents are discussed in greater detail in the Local Agents on page 79.

Watchdogs

The actions an agent watchdog can take are the following:

- 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 HPCA Console if it has been subscribed to.

You can use the HPCA Console to do the following:

- Create an agent watchdog
- Specify timers to detect when the local agent initializes and periodically transmits “heartbeat” signals to its agent watchdog
- Specify transition states for the local agent that will trigger the watchdog actions. Valid states include the following:
  - not started
  - stopped
  - running
  - expired
  - suspended
- Set the actions for the agent watchdog to take if the transition criteria are met (namely, enable Agent Presence policy and/or enable event logging)
- Deploy (and undeploy) the agent watchdog to multiple vPro devices

- Create the list of applications to be monitored by the local agent
- Create the message that will be displayed upon activation of the Agent Presence policy

Local Agents

As indicated, the local agent secures the vPro device by monitoring the state of any critical applications running on the device. The list of applications that the local agent monitors is user-defined. If a monitored application stops running, the local 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.

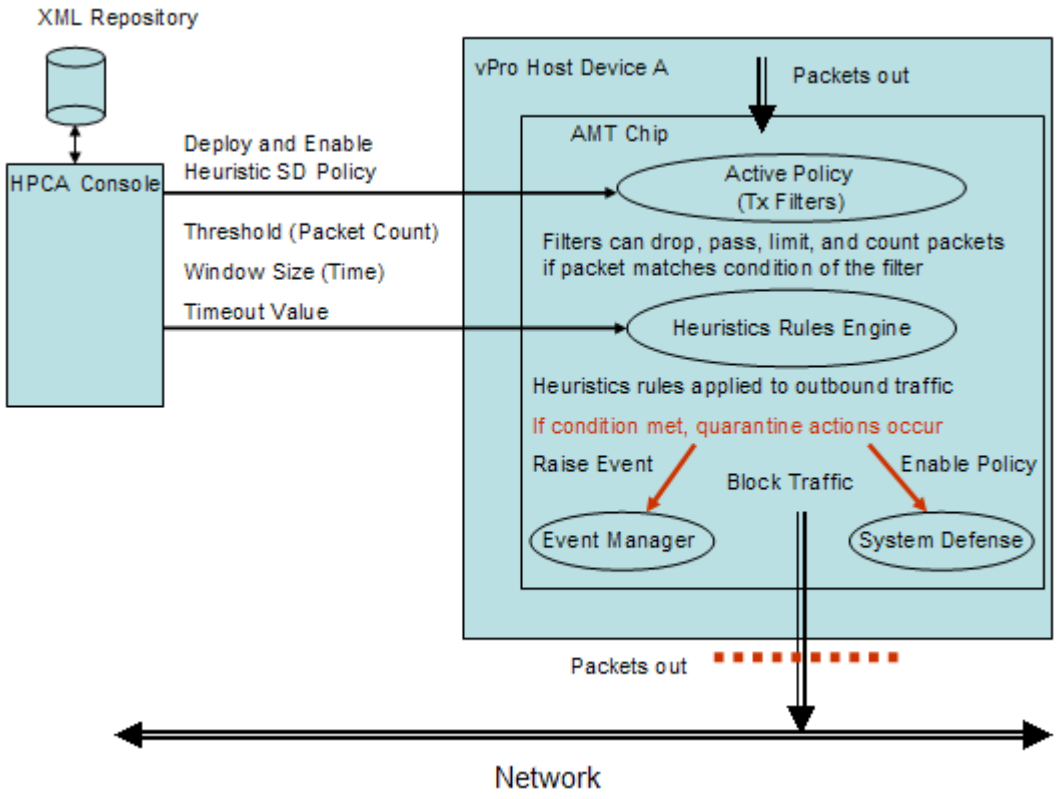
When the local agent is installed (and the software list of applications has been created and deployed to the device), it is automatically started as an NT service. Once started, the local agent does the following:

1. Registers with the agent watchdog.
2. Gets the heartbeat interval from the vPro chip and starts sending heartbeats to the agent 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 agent watchdog and displays the user-defined system message that it reads from the 3PDS.

Network Outbreak Containment Heuristics

The following diagram shows the architectural overview of a worm-containment system.

Figure 12 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.

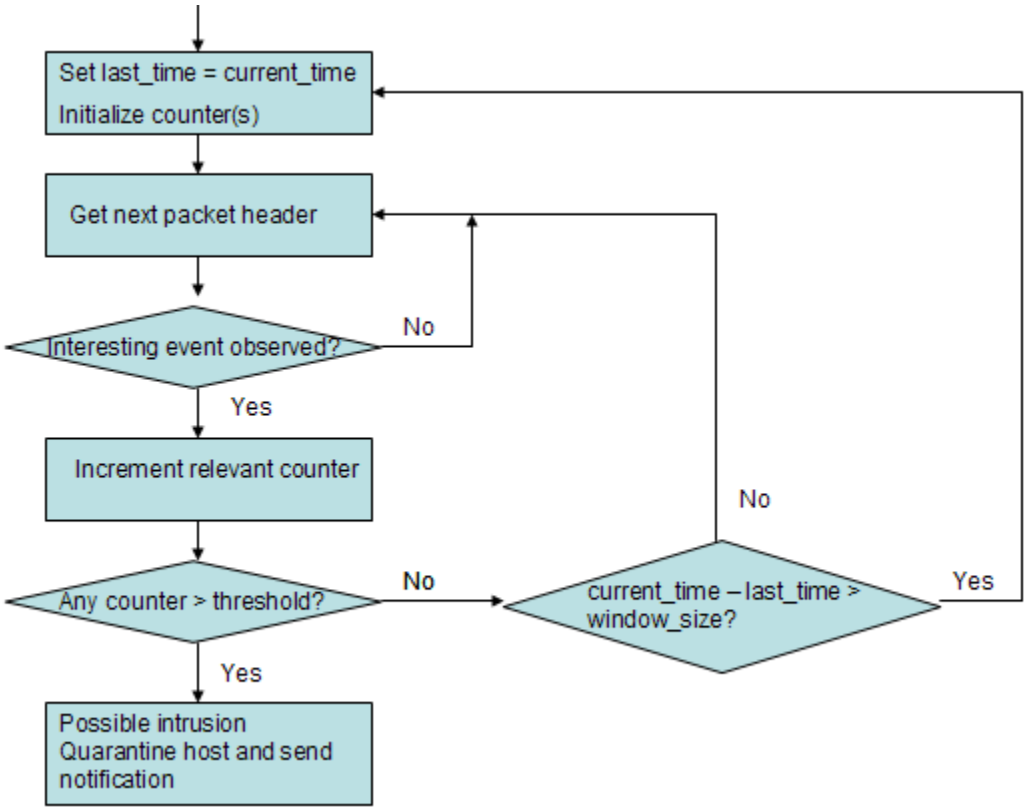
The Heuristics Rules Engine analyzes the traffic. If the Heuristics Rules Engine detects evidence of anomalous traffic, it can perform any of the following actions:

- 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 diagram shows the basic mechanism employed by all heuristics.

Figure 13 Basic Operation of Heuristics



For additional information, refer to the Intel study on a heuristics-based worm-containment system at the following URL: **http://www.intel.com/technology/comms/download/worm_containment.pdf**.

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 HPCA Console allows 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.

The recommended configurations for window sizes and threshold combinations are the following:

- Fast: 8 packets in 10 milliseconds
- Slow: 64 packets in 50 seconds

Containment Actions and Timeout Values

The HPCA Console also allows you to specify the autonomous actions the system should take if the thresholds are exceeded. As indicated on page 80, 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 HPCA 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 HPCA Console.

Use Cases

The following use cases are described in this section:

1. Hardware Failure and Replacement
2. Operating System Failure and Reboot
3. Virus Infection Detection and Quarantine
4. Device Quarantine and Remediation
5. Monitoring Critical Software
6. Worm Infection and Containment

Most of the use cases described here are relevant to vPro devices. DASH devices are mentioned wherever applicable. However, the navigation and procedureal details may vary for DASH devices. Refer to the Device Management chapter for detailed procedural information.

1. Hardware Failure and Replacement

This use case is divided into the following sections:

- Overview
- Use Case Steps

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 HPCA 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 HPCA 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 Steps

To subscribe to vPro devices for event alert notifications

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 checking the checkbox for the device or by checking the select all checkbox in the upper left.
3. From the  alert subscription management icon pull-down list, select **Subscribe to Alerts**.

See Alert Subscription Management on page 132 for more details.

To view alerts

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 HPCA Console. In this case, you are specifically looking for event alerts caused by hardware failures.

See Viewing Alerts on the vPro Device on page 171 for more details.

To view hardware assets

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.

See Viewing Hardware Assets on page 141 for more details.

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

2. Operating System Failure and Reboot

This use case is divided into the following sections:

- Overview

- Use Case Steps

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 HPCA Console Server to further diagnose the problem

Use Case Steps

To lock the front panel on the vPro device

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**.

See Configuring Front Panel Settings on the vPro Device on page 160 for more details.

To reboot the system with IDE-R CD Drive

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.

See Rebooting the vPro System with IDE-R on page 148 for more details.

3. Virus Infection Detection and Quarantine

This use case is divided into the following sections:

- Overview
- Use Case Steps

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 HPCA 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 allowed 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. Once 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

To subscribe to vPro devices for event alert notifications

Follow the steps in To subscribe to vPro devices for event alert notificationsin use case 1. Hardware Failure and Replacement.

To view alerts

Follow the steps in To view alertsin use case 1. Hardware Failure and Replacement. In this case, you are specifically looking for event alerts triggered by a rate limit filter.

To create the quarantine filter

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**.

See Managing System Defense Filters on page 103 for more details.

To create the quarantine policy

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**.

See Managing System Defense Policies on page 106 for more details.

To enable, activate, and deploy the Quarantine policy to the vPro device

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.

See Managing System Defense Policies on page 106 for more details.

To deactivate the Quarantine policy from the vPro device

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.

See Managing System Defense Policies on the vPro Device on page 156 for more details.

4. Device Quarantine and Remediation

This use case is divided into the following sections:

- Overview
- Use Case Steps

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 HP 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 HP 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 go through the following procedure 4 times, once for each filter you need to create.

To create the remediation filters

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:

Table 5

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:

Table 6

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**.

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.

See the Managing System Defense Filters on page 103 for more details.

To create the remediation policy

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**.

See Managing System Defense Policies on page 106 for more details.

To enable, activate, and deploy the remediation policy to the vPro device

Follow the steps in To enable, activate, and deploy the Quarantine policy to the vPro device in use case 3. Virus Infection Detection and Quarantine. In this case, select the Remediation policy.

To deactivate the Remediation policy from the vPro device

Follow the steps in To deactivate the Quarantine policy from the vPro device in use case 3. Virus Infection Detection and Quarantine. In this case, select the Remediation policy.

5. Monitoring Critical Software

This use case is divided into the following sections:

- Overview
- Use Case Steps

Overview

A local agent is installed and started on a vPro device to monitor a list of security software applications, a monitored security application stops, and the local agent stops sending heartbeats to the watchdog. This transition state causes the watchdog to take the actions that the administrator specified when creating the agent 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 local agent failure and set this policy as the Agent Presence policy
- Create the agent watchdog and specify its actions
- Deploy the Agent Presence policy and watchdog to the vPro device
- Manage local agent settings and deploy the settings to the vPro device
- Install the local agent on the vPro host operating system (the local agent is started automatically by the installer.
- Restart the security process after the event alert is sent:

After the local 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 local agent was monitoring. Once the security software is restarted, the local 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

To view the Even Filter for the vPro device

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.

See the Viewing vPro Event Filters on page 140 for more details.

To subscribe to vPro devices for event alert notifications

Follow the steps in the To subscribe to vPro devices for event alert notificationsin a previous use case.

To create a filter for the Agent Presence policy

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**.

See Managing System Defense Filters on page 103 for more details.

To create the Agent Presence policy

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**.

See Managing System Defense Policies on page 106 for more details.

To set and deploy the Agent Presence policy to the vPro device

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 local 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 agent watchdog if the local 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.

See Managing System Defense Policies on page 106 for more details.

To create the agent watchdog

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 agent watchdog. The Agent Watchdog wizard opens.
3. Click **Next** to continue. In this window, specify the following:
   - **Agent Type**: Select **HP local agent**.
   - **Name**: Enter **AlphaWatchdog**.

— **Agent GUID**: This field is grayed out for the HP local agent because the GUID for the HP local 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 local agent transition occurs.

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

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

See Managing Agent Watchdogs on page 114 for more details.

To deploy the agent watchdog to the vPro device

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 Check the box next to AlphaWatchdog.

3 Click the  deploy agent watchdog icon on the toolbar. The Watchdog 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 local agent.

6 Follow the remaining steps in the wizard.

See Managing Agent Watchdogs on page 114 for more details.

To configure the system message and software list

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  local 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 local 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.

See To configure the system message and software list on page 117 for more details.

To deploy the system message and software list

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. Check the checkbox next to the vPro device that will be running the local agent.
7. Click **Next** and follow the remaining steps of the wizard.

See To deploy the system message and software list on page 117 for more details.

To install and start the local agent on the vPro device

1. Copy the `oobmclocalagent.msi` file located in the `Media\oobm\win32\LocalAgent` directory on the HPCA 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. See Configuration Client Role on page 42 in the SCS and vPro Setupchapter for more details about this role.
   - **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 allows 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 check 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.

See Installing the OOBM Local Agent on page 42 in the SCS and vPro Setup chapter for more details.

The local agent is an NT service and starts as soon as it is installed.

All of the applications on the software list that the local agent will monitor msut be runnng when the local agent starts. If not, the local agent will shut down the watchdog as soon as it starts.

To activate the Agent Presence policy on the vPro device

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

To send the alert

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

To view alerts

Follow the steps in the To view alerts in a previous use case. In this case, you are looking for event alerts caused by local agent failure.

To restart the security process

Enter the command line or double-click the executable file that invokes the security application.

To deactivate the Agent Presence policy on the vPro device

After the local 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.

6. Worm Infection and Containment

This use case is divided into the following sections:

- Overview
- Use Case Steps

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.

Once 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

To subscribe to vPro devices for event alert notifications

Follow the steps in To subscribe to vPro devices for event alert notifications section in a previous use case.

To create an heuristics specification

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.

    See Window Size and Threshold Values on page 81 and Containment Actions and Timeout Values on page 82 for more details.
- **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.

See Managing Heuristics Information on page 110 for more details.

To deploy the heuristics specification

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.

See Managing Heuristics Information on page 110 for more details.

To view alerts

Follow the steps in the To view alerts section in a previous use case. In this case, you are looking for event alerts caused by the Heuristics Rules engine.

6 Administrative Tasks

This chapter describes the Out of Band Management (OOBM) tasks you can perform in the role of Administrator through the HPCA Console. These tasks include the following:

- Enablement
- Device Type Selection
- vPro System Defense Settings

Enablement

You can turn on OOBM functionality through the HPCA Console.

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

To enable OOBM

1. Log into HPCA 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 back into the HPCA Management Console.

When you log back into the HPCA Management Console, you will see additional OOBM options as described in the following Configuration, Operations, and Managementsections.

Configuration

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, another option may appear. See vPro System Defense Settings.

Operations

Out of Band Management will now be visible in the left navigation pane on the **Operations** tab.

Your Device Type Selection determines the options you will see under Out of Band Management. See Operationsin the Getting Started Managing OOB Devices chapter.

Management

You will now be able to access OOB Device Details directly from the **Management** tab of the HPCA console.

This is in addition to the way you can normally access it from the **Operations** tab as described in the Device Management and Group Management chapters in this guide.

Client Automation Enterprise

There are a number of ways you can access the OOB Device Details from the **Management** tab in CAE.

Devices 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.

Devices 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.

Devices 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.

Devices going through 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.
3. You can use any of the preceding device procedures, namely Devices using Device Pull-down Menu, Devices using the OOB Device Details Icon, Devices using the View/Edit Properties Icon to access the Out of Band Device Details window.

Client Automation Standard

There are a number of ways you can access the OOB Device Details from the **Management** tab in CAS.

Device Management using OOB Device Details Icon

1. Click **Device Management** in the left navigation pane on the **Management** tab. The Device Management window opens.
2. Select the **Devices** tab. In the toolbar on the Device table, 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.

Device Management using Device Name Link

1. Click **Device Management** in the left navigation pane on the **Management** tab. The Device Management window opens.
2. Select the **Devices** tab.
3. Click a device name link in the Device table. The Device Details window opens.
4. Select the **General** tab.
5. Under Tasks, click **Out of Band**. If the device supports OOBM, the Out of Band Device Details window opens. Otherwise, an error message is displayed.

Group Management using OOB Device Details Icon

1. Click **Group Management** in the left navigation pane on the **Management** tab. The Group Management window opens.
2. Select the **Groups** tab.
3. Click a group name link in the Group table. The Group Details window opens.
4. Select the **Devices** tab. In the toolbar on the Device table, the Out of Band Details icon appears. Proceed as described inDevice Management using OOB Device Details Icon.

Software Management using OOB Device Details Icon

1. Click **Software Management** in the left navigation pane on the **Management** tab. The Software Management window opens.
2. Follow the same general procedure as in Group Management using OOB Device Details Icon only selecting the **Software** tab in step 2.

Patch Management using OOB Device Details Icon

1. Click **Patch Management** in the left navigation pane on the **Management** tab. The Patch Management window opens.
2. Follow the same general procedure as in Group Management using OOB Device Details Icon only selecting the **Patches** tab in step 2.

OS Management using OOB Device Details Icon

1. Click **OS Management** in the left navigation pane on the **Management** tab. The OS Management window opens.
2. Follow the same general procedure as in Group Management using OOB Device Details Icon only selecting the **Operating Systems** tab in step 2.

Device Type Selection

This option tells Out of Band Management the types of OOB devices you want to manage. Depending on the device type(s) that you choose, the HPCA Console displays an interface relevant to that selection. It is possible to make one of three choices for device type, DASH Devices, vPro Devices, or Both.

To select the device type

1. Log into HPCA Console and select the **Configuration** tab.
2. Under **Out of Band Management**, click **Device Type Selection**. The Device Type Selection window opens.
3. For DASH devices, check **Manage Dash Devices**. 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.
4. For vPro device, check **Manage vPro Devices**. 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
5. 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.
6. Log out and log back into the HPCA Console to see the Out of Band Management options that are now available on the **Configuration** and **Operations** tab reflecting your device type selection.

vPro System Defense Settings

If you have chosen to manage vPro devices on the Device Type Selection window, you will see this option on the **Configuration** tab after you log back into the HPCA Console. This option allows you to manage System Defense settings for vPro devices. These include the following:

- Managing System Defense Filters

- Managing System Defense Policies
- Managing Heuristics Information
- Managing Agent Watchdogs

Managing System Defense Filters

You can use the HPCA Console to view, create, update, and remove System Defense filters for vPro devices in the System Defense filters repository.

System Defense filters are assigned to System Defense policies. The filters become activated when their corresponding policy becomes the active policy.

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

Table 7 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

To refresh the System Defense filter view

1 Log in to the HPCA 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 HPCA Console.

3 Click the  refresh icon on the toolbar.

To add System Defense filters

1 Log in to the HPCA 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 HPCA 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 HPCA 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 allows 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 allows 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 allows 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 allows 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. See Port Determination Table on page 105.

Destination Port Range: This option allows 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. See the Port Determination Table on page 105.

Table 8 Port Determination

		Filter Mode	
		Packets Transmitted from vPro Device	**Packets Received by vPro Device**
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	Refers to the ports on the remote device or devices. Packets are filtered from this source port range on the remote source device or
	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.

To update System Defense filters

1 Log in to the HPCA 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 HPCA 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.

To remove System Defense filters

1 Log in to the HPCA 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 HPCA 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 HPCA 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. When a policy becomes the active policy, the filters associated with this policy become activated.

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

Table 9 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

To refresh the System Defense policy view

1 Log in to the HPCA 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 HPCA Console.

3 Click the refresh icon on the toolbar.

To add System Defense Policies

1 Log in to the HPCA 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 HPCA 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.

To update System Defense policies

1 Log in to the HPCA 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 HPCA 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.

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

To deploy System Defense policies

1 Log in to the HPCA 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 HPCA 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.

To undeploy System Defense policies

1 Log in to the HPCA 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 HPCA 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.

To set the Agent Presence policy

1. Log in to the HPCA 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 HPCA 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.

To enable System Defense policy

1. Log in to the HPCA 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 HPCA 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.

To remove System Defense policies

1. Log in to the HPCA 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 HPCA 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 HPCA Console to view, create, update, remove, and add actions to heuristic information. These heuristics can then be deployed to multiple vPro devices.

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

Table 10 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

To refresh the heuristics view

1 Log in to the HPCA 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 HPCA Console.

3 Click the  refresh icon on the toolbar.

To add heuristics

1 Log in to the HPCA 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 HPCA 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.

See Window Size and Threshold Values on page 81 and Containment Actions and Timeout Values on page 82 for more details.

- **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.

To update heuristics

1 Log in to the HPCA 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 HPCA 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.

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

To deploy agent heuristics

1 Log in to the HPCA 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 HPCA 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.

To undeploy heuristics

1 Log in to the HPCA 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 HPCA 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.

To remove heuristics

1 Log in to the HPCA 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 HPCA 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 in order to contain the worm.
- Remove heuristic information that is no longer needed.
- Deploy (and undeploy) heuristics to multiple vPro devices.

Managing Agent Watchdogs

You can use the HPCA Console to view, create, update, remove, and add actions to agent watchdogs in the watchdog repository. These watchdogs can then be deployed to multiple vPro devices. 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 local agent to monitor.

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

Table 11 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
	Undeploys selected watchdogs from vPro devices
	Deletes watchdogs from the repository
	Configures the local agent system message and software list
	Deploys the local agent system message and software list

To refresh the agent presence view

1 Log in to the HPCA 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 HPCA Console.

3 Click the  refresh icon on the toolbar.

To add an agent watchdog

1 Log in to the HPCA 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 HPCA Console.

3 Click the  add icon to create an agent watchdog. The Agent Watchdog Wizard opens.

4 Click **Next** to continue. In this window, specify the following:

— **Agent Type**: Select HP local agent or third party vendor agent to specify which agent you have installed on the vPro device. The HP local agent is selected by default.

— **Name**: Enter a unique name for the agent watchdog.

— **Agent GUID**: Enter the GUID for a third party vendor agent. This field is grayed out if you have selected the HP local agent because the GUID for the HP local agent is known.

— **Heart Beat Interval**: Enter the time between heartbeats from the local agent to the agent 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 agent 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 local agent that will trigger the actions.

To: Select the final state for the local 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 local 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 then 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 local 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 HPCA 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 agent watchdog is displayed in the Agent Watchdogs table with the number of actions count properly set. The watchdog and actions are applied to the repository.

To update agent watchdogs

1 Log in to the HPCA 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 HPCA Console.

3 Click the agent watchdog name link of the watchdog you want to modify in the Watchdog Name column of the agent watchdogs table. The Agent 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 step 5 in the To add an agent watchdog on page 114.

— Remove actions by checking the 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.

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

To deploy agent watchdogs

1 Log in to the HPCA 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 HPCA Console.

3 Check the box next to each watchdog that you want to deploy. You can deploy only one HP local agent watchdog. You can deploy multiple third party agent watchdogs, one per third party local agent running on the vPro device.

4 Click the  deploy agent watchdog icon on the toolbar. The Watchdog 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 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.

To undeploy agent watchdogs

1 Log in to the HPCA 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 HPCA Console.

3 Check the box next to each agent watchdog that you want to undeploy.

4 Click the  undeploy agent watchdog icon on the toolbar. The Watchdog 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 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.

To remove agent watchdogs

1 Log in to the HPCA 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 HPCA Console.

3 Check the 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 Agent Watchdog table and are also undeployed from the provisioned vPro devices

To configure the system message and software list

1 Log in to the HPCA 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 HPCA Console.

3 Click the  local 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 upon 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 local agent to monitor. For example, you can enter **symantec.exe**.

> 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 local 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.

To deploy the system message and software list

1 Log in to the HPCA 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 HPCA 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 local 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**.

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

You can use the agent watchdog interface to:

- Define a watchdog agent to monitor a local agent on the vPro device.
- Configure heartbeat rate and startup interval for the local agent when it is being monitored by the watchdog.
- Remove an agent watchdog that is no longer needed.
- Deploy (and undeploy) agent 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 local agent to monitor on the target vPro device.

7 Provisioning vPro Devices

This chapter provides an Overview about provisioning vPro devices and describes Delayed Remote Configuration of the vPro Device.

Overview

Through the HPCA Console, you can provision vPro devices that were not provisioned during the initial Setup and Configuration Service (SCS) provisioning process. The initial provisioning process is described in SCS and vPro Setup on page 17 and is referred to as bare metal Remote Configuration.

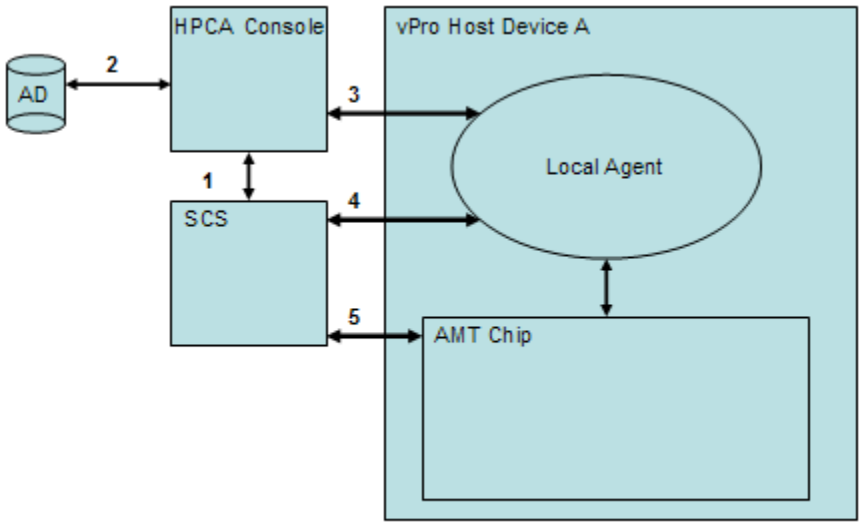
The type of provisioning performed through the HPCA Console is referred to as delayed Remote Configuration provisioning. It is considered *remote* configuration because you do not have to manually install a PID/PPS pair or enter information about the provisioning server address, the domain name, and 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 allowed for that device when it was initially connected to the network.

In order to use Remote Configuration, you must follow all of the requirements discussed in Configuring the vPro Device through Remote Configuration on page 38 in the SCS and vPro Setup chapter.

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 HPCA Console communicates with the local agent running on the vPro device, the SCS server, and the Active Directory.

Figure 14 Delayed Remote Configuration through HPCA Console



The communication exchange is the following:

1 HPCA Console communicates with SCS to get a list of already provisioned devices and devices that are currently being provisioned.

2 HPCA 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 HPCA Console tries to communicate with the local agent on the default port. If the agent is installed, the devices are displayed with a status of unprovisioned in the HPCA Console. Once communication is established with the local agent, the HPCA Console requests that the local agent start the delayed configuration process.

4 If the device is not provisioned or in the in-provisioning state, the local agent tries to contact SCS to store the FQDN, UUID and Profile ID of the device. The hello packets are then generated.

5 SCS provisions the vPro device using the PKI-CH protocol.

Delayed Remote Configuration of the vPro Device describes the details of this process.

Delayed Remote Configuration of the vPro Device

This section covers the following topics:

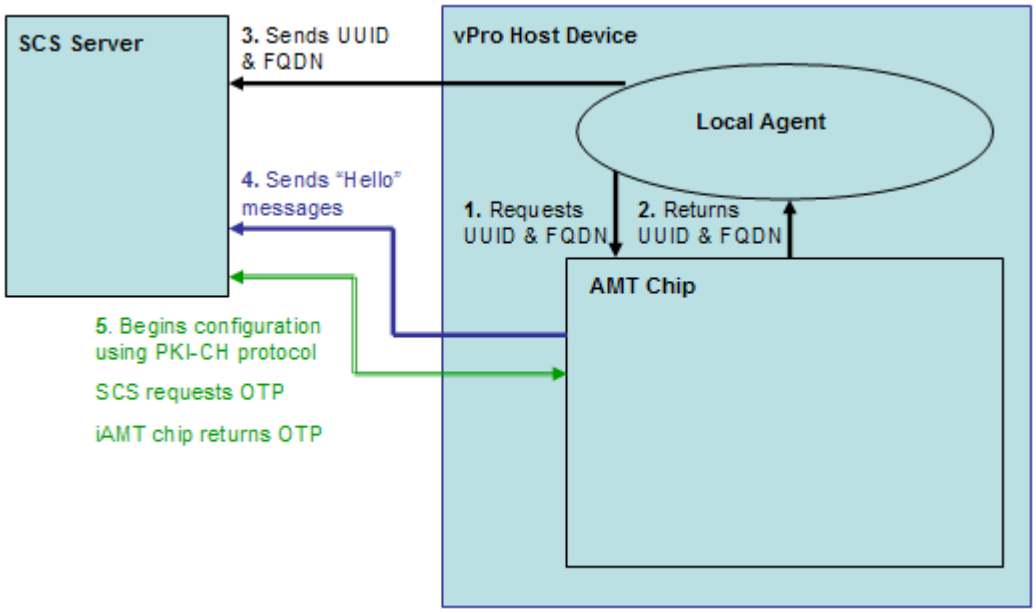
- Transitioning to Setup Mode
- Remote Configuration Provisioning Process
- Performing Provisioning Tasks

Transitioning to Setup Mode

The following diagram shows the steps involved in transitioning the vPro device to Setup mode when using the local agent for Remote Configuration. This is referred to as *delayed* configuration because the device was not provisioned immediately upon being connected to the network. See Bare Metal Remote Configuration of the vPro Device on page 40 for an explanation of this alternative (immediate) configuration.

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.

Figure 15 Transitioning to Setup Mode in Delayed Configuration



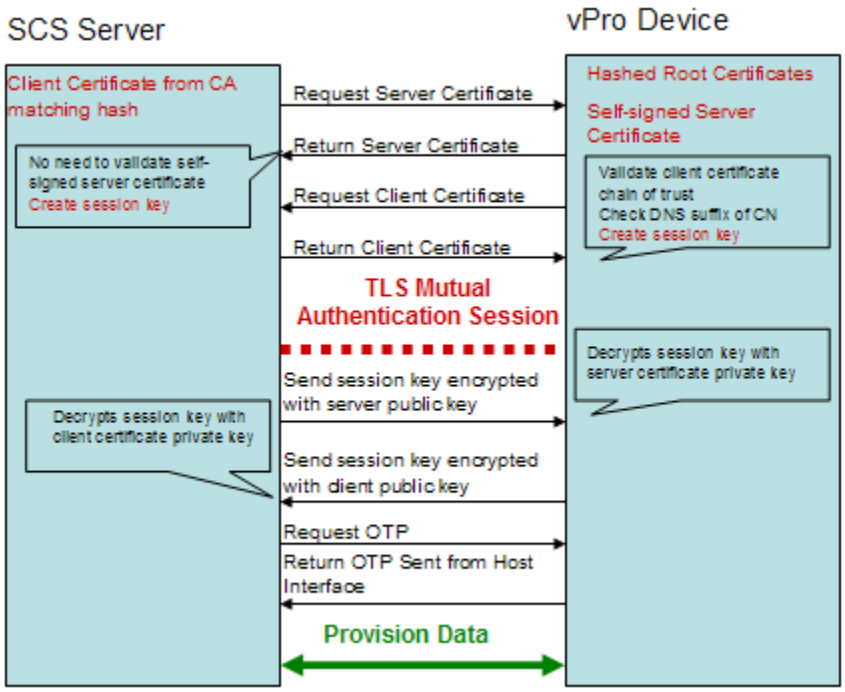
The local agent must be installed on the vPro host device. The local agent detects the vPro device and the following occurs:

1. The local agent requests the UUID and FQDN from the vPro device.
2. The vPro device returns these values to the local agent.
3. The local 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.

Figure 16 Remote Configuration Provisioning Process



The provisioning process includes the following steps:

1 The local 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 (configurable) the first time only that it is enabled. If the time runs out before setup and configuration completes, any subsequent calls from the local agent to start configuration will open 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 as described in Acquiring and Configuring a Certificate for Remote Configuration on page 40 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 and it creates another session key, which it encrypts with the client public key that the SCS Server sent it 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 in order to complete the configuration process.

Performing Provisioning Tasks

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

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

This option allows 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 provisioning 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 provisioning server's IP address and name have changed. It allows you to clear everything and proceed with fresh provisioning.

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

- Install the local agent on the vPro device if you have not done so already. See Installing the OOBM Local Agent on page 42.
- If additional security is required as part of your network security policy, go back into the SCS setup and enable one-time password (OTP). See To configure the profile on page 34.

To provision the vPro device

1 Log into the HPCA 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 HPCA 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. Upon 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 local agent on the vPro device are displayed.

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.

To reprovision the vPro device

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.

To partially unprovision the vPro device

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.

To fully unprovision the vPro device

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.

8 Device Management

This chapter tells you how to manage OOB devices through the HPCA 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 HPCA Console is **Device Management**. This option allows:

- Managing Multiple Devices
- Managing Individual Devices on page 135

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 allow 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.

Table 12 Device List Toolbar

Icon	Function
	Refreshes the OOB device information displayed in the list from the information stored in the OOBM Database
	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

Table 12 Device List Toolbar (cont'd)

Icon	Function
	Deploys System Defense policies to selected vPro devices
	Deploys heuristics worm containment information to selected vPro devices
	Deploys agent watchdogs to selected vPro devices
	Deploys agent software list and system message to selected vPro devices

When you log in to the HPCA 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.

As indicated in the device list toolbar table, the discovery icon allows 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. 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 `<HPCA_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 allows 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 HPCA 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

1. Login into the HPCA 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 Discover Devices Wizard opens.
4. Click **Next** to continue, The Discovery Options window opens.
5. The device type you selected on the **Configuration** tab of the HPCA 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

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 HPCA Console makes calls to each of the devices in order 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 HPCA 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 HPCA 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 checking the checkbox for the device or by checking the select all checkbox 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 HPCA 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.

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 102.

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.

To specify individual credentials for DASH devices

1 Log into the HPCA 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 **Operator** 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.

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 HPCA Console.

Refreshing Device Information

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

To refresh device information

1 Select the OOB devices you want to manage as described in the To select multiple devices procedure.

2 Click the  reload device information icon. The device information displayed for the selected devices in the HPCA Console will now be synchronized with the information stored on the OOB device.

If there are no System Defense policies in the HPCA 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.

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

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

1. Select the OOB devices you want to manage as described in the To select multiple devices procedure.
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

1. Select the vPro devices you want to manage as described in the To select multiple devices procedure.
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 HPCA Console.

Management of Common Utilities

The common utilities icon on the toolbar allows 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 HPCA Console:

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

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

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.

To reset the flash limit on multiple vPro devices

1. Select the vPro devices you want to manage as described in the To select multiple devices procedure.
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 allows 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

1. Select the vPro devices you want to manage as described in the To select multiple devices procedure.
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.

   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 mal-ware attacks.

Deployment of Heuristics

To deploy heuristics to multiple devices

1. Select the vPro devices you want to manage as described in the To select multiple devices procedure.
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 Agent Watchdogs

To deploy agent watchdogs to multiple devices

1 Select the vPro devices you want to manage as described in the To select multiple devices procedure.

2 Click the  agent watchdog deploy icon. The Agent 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 HP local agent watchdog. You can deploy multiple third party agent watchdogs, one per third party local 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 agent watchdogs to multiple vPro devices to monitor the local agents on these systems. Monitoring local 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

1 Select the vPro devices you want to manage as described in the To select multiple devices procedure.

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 local 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**.

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

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

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 allows you to do the following:

- View the power state as described on page 139
- View and clear the vPro Event log as described on page 140
- View the event filters on the vPro device as described on page 140
- View general asset information for vPro devices as described on page 141
- View hardware assets as described on page 141
- View a list of applications registered with the Third Party Data Store (vPro) or located in the network controller's NVRAM (DASH) as described on page 142
- Perform remote operations such as power up, power down, and reboot as described on page 143
- Perform KVM redirection in text or graphical mode as described on page 154.
- View and delete System Defense filters on vPro devices as described on page 155
- View, delete, and enable System Defense policies and set an Agent Presence policy on vPro devices as described on page 156
- View and delete heuristics information on vPro as described on page 158
- View and delete agent watchdogs on vPro devices as described on page 159
- Configure front panel settings on vPro devices during remote power operations as described on page 160

- Reset the flash limit on vPro devices as described on page 160

Refer to the Management Operations on Out of Band Devices Table on page 68 to be clear about the management operations that are supported per device type.

Viewing the 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.

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). Upon 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 allows 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 HPCA Console are mapped to the ACPI power states in the following table:

- 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.
- "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.

Table 13 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
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)

Table 13 Mapping Power Operations to Power States (cont'd)

vPro Power Operation	DASH Power Operation	Description	ACPI State
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 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

Table 13 Mapping Power Operations to Power States (cont'd)

vPro Power Operation	DASH Power Operation	Description	ACPI State
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 Supported	Power Cycle (Hard Graceful) Boot Source: *<boot_source>*	Mechanical off state (preceded by request to perform orderly shutdown) followed by Awake state	G0 to G3 with return to G0/S0
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

To view the power state of the OOB device

1. Log in to the HPCA 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.

The power state displayed is the last known state. This may not be the same as the current power state. In order to be sure that you are seeing the current power state, you must use the refresh icon next to the power state message.

Viewing the vPro Event Log

The **Diagnostics** area of the workspace allows 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 the vPro event log

1 Log in to the HPCA 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 allows 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 the vPro event filters

1 Log in to the HPCA 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 allows you to view general asset information about a remote vPro device regardless of its power state or general health.

To view general asset information

1 Log in to the HPCA 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 allows 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.

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

1. Log in to the HPCA 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.

   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 allows you to view the software assets on a remote OOB enabled device.

For vPro devices, this feature allows you to view the list of software applications that are being monitored by the local agent on the vPro device. See Managing Agent Watchdogs on page 114. This list is registered in the third party data storage (3PDS) on that device.

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

To view software applications

1. Log in to the HPCA 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 allow you to view the information for that application.

You can use this information to:

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

Changing the Power State

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

Refer to the Management Operations on Out of Band Devices Table on page 68 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 HPCA Console without user intervention or leaving the management console.

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, once 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 HPCA 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.

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 HPCA console. KVM functionality is not available on vPro machines with AMT prior to release 6.0. See KVM Redirection on vPro Devices on page 154.

On DASH devices, the HPCA 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.

To power up the device

1 Log in to the HPCA 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. See Configuring Front Panel Settings on the vPro Device on page 160 for more details.

— 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.

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. Refer to the Management Operations on Out of Band Devices Table on page 68 to see the mapping to the DASH remote operation.

Table 14 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. See Configuring the Boot Settings on the DASH Device on page 161. 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**.
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. See Configuring the Boot Settings on the DASH Device on page 161. 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**.

Table 14 Powering up a device (cont'd)

Drive/BIOS	Steps
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.
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.

Table 14 Powering up a device (cont'd)

Drive/BIOS	Steps
Primary Boot Device (vPro only)	1 From the pull-down menu next to **Remote Operation**, select **Power up to Primary Boot Device**. This option allows 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 allows you to see the operation displayed to the HPCA 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.

To power down the device

1 Log in to the HPCA 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 allows 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

1. Log in to the HPCA 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 Configuring the Boot Settings on the DASH Device Table on page 161.

   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. See Configuring Front Panel Settings on the vPro Device on page 160 for more details.

   — 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.

Table 15 Rebooting a device from a local drive

Drive	Steps
Local Hard Drive	1 From the pull-down menu next to **Remote Operation**, select **Reboot 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. See Configuring the Boot Settings on the DASH Device on page 161. 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**.

Table 15 Rebooting a device from a local drive (cont'd)

Local CD Drive	1 From the pull-down menu next to **Remote Operation**, select **Reboot 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. See Configuring the Boot Settings on the DASH Device on page 161. 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**.
Primary Boot Device (vPro only)	1 From the pull-down menu next to **Remote Operation**, select **Reboot to Primary Boot Device**. This option allows 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 allows you to see the operation displayed to the HPCA Console if you select to do so. 2 For **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 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.

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 the vPro System with IDE-R

The **Diagnostics** area of the workspace allows 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.

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

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 48 in the Out of Band Management Configuration chapter.

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.

To reboot the system with IDE-R

1. Log in to the HPCA 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 vPro device with IDE-R from various drives on a remote device as shown in the following table.

   Also in the Task window for vPro device, 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. See Configuring Front Panel Settings on the vPro Device on page 160 for more details.

Table 16 Rebooting a vPro device with IDE-R

Drive	Steps
IDE-R CD Drive (vPro only)	1 From the pull-down menu next to **Remote Operation**, select **Reboot to IDE-R**. The **IDE-R Option** is displayed. 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 reboot 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 **Reboot to IDE-R**. The **IDE-R Option** is displayed. 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 reboot process. This window stays open until you close it.

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
- Capture an image of a device for recovery or redeployment

Rebooting the vPro System to BIOS Settings

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

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

1. Log in to the HPCA 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.

   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. See Configuring Front Panel Settings on the vPro Device on page 160 for more details.

Table 17 Rebooting a vPro device to BIOS settings

BIOS	Steps
BIOS Setup (vPro only)	1 From the pull-down menu next to **Remote Operation**, select **Reboot 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 reboot process. This window stays open until you close it.
BIOS Pause (vPro only)	1 From the pull-down menu next to **Remote Operation**, select **Reboot 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 reboot process. This window stays open until you close it.

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 the System to Preboot Execution Environment

The **Diagnostics** area of the workspace allows 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.

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

1. Log in to the HPCA 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. See Configuring Front Panel Settings on the vPro Device on page 160 for more details.

   — 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. See Configuring the Boot Settings on the DASH Device on page 161.
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 HPCA 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 the Mapping Power Operations to Power States Table on page 137 table for a description of these operations and the power states to which they map.

The procedure in the HPCA 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.

To boot a DASH device using one of the preceding operations

1. Log in to the HPCA 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.

   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.
7. 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. See Configuring the Boot Settings on the DASH Device on page 161. This step is not relevant for the Power Off and sleep operations.
8. Click **Next.** The Confirmation Summary window opens. Review the information in this window.
9. Click **Next** to continue. Summary information displays to your management console.
10. 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 allows 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 HPCA console. The VNC Viewer uses port 5900.
- On the machine where you access the HPCA 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.

To perform KVM redirection on a vPro device

1. Log in to the HPCA 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.
   - Enter a time-out value in minutes for the KVM session. This value determines the amount of time that the KVM session will stay open. If the session times out, you will have to reconnect to the session through the HPCA Console.
   - 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.

     It is possible to enable this option in the HPCA 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 allows 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.

To open the System Defense filters management window

1 Log in to the HPCA 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 HPCA Console.

To refresh the System Defense filter view

1 Open the System Defense filters management window as described in To open the System Defense filters management window.

2 Click the  refresh icon on the toolbar.

To see the details of a System Defense filter

1 Open the System Defense filters management window as described in To open the System Defense filters management window.

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.

To remove System Defense filters

1 Open the System Defense filters management window as described in To open the System Defense filters management window.

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 allows 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

To open the System Defense policies management window

1. Log in to the HPCA 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 HPCA Console.

To refresh the System Defense policy view

1. Open the System Defense policies management window as described in To open the System Defense policies management window.
2. Click the  refresh icon on the toolbar.

To toggle between policies deployed to the wired and wireless NIC

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 To open the System Defense policies management window. 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.

To see the details of a System Defense policy

1. Open the System Defense policies management window as described in To open the System Defense policies management window.
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 inTo toggle between policies deployed to the wired and wireless NIC on page 156 and repeat this procedure for the other NIC.

To set an Agent Presence policy

1 Open the System Defense policies management window as described in To open the System Defense policies management window.

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 an agent 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 To toggle between policies deployed to the wired and wireless NIC on page 156 and repeat this procedure for the other NIC.

To enable a System Defense policy

1 Open the System Defense policies management as described in To open the System Defense policies management window.

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 To toggle between policies deployed to the wired and wireless NIC on page 156 and repeat this procedure for the other NIC.

To remove System Defense policies

1 Open the System Defense policies management window as described in To open the System Defense policies management window.

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 inTo toggle between policies deployed to the wired and wireless NIC on page 156 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 an agent 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 allows you to view and remove heuristics information that has been deployed to a specific vPro device.

To open the heuristics management window

1. Log in to the HPCA 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 HPCA Console.

To refresh the heuristics view

1. Open the heuristics management window as described in To open the heuristics management window.
2. Click the  refresh icon on the toolbar

To see the details for a heuristics specification

1. Open the heuristics management window as described in the To open the heuristics management window.
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.

To see the heuristics state information for a NIC interface on the device

1. Open the heuristics management window as described in To open the heuristics management window.
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.

To clear heuristics actions

1. Open the heuristics management window as described in To open the heuristics management window.
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.

To remove heuristics

1. Open the heuristics management window as described in To open the heuristics management window.
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 Agent Watchdogs on the vPro Device

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

To open the agent watchdog management window

1. Log in to the HPCA 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 **Agent Watchdogs** link under the **System Defense** section on the left-side of the window. A window opens displaying the Agent Watchdogs that have been created and deployed to the vPro device through the HPCA Console.

To refresh the agent watchdog view

1. Open the agent watchdog management window as described in To open the agent watchdog management window.
2. Click the refresh icon on the toolbar.

To see the details of an agent watchdog

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

To remove agent watchdogs

1. Open the agent watchdog management window as described in To open the agent watchdog management window.
2. Check the box next to each watchdog that you want to delete.

3 Click the delete icon on the toolbar. The selected agent watchdogs are removed from the agent watchdog table for the specific vPro device.

You can use the agent watchdog interface to:

- View the watchdog agents on the vPro device.
- Remove an agent 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 allows you to lock and unlock the keyboard and power button on the vPro device during remote power operations.

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 HPCA Console. It is recommended that you check with your hardware vendor for specific support-related information.

To configure front panel settings

1 Log into the HPCA 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 HPCA Console.

Resetting the Flash Limit on the vPro Device

The **General Settings** area of the workspace is available for vPro devices only. It allows you to reset the flash limit for the vPro device. See Management of Common Utilities on page 132 for more information about flash memory.

To reset the flash limit

1 Log into the HPCA 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 allows 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 allows 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. See Changing the Power State on page 143.

To configure the boot settings

1 Log into the HPCA 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.

> 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.

> 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.

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.

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.

9 Group Management

This chapter tells you how to manage Client Automation device groups that contain vPro devices through the HPCA 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 HPCA Console is **Group Management**.

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

This option allows you to do the following:

- Managing Multiple Groups of vPro Devices
- Managing Individual vPro Devices

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 allow you to manage multiple groups at once.

Table 18 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 local agent software list to selected groups
	Provisions device groups

Table 18 Group List Toolbar (cont'd)

Icon	Function
	Deploys and undeploys System Defense policies to selected groups
	Deploys and undeploys agent watchdogs to selected groups
	Deploys and undeploys heuristics to selected groups

As indicated in the device list toolbar table, the icon allows 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 `<HPCA_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

1. Login into the HPCA 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 checking the checkbox for the group or by checking the select all checkbox 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

1. Select the groups you want to manage as described in To select multiple groups.
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

1. Select the groups you want to manage as described in To select multiple groups.
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 HPCA Console.

Deployment of Local Agent Software List

To deploy local agent software list

1. Select the groups you want to manage as described in To select multiple groups.
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 local agent to monitor on the target vPro device group.

Provisioning

See Provisioning vPro Devices for complete details.

To perform provisioning operations

1 Select the groups you want to manage as described in To select multiple groups.

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 123 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.

To view the provisioning status log

1 Select the groups you want to manage as described in To select multiple groups.

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.

You can use this functionality to effectively perform provisioning operations on device groups and view the results with minimal effort.

Deployment of System Defense Policies

To deploy System Defense Policies

1 Select the groups you want to manage as described in To select multiple groups.

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.

To undeploy System Defense Policies

1 Select the groups you want to manage as described in To select multiple groups.

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.

You can use this functionality to easily deploy multiple System Defense policies to multiple vPro device groups to protect these systems from mal-ware attacks.

Deployment of Agent Watchdogs

To deploy agent watchdogs

1 Select the groups you want to manage as described in To select multiple groups.

2 Select **Deploy Agent Watchdogs** from the pull-down menu on the  manage agent 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.

To undeploy agent watchdogs

1 Select the groups you want to manage as described in To select multiple groups.

2 Select **Undeploy Agent Watchdogs** from the pull-down menu on the  manage agent 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.

You can use this functionality to easily deploy multiple agent watchdogs to multiple vPro device groups to monitor the local agents on these systems. Monitoring local 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 Heuristics

To deploy heuristics

1. Select the groups you want to manage as described in To select multiple groups.
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.
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.

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

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
- Properties Tab

- Devices Tab

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, refer to the *HP Client Automation Core and Satellite Standard 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. See Device Management.

10 Alert Notifications

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

Viewing Alerts on the vPro Device

You can use the HPCA Console to view event alerts. These alerts are generated by provisioned vPro devices when an event occurs, and they are sent to the HPCA 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 HPCA 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 generated 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 HPCA Console and select the **Operations** tab.
1. 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.
1. Click the  detail icon in the Detail column. A window opens that displays the property details for the selected alert.

You can use alerts subscriptions to determine if a noteworthy event alert has occurred that requires immediate action.

11 Troubleshooting

This chapter provides information for debugging the most common problems that can occur when using the Out of Band Management features in the HPCA Console as described in Common Problems.

It also explains best practices for backing up your OOBM data in case of corruption or the need to reinstall the product as described in Backing up OOBM Data.

It also summarizes the port requirements for Out of Band Management communication as described in Summary of Port Information.

It also provides a checklist of questions that you should answer before calling HP support as described in Checklist Questions.

Common Problems

In general when a problem occurs, it is always a good idea to review the log files in the `C:\Program Files\Hewlett-Packard\HPCA\tomcat\logs` directory (if you have installed HPCA in the default location). They contain all the output from the HPCA Console.

In addition, for agent-related problems, you should open the Event Viewer (**Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Event Viewer**) on the vPro client device.

The troubleshooting areas covered in this section include the following:

- General
- Provisioning
- Discovery
- Remote Operations
- Power State
- Reboot
- System Defense and Agent Presence
- Wireless
- Migration Issues

General

HPCA Console hangs when selecting vPro device type

Table 19 Console hangs for vPro device type selection

Possible Cause	Solution
SCS Service failed to communicate with the Out of Band Management Service because of excessive CPU utilization (Tomcat is utilizing 100% of the CPU)	If the problem persists, reboot the HPCA Tomcat server.

Error error page shown in place of single device console is not cleared

Table 20 Error page not cleared

Possible Cause	Solution
Internet Explorer browser cache is not cleared. Sometimes the error page that is shown in place of the single device console is not cleared till the Internet Explorer reopens.	Clear the cache of the Internet Explorer manually.

Keyboard and power button are locked although it is not set to locked in the HPCA Console

Table 21 Front panel locking problems

Possible Cause	Solution
Locking depends on the version of the BIOS running on the vPro device. Some versions, by default, lock the power button and keyboard.	On some devices, the BIOS settings are user configurable. Refer to the device documentation for BIOS versions that are configurable.

Cannot connect to vPro device using the wired NIC

Table 22 Connection problem on vPro device with wired NIC

Possible Cause	Solution
Possible causes are the following: 1. The vPro device has been removed from the network. 2. The web services for the vPro device are busy.	In these cases, select the devices of interest and refresh the HPCA Console screen by using the Refresh from Repository icon after a time lag of several seconds so that the HPCA Console web service requests can be fetched again from the vPro device.

Timeouts occur when using the HPCA Console

Table 23 Timeouts on HPCA Console

Possible Cause	Solution
Slow network traffic	Reconfigure the timeout period. See Configuring the IDE-R and SOL Time-out Values on page 48 for details.

Wrong alert subscription status on OOBM device management screen

Table 24 Wrong alert subscription status

Possible Cause	Solution
Issue is due to third-party dependencies of OOBM. When HPCA is installed on Windows Server 2008, the alert subscription operation, though successful, is incorrectly reported in the status column. This will cause a problem when the user is performing the alert subscription operation on vPro device by selecting **Operations** > **Out Of Band Management** > **Device Management** > **Alert Subscription**.	There is no workaround for this problem.

Accessing OOBM Device Details window after long idle period on console causes you to exit to login screen

Table 25 Long idle periods cause exit to login screen

Possible Cause	Solution
Database access related issue	Close the browser and re-login to HPCA Console in a new browser session.

Can not save SCS properties when managing vPro devices in device type selection window

Table 26 Domain name validated for SCS login

Possible Cause	Solution
For SCS login, the User Name was not specified in the domainName\userName format. This format is now required and authenticated. In earlier releases of OOBM, the domainName part of the login name was ignored. As a result, even if you provided the wrong domainName, it appeared to be accepted. Also, in earlier OOBM releases, the example given for the User Name login (provisionserver.yourenterprise.com\Administrator) was incorrect but worked because the domain name was ignored by OOBM.	You must provide the User Name login in the correct domainName\userName format in order to save SCS properties.

Cannot access DASH device after changing DASH credentials

Table 27 Problem when changing DASH credentials

Possible Cause	Solution
Previous credentials are cached causing the erroneous behavior	If you have changed the DASH device credentials, you must restart the Tomcat service to make them effective.

Synchronizing vPro devices with SCS repository takes a long time

Table 28 vPro SCS synchronization problem

Possible Cause	Solution
Several web services calls are made to determine the list of available vPro devices. This may take several minutes depending on how many systems are not available or on current network routing issues.	You can improve performance by reducing the web service timeout value. However, reducing the timeout value may cause some available machines to be missed or other operations (such as power or deployment) to not be completed.

Cannot access the correct vPro device

Table 29 vPro access problem

Possible Cause	Solution
IP address conflict problem, that is more than one vPro device may have the same IP address	IP addresses must be distinct. Contact the Network Administrator to resolve this problem.

Text is not displayed correctly by HyperTerminal during SOL operations

Table 30 Text display problems with HyperTerminal

Possible Cause	Solution
Wrap lines that exceed terminal width option may be enabled in HyperTerminal.	Open HyperTerminal. Go to File Properties. Select the **Settings** Tab. Click **ASCII Setup**. In the ASCII Setup window, uncheck the Wrap lines that exceed terminal width option.

Deployment of software list to OOB devices throws network error 26 in TLS mode

Table 31 Deployment of software list thros network error in TLS mode

Possible Cause	Solution
Client certificate is not properly configured on HP Client Automation install machine. Deployment of the software list to OOB devices causes the network error of 26 to be thrown in TLS mode. This will cause a problem when the user is performing the software list deployment operation by selecting **Operations** > **Out Of Band Management** > **Device Management** > **Software List Deployment**.	Install the client certificate on HP Client Automation installed machine and specify the certificate's subject name as the value for the "ca_server_commonname" property in the `config.properties` file.

Cannot read or write to the managed vPro device

Table 32 Flash limit exception errors

Possible Cause	Solution
Flash limit exceeded for vPro storage. Flash wear-out protection mechanism can cause a flash limit exception to occur if you have made several read/write accesses to the same vPro device. When the counter reaches 200, the vPro device does not allow anymore write operations.	Use the **Reset Flash Limit** option from the pull-down menu on the common utilities icon. See Management of Common Utilities on page 132 for details.

I18N issues with OOBM and SCS

Table 33 I18N issues with SCS

Possible Cause	Solution
Dependencies on underlying components and technologies like the hardware BIOS or the Intel SCS. Although HPCA Console can be installed on non English operating systems, there are some restrictions due to dependencies on underlying components and technologies like the hardware BIOS or the Intel SCS. As a result, you cannot enter non English names for several user-defined items, including filters, watchdogs, and policies by selecting **Configuration** > **Out Of Band Management** > **vPro System Defense Settings**. The SOL console for the BIOS setup works only for supported character sets. Similarly, other features may not work as expected in non English locales. Numbers, dates, and time are not being displayed in the format of the non-English operating system's locale.	There is no workaround for this problem.

English path separator is displayed on Japanese locale for OOBM features

Table 34 English path separator appears in non-English locale

Possible Cause	Solution
Limitation in the underlying Intel SCS component. The HPCA Console shows the English path separator on a Japanese locale. This problem will occur only for the OOBM functionality.	There is no workaround for this problem.

Cannot read or write to the managed vPro device

Table 35 Flash limit exception errors

Possible Cause	Solution
Flash limit exceeded for vPro storage. Flash wear-out protection mechanism can cause a flash limit exception to occur if you have made several read/write accesses to the same vPro device. When the counter reaches 200, the vPro device does not allow anymore write operations.	Use the **Reset Flash Limit** option from the pull-down menu on the common utilities icon. See Management of Common Utilities on page 132 for details.

Provisioning

Status of provisioned vPro device does not appear as provisioned in the Device List table on the vPro Provisioning tab

Table 36 Display of vPro status problem

Possible Cause	Solution
Table not refreshed with updated information	Re-discover the device using Active Directory discovery. The status of the device will be updated after this operation.

Cannot set ACLs when provisioning vPro devices whose version of AMT firmware is less than 4.0 on SCS 5.0

Table 37 ACL configuration problem on vPro devices

Possible Cause	Solution
All realms have been selected when creating the profile for vPro devices with 4.0 AMT firmware or earlier	Create a separate profile for devices with the earlier version of AMT firmware. In this profile, select only the Redirection, PT Administration, Hardware Asset, Remote Control, Storage, Event Manager, Storage, Administration, Agent Presence Local, Agent Presence Remote, Circuit Breaker, Network Time, General Info, and Firmware Update realms.

Console throws SCS error when provisioning vPro devices

Table 38 SCS error when provisioning vPro device

Possible Cause	Solution
Internal error retruned from Intel SCS. In some cases when you are trying to provision vPro devices through the HPCA Console, the console throws up an SCS error or an error message without any other information.	This is harmless and can be ignored. The provisioning operation has been initiated successfully on the vPro device and this can be confirmed by verifying the results of the operation after a period of time.

Provisioning vPro device multiple times causes console to exit to login screen

Table 39 Provisioning causes exit to login screen

Possible Cause	Solution
Database access related issue	In some cases when you attempt to provision a vPro device multiple times through the HPCA Console, the console may exit to the login screen. In such cases, close the browser completely and re-login to the HPCA Console.

Discovery

Failure to discover vPro devices although OOBM agent is installed

Table 40 vPro device discovery failure

Possible Cause	Solution
Port 9998 might be blocked by the firewall.	Ensure that port 9998 is not blocked on the vPro device.

No hardware assets are discovered for a managed vPro device

Table 41 Hardware discovery problems

Possible Cause	Solution
Internal error occurred in the vPro device during this operation	Shut down the device, remove the power cord, wait 10 to 15 seconds, and restart the device.

Table 41 Hardware discovery problems

Incorrect provisioning of the vPro device	Reconfigure the target vPro device. See Configuring the vPro Device through the MEBx on page 37 for details.
Container space limitation prevents capture of additional asset data. Can occur if there are a large number of devices on a system.	Disconnect some of the devices.
Network error occurred while querying for hardware assets due to heavy network traffic	Re-issue the command after a time lag.

No software assests are discovered for a managed vPro device

Table 42 Software discovery problems

Possible Cause	Solution
No applications are registered	It is the responsibility of the software installed on the vPro device to register with the 3PDS. The HPCA Console does not support registration of applications.
Network error occurred while querying for software assets due to heavy network traffic	Re-issue the command after a time lag.

Some properties are displayed as blank for discovered hardware and software assets

Table 43 Blank values for some discovered hardware and software assets

Possible Cause	Solution
No information is available for the property on the device.	This is normal behavior if no information for a particular property is stored on the device.

HPCA cannot connect to SCS and discover vPro devices in some cases involving Windows Server 2008 R2

Table 44 Console cannot connect to SCS and discover vPro devices

Possible Cause	Solution
Cause not known. HPCA cannot connect to SCS when HPCA is installed on Windows Server 2008-x64-R2 and SCS and Active Directory are both installed on the same machine running Windows Server 2008-x64.	When HPCA is installed on Windows Server 2008-x64-R2, and it is required that both Active Directory and SCS are on win2k8-x64, install Active Directory and SCS on different physical or virtual machines running win2k8-x64.

OOBM groups will fail to reload when the OOBM device database does not have the latest devices

Table 45 OOBM groups fail to reload

Possible Cause	Solution
OOBM database is not updated with the latest devices. OOBM groups will fail to reload and the error "No devices with Given Name" is displayed. As a result, groups will not be updated. This will cause a problem when the user is performing the groups reload operation by selecting **Operations** > **Out Of Band Management** > **Group Management** > **Reload**.	Perform the OOBM device discovery operation again to update to the latest devices. This will solve the groups reload error.

Discovery of valid DASH device fails

Table 46 DASH device discovery failure

Possible Cause	Solution
This can occur because the device fails to respond in time because of network traffic.	Increasing the configuration values of `HTTP_READ_TIMEOUT` and `HTTP_CONNECT_TIMEOUT` may resolve this problem. The procedure for changing configuration values is described in Out of Band Management Configuration on page 47.

DASH device discovered and displayed with IP address instead of hostname

Table 47 DASH device discovery problems

Possible Cause	Solution
Device has been discovered by specifying the IP address and the DNS server is not configured for “reverse DNS lookup.”	Specify the hostname when attempting to discover DASH devices. See Device Discovery on page 128. If the DNS server is not configured for “reverse DNS lookup,” it is not possible to get the translation from IP address to hostname for the device. All operations should work as expected irrespective of whether the IP address or hostname is displayed.

Provisioned vPro device not discovered or shown as unavailable

Table 48 vPro device discovery problems

Possible Cause	Solution
The vPro device although provisioned earlier may no longer be provisioned.	Reprovision the vPro device. See Configuring the vPro Device through the MEBx on page 37 for details.
The vPro device may have been removed from the Domain Controller although it still exists in the SCS database.	Ensure that the vPro device exists in the Domain Controller with the correct FQDN.
The vPro device has multiple entries in the DNS server.	Ensure that the vPro device has only one entry in the DNS server.
The vPro device has a different IP address in the DHCP server from the one displayed in the device list in the HPCA Console.	Ensure that the vPro device has the same IP address in the HPCA Console device window as that in the DHCP server.

Provisioned vPro devices in Client Automation groups are not shown on Devices tab in Group Details window

Table 49 Group device discovery problems

Possible Cause	Solution
The vPro device in the Client Automation group may not be listed with a FQDN.	Import the device in to the Client Automation group by using the FQDN and add this device to the group. Then reload the Client Automation group into the HPCA Console.

Remote Operations

The PuTTY console fails to open when performing remote operations on DASH devices

Table 50 PuTTY console does not open

Possible Cause	Solution
Another PuTTY console may be running on the system. While performing DASH remote operation with the display to console option enabled, the PuTTY console will fail to open if another PuTTY console is running on the system.	Ensure that no other PuTTY console is running before performing DASH remote operation.

Telnet console does not open when performing remote operations

Table 51 Telnet console does not open

Possible Cause	Solution
Specific internet settings are not set correctly and are preventing the display of the telnet console	In your Internet Explorer, go to **Tools** > **Internet Options** > **Advanced**. Ensure that both the **Disable script debugging (Internet Explorer)** and **Disable script debugging (other)** options are selected.
Default security settings for ActiveX controls are preventing the display of the telnet console	In your Internet Explorer, go to **Tools** > **Internet Options** > **Security**. Click **Custom Level**. Select Enable for **Download unsigned ActiveX controls** and **Initialize and script ActiveX controls not marked as safe**.

Telnet session does not open on the client console on Windows Server 2003 64-bit platforms

Table 52 Telnet session does not open on Windows Server 2003 64-bit

Possible Cause	Solution
OOBM is not able to open the telnet connection on this platform	Use HyperTerminal to view the vPro device text console. Configure the PuTTY client to view the DASH device text console.

PuTTY client may not show the DASH client console on Windows 64-bit platforms

Table 53 PuTTY client does not show DASH client console on Windows 64-bit

Possible Cause	Solution
PuTTY is not able to establish the connection with the client DASH device on Windows 64-bit systems.	There is no workaround for this problem.

OOBM remote operations fail on vPro device after changing the provisioned state of the device

Table 54 Remote operations fail on vPro device after changing provisioning

Possible Cause	Solution
Inconsistency between the information in the OOBM database and the SCS database. When changing the provisioned state of a vPro device (including changing TLS mode and re-provisioning the device with a different SCS profile), remote operations on individual or multiple vPro devices fail.	Select the device for which the provisioned state has changed and click the **Reload Device Information** button from **Operations** > **Out of Band Management** > **Device Management**. Alternatively, click the **Reload Device Information** button (without selecting a device). The latter takes longer but will refresh all device information so that latest information is loaded into OOBM database and is consistent with the information in SCS database.

Nothing appears to be happening when performing OOBM remote operations on vPro device

Table 55 Nothing appears to be happening when performing remote operations

Possible Cause	Solution
• Inconsistency between the information in the OOBM database and the SCS database • Unavailability of the device on the network	Close the Device Detail window and open a new one. This should allow you to see the error messages. If the problem is caused by an inconsistency between the OOBM and SCS databases, click the **Reload Device Information** button under **Operations** > **Out Of Band Management** > **Device Management** > **Refresh All**.

OOB DASH device boots from hard drive regardless of boot order

Table 56 DASH device always boots from hard drive

Possible Cause	Solution
Issues with the Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware. If the user has included USB in the boot order and if the USB boot source is not bootable, the system will boot from the hard-drive regardless of the other boot sources in the boot order. This will cause a problem when the user is performing boot operations on a DASH device when selecting **Operations** > **Out Of Band Management** > **Device Management** > <*DASH Device*> > **Remote Operations**.	There is no workaround.

OOB DASH device tries all boot sources including ones that are not specified in the boot order

Table 57 DASH device tries all boot sources regardless of specification

Possible Cause	Solution
Issues with the Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware If the user selects the persistent boot option, the device will try all the boot sources, including those that are not specified in boot order. This will cause a problem when the user is performing boot operations on a DASH device when selecting **Operations** > **Out Of Band Management** > **Device Management** > <*DASH Device*> > **Remote Operations**.	There is no workaround.

Incorrect network controller set as first boot source for OOB DASH devices

Table 58 Incorrect network controller set as first boot source for DASH device

Possible Cause	Solution
Issues with the Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware. For Dash-enabled devices, if you change the boot order to make Network the first boot device, it will set the embedded network controller as the first boot source instead of the Broadcom DASH NIC. As a result, the PXE boot from the Broadcom NIC will fail.	Go into the F10 Setup Advanced menu. The embedded NIC PXE option ROM can be prevented from loading by disabling the NIC PXE Option ROM Download option in the Device Options list. Retry booting from the Broadcom PXE after you have disabled this option.

Cannot go to the next page from the Remote Operations Wizard Task page

Table 59 Remote Operations Wizard frozen problem

Possible Cause	Solution
Incorrect version of the JRE	Install JRE version 1.5 or later and select the option in the Internet Explorer to install the JRE plug-in. To select this option, in your Internet Explorer, go to **Tools** > **Internet Options** > **Advanced** and select the **Use JRE 1.5.*XX* for <applet> (requires restart)** option. Restart the Internet Explorer once the JRE is installed and enabled.

Telnet session fails to open for SOL/IDE-R operations on vPro devices

Table 60 Failure to open telnet session for SOL/IDE-R operations

Possible Cause	Solution
The telnet client may not be installed. By default, the telnet client is not installed on Windows Server 2008. When HPCA is installed on Windows Server 2008 x64 (AMD64T), the telnet session does not open for SOL/IDER operations. The boot operation however is successful and the machine boots from the correct media. The Heal use case is not fully supported due to this issue. For example, the BIOS updates cannot be performed.	Install the telnet client by using the server manager option in Windows Server 2008.

Remote Operations wizard for DASH device keeps on showing progress bar without showing operation completion

Table 61 Remote Operation Wizard keeps on showing progress bar

Possible Cause	Solution
The device hardware is not sending an acknowledgement for the remote operation to the Remote Operation wizard causing the wizard to continuously wait. However, the remote operation is successful.	The only way to execute another OOBM remote operation is to log out and close the current IE session and log in again in a new IE session.

Boot configuration setting for DASH devices remains enabled for a while

Table 62 Boot configuration setting for DASH devices remain enabled

Possible Cause	Solution
This reflects the fact that the operation is still in progress and then eventually completes.	This is the expected behavior.

Remote operations like Hibernate (Soft) and Suspend do not work on target DASH device

Table 63 Hibernate and Suspend operations do not work on DASH device

Possible Cause	Solution
The Broadcom management agent may not be running on the target DASH device or the DASH device may not be in the Windows OS running state. If either of these conditions exist, Hibernate and Suspend operations will not function on the DASH device even though the operaton is shown as successful in the HPCA console.	Make sure that the latest Broadcom management agent has been installed and that the management agent service is running on Windows on the target DASH device.

vPro device IDE-R operations information does not align properly in HyperTerminal console

Table 64 IDE-R information does not align in HyperTerminal

Possible Cause	Solution
Timing issues or issue with the firmware from hardware vendor.	There is no workaround for this problem.

Multiple users performing operation on same OOBM device causes erratic behavior

Table 65 Multiple users performing operations on same device

Possible Cause	Solution
Architectural limitation.	At any given time, only a single user should be performing remote operations on a device.

vPro device does not power down after IDE-R reboot

Table 66 vPro device power down problem after IDE-R reboot

Possible Cause	Solution
Web services are busy performing current operation	The vPro device may not successfully perform a Power Down command after an IDE-R reboot. Waiting ten seconds before issuing the Power Down command should work around the problem.

vPro device floppy IDE-R reboot produces unintelligible output to SOL display

Table 67 vPro device produces unintelligible output to SOL

Possible Cause	Solution
This can be caused by creating the bootable floppy from an MS Windows version of MS-DOS (for example, using Format in Windows to create an MS-DOS Startup Disk).	Use another means of creating a bootable floppy drive.

vPro devices appear grayed out after power down command

Table 68 vPro device grayed out after power down

Possible Cause	Solution
Your ME power setting options may not be set properly. In the SCS profile, the power policy may not be set properly. Also, there may be multiple entries for the vPro device in the DNS server.	Make sure your ME power setting options are set to always on ME or wake on ME in all possible power states. Also, check in the SCS profile that the power policy is set to always ON. And finally, check if there are multiple entries for the vPro device in the DNS server. If there are multiple entries, delete the wrong entries, restart the DNS server, flush the DNS in the HPCA Console server, and re-start the HPCA Console server. Alternatively, you can increase the web service timeout value on the HPCA server.

OOB devices transitioning to S1/S2 or Sleep-Light power states show erratic behavior

Table 69 S1/S2 or Sleep Light power states show erratic behavior

Possible Cause	Solution
Some hardware vendors do not support the S1/S2 or Sleep-Light power states.	Refer to the documentation from the hardware vendor for more details.

OOB device stays in suspended state after power down

Table 70 Device stays in suspended state after power down

Possible Cause	Solution
On certain hardware, if the system is in a suspended state and a user invokes power off, the HPCA Console reports success, but the machine stays in the suspended state. This is due to the fact that the hardware in these cases does not support the power off operation from the suspended state.	Refer to the documentation from the hardware vendor if you are seeing such behavior for more details.

Graceful power operations on DASH devices are displayed as supported options but are not working

Table 71 Graceful remote operations not working on DASH devices

Possible Cause	Solution
Broadcom management agent is not installed	Install latest Broadcom management agent on DASH device.

Power State

Cannot view or change the power state of a managed vPro device

Table 72 Power state problems

Possible Cause	Solution
Network error occurred while querying the system due to heavy network traffic	Re-issue the command after a time lag.
Failure to power down occurred because of an active IDE-R/SOL session	Power down command is not supported when there is an active IDE-R/SOL session. The console throws the "Parameters are valid but not supported by platform" exception. Check if there is an active session. If so, close the session and try to power down after a time lag.

Power state of a device is grayed out after a power down operation

Table 73 Power display problems

Possible Cause	Solution
Timeout period exceeded	Reconfigure the timeout period. See Configuring the IDE-R and SOL Time-out Values on page 48 for details.

Reboot

To troubleshoot reboot problems, you must examine the global configuration settings for IDE-R and SOL and the remote control options.

Must perform boot order operation before reboot of OOB DASH devices for one time boot setting

Table 74 Must perform boot order operation before reboot of DASH devices

Possible Cause	Solution
Issues with the Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware. If the user selects the boot configuration setting of one time boot for a reboot operation on Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware, the user is required to perform the boot order operation before reboot. Otherwise, the remote operation will display erratic behavior. Also note that although the user has performed an explicit boot order operation, after reboot, the boot order will get reset to default boot order. This will cause a problem when the user is performing boot operations on a DASH device by selecting **Operations** > **Out Of Band Management** > **Device Management** > <*DASH Device*> > **Boot Configuration**.	There is no workaround.

On DASH device, one time boot configuration does not reset

Table 75 One time boot configuration does not reset on DASH device

Possible Cause	Solution
Issue with system BIOS. One time boot configuration on the DASH device is not resetting even after the device reboots. When the one time boot configuration is selected or enabled for any remote operation, it is not unselected or disabled once the remote operation has been successfully completed. Once this problem occurs, all the future remote operations will always use the one time boot configuration. This will cause a problem when the user is setting the one time boot configuration on a DASH device by selecting **Operations** > **Out Of Band Management** > **Device Management** > <*DASH Device*> > **Boot Configuration**.	Change the boot order of the one time one-boot configuration before performing any reboot operation by selecting **Operations** > **Out Of Band Management** > **Device Management** > <*DASH Device*> > **Remote Operations**.

Cannot change boot configuration setting for DASH device to default and permanent boot

Table 76 Cannot change boot configuration on DASH device

Possible Cause	Solution
The settings are hard coded to the permanent boot configuration setting for the first boot configuration setting listed. It is not possible to change the boot configuration settings to default and permanent boot. The user cannot change this to one time boot. However, the user can change the settings for second boot configuration setting listed to one time boot. This will cause a problem when the user is performing boot configuration settings on a DASH device when selecting **Operations** > **Out Of Band Management** > **Device Management** > <*DASH Device*> > **Boot Configuration**.	There is no workaround for this problem.

Cannot see the reboot process on the HPCA Console using SOL

Table 77 Problems seeing reboot using SOL

Possible Cause	Solution
Port 9999 is being used by another device	Free up port 9999 for SOL transmission.
SOL redirection was not enabled during provisioning	Enable SOL redirection using Intel SCS. See Configuring the vPro Device through the MEBx on page 37 for details.
Bootable floppy created with Windows Explorer	Using Format in Windows to create an MS-DOS Startup Disk produces a bootable drive but the output to SOL is unintelligible. Use another means of creating a bootable floppy drive.

Cannot remotely reboot a managed vPro device

Table 78 Problems rebooting

Possible Cause	Solution
Incorrect reboot parameters	View logs to check reboot parameters. If they are incorrect, try rebooting with the correct parameters.
Known limitations in firmware for certain options	Check the Intel vPro Provisioning Server Release Notes located in the `Media\oobm\win32\AMT Config Server` directory on the HPCA Core distribution media.

Table 79 Problems rebooting with IDE-R

Possible Cause	Solution
Physical bootable device (drive/image) is not present in the management console.	Boot to an existing drive in the management console. If the physical device is not present, use the ISO image instead.
Image in the media is not bootable.	Check if image is bootable. If not, replace it with bootable image.
If trying to reboot to CD/DVD, the CD drive on the HPCA Console server does not match the default `D:` drive setting.	Reconfigure the default drive setting to match the CD/DVD drive on HPCA Console server. See Configuring IDE-R Drives on page 47 for details.

Cannot remotely reboot a managed vPro device to BIOS settings

Table 80 Problems rebooting to BIOS settings

Possible Cause	Solution
BIOS does not support booting to BIOS settings	Upgrade BIOS on the target device to a version of the BIOS where this feature is supported.

Cannot reset the boot order of a managed vPro device

Table 81 Problems resetting the boot order

Possible Cause	Solution
Difficult to determine	Perform a local HDD boot command and reboot the target device.

System Defense and Agent Presence

Cannot deploy System Defense policies to the managed vPro device

Table 82 Add System Defense network filter error

Possible Cause	Solution
Filter limit of 31 inbound and 30 outbound filters has been exceeded for vPro device	Delete some of the existing filters on the vPro device. See Managing System Defense Filters on page 103 for details.

System Defense policies do not always function properly on vPro devices with wireless network driver

Table 83 System Defense policies on devices with wireless NIC

Possible Cause	Solution
Wireless network driver version on vPro device is not consistent with the installed verson of the Intel AMT.	To ensure proper functionality of System Defense policies, the wireless network driver version on the vPro device must be consistent with the installed version of Intel Active Management Technology. More details regarding version compatibility can be obtained from the hardware vendor.

Cannot deploy agent watchdog the managed vPro device

Table 84 Watchdog deployment error

Possible Cause	Solution
Only one HP local agent watchdog can be deployed to a vPro device. Multiple third party agent watchdogs can be deployed, one per third party local agent installed on the vPro device. The total number of agent watchdogs that can be deployed to a single device is 16.	Remove or undeploy agent watchdogs from the vPro device. See Managing Agent Watchdogs on page 114 for details.
Invalid, contradictory actions defined for the watchdog.	Review actions specified for the agent watchdog and modify contradiction. See Managing Agent Watchdogs on page 114 for details.

Local agent installation fails with error code 1920

Table 85 Local agent installation error

Possible Cause	Solution
Issues with a previous install or uninstall of the local agent.	Remove the HPCA-OOBM local agent service from the vPro device. To do this, right click the My Computer icon and navigate to **Manage** > **Services and Applications** > **Services**. Check for the HPCA-OOB local agent service. If this service exists, do the following: • Open a command prompt window • Type `sc delete HPCA-OOBM` • Restart the system
You did not provide a user name and password when installing the local agent.	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 will fail with error code 1920.

Local agent shuts down

Table 86 Local agent shutdown behavior

Possible Cause	Solution
No applications have been defined for it to monitor.	Create and deploy a software list of applications for the local agent to monitor. See Managing Agent Watchdogs on page 114 for details.

Deployment of local agent software list on vPro device throws SOAP error

Table 87 Deployment of agent software list causes SOAP error

Possible Cause	Solution
vPro Web Services returns the error. Deployment of the local agent software list may throw one of several errors including "Network Error – SOAP error code: 22," "Integrity check error," "Not initialized," and "Invalid parameter."	Retry the same operation after a time lag. If the error still occurs, logout and re-login to the HPCA Console.

Local agent does not appear in software list on vPro device

Table 88 Agent is not in software list on vPro device

Possible Cause	Solution
Architectural limitation occurring when the local agent is installed by one user account and viewed by a user who has logged in with another account.	There is no workaround for this problem.

Deploying Agent Presence policy to one NIC on an vPro device with multiple NICs returns error

Table 89 Deploying Agent Presence policy to vPro device with multiple NICs

Possible Cause	Solution
Internal error.	Deploy the Agent Presence policy to both NICs and then undeploy the Agent Presence policy from the unwanted NIC.

Anti spoofing filter causes all outgoing traffic on vPro device to be dropped

Table 90 Anti spoofing filter causes all outgoing traffic to be dropped

Possible Cause	Solution
If a vPro device is provisioned with a profile in SCS with environment detection enabled and the device is connected to a domain, which has not been specified in the environment detection domain(s), all outgoing traffic will be dropped if the System Defense policy on the vPro device has the anti spoofing filter enabled.	Connect the device to a domain specified in the environment detection domain(s).

Local agent cannot register with watchdog on vPro device

Table 91 Local agent registration problem

Possible Cause	Solution
If the local agent is not able to register with the agent watchdog, the issue may be with Digest username (Intel AMT username). In the Intel AMT firmware, the Digest username is case sensitive. You must specify the Digest username with the exact case when installing the local agent. Otherwise, the local agent will not be able to register successfully with the agent watchdog.	Be sure to specify the Digest username correctly with the exact case.

Repeated messages are displayed when local agent is stopped on vPro device

Table 92 Repeated messages when local agent is stopped

Possible Cause	Solution
Internal error in HPCA-OOBM Agent	If this occurs, restart the HPCA-OOBM agent service (HPCA-OOBM) on the client vPro device.

Cannot access vPro device after changing Digest credentials

Table 93 Cannot access vPro device after changing credentials

Possible Cause	Solution
Agent gets the password only during install time and not dynamically when it is changed. You will not be able to access a vPro device if you have changed the Digest username/ password for this device through the SCS console.	To be able to access and manage this device after changing the Digest credentials, you must stop the local agent (HPCA-OOBM) service on the vPro device. If you are using the Agent Presence functionality, you must reinstall the local agent on the vPro device with the new password.

Local agent does not work properly on vPro device after changing from TLS profile to non-TLS profile

Table 94 Local agent and TLS profile

Possible Cause	Solution
If the local agent is installed using a TLS profile, and at some point, the vPro device is re-provisioned with a non-TLS profile, the local agent will not work properly. Similarly, if the local agent is installed using a non TLS profile, and at some point, the vPro device is re-provisioned with a TLS profile, the local agent will not work properly.	If this occurs, you must re-install the local agent using appropriate profile.

Local agent admin pop-up message displays briefly and disappears

Table 95 Local agent admin message display

Possible Cause	Solution
This is the default behavior of the admin pop-up message when the Agent Presence policy is activated.	Open the Windows Event Viewer on the vPro device to see all agent-related log messages.

Cannot deploy local agent software list and system message to the managed vPro device

Table 96 Deploy local agent software list and system message error

Possible Cause	Solution
• Multiple actions occurring at the same time to the 3PDS • Multiple accesses to 3PDS during one session • Data transfer problem over the network	Retry deployment after a time lag.

Cannot deploy the local agent software list or view the software information in TLS mode

Table 97 Local agent problems in TLS model

Possible Cause	Solution
The Tomcat service may not be running on the Domain administrator account.	Ensure that the HPCA Tomcat Server service is running on the Domain administrator account. If not, reconfigure and restart Tomcat.
The common name on the Certificate Authority (CA) may not be specified correctly.	Ensure that the common name on the CA is specified correctly. The setting can be found in the `local_settings.ini` file in the installation directory.

There is no change in the watchdog state on the HPCA Console after the local agent is successfully installed.

Table 98 Watchdog registration error

Possible Cause	Solution
Watchdog registration failed.	Open the Windows Event Viewer on the vPro device and check for watchdog registration log messages. If unsuccessful, install the Host Embedded Controller Interface (HECI) driver and the Local Manageability Service (LMS) service on the vPro device and re-check the watchdog status.

Deployed Agent Presence Policy not activated when defined actions occur

Table 99 Agent Presence Policy not activated

Possible Cause	Solution
The defined actions may not have occurred in the anticipated order. The local agent may have expired before the local agent transitioned to the specified state.	It is safest to specify “Do not Care About State” as the transition to state when specifying agent watchdog actions.

Agent Presence Policy is activated immediately after deployment

Table 100 Agent Presence Policy immediately activated

Possible Cause	Solution
The transition state activating the Agent Presence policy may have already occurred triggering the immediate activation of the Agent Presence Policy by the agent watchdog.	Delete the existing watchdog and redeploy.

Cannot deploy System Defense policies with special characters in name

Table 101 System Defense policy name error

Possible Cause	Solution
It is possible to create filters and policies with non ASCII characters in their names, but it is not possible to deploy them. Also, filters and policies with special characters like ‘:’, ‘,’, '>', '<', '&', and “” in their names cannot be deployed. This limitation is indicated in the Intel AMT specification.	Create filters and policies with names that adhere to the specification.

Wireless

Cannot connect to a wireless device through the HPCA Console

Table 102 Wireless device connect problem

Possible Cause	Solution
Web service timeout occurred since the time it takes to communicate with a wireless device is greater. When the HPCA Console cannot connect, the devices appear grayed out in the console.	Reconfigure the timeout period. See Configuring the IDE-R and SOL Time-out Values on page 48 for details.

Cannot connect to vPro device using the wireless NIC

Table 103 Cannot connect using wireless NIC

Possible Cause	Solution
Expected behavior for the 2.5 version of vPro devices when only the wireless NIC is configured and the device is not plugged in and powered on.	Connect the vPro devices to a power source and power them on.

Failure to establish SOL/IDE-R session on wireless network for vPro devices

Table 104 SOL/IDE-R session failure over wireless network

Possible Cause	Solution
Time-out occurred because vPro devices with wireless NICs require a greater amount of time to communicate with the OOBM Server.	Configure the `IDER*` and `SOL*` parameters as described in Configuring the IDE-R and SOL Time-out Values on page 48 in the Out of Band Management Configuration chapter.

Policy settings for wireless NIC fail

Table 105 Wireless policy deployment problem

Possible Cause	Solution
The vPro device does not have a wireless NIC although the policy appears to have deployed successfully.	Undeploy the policy or install a wireless NIC on the vPro device and redeploy the policy.

Migration Issues

SCS console does not show profiles correctly after migration to SCS 5.3

Table 106 SCS migration issue when displaying profiles

Possible Cause	Solution
The SCS data has been migrated from a previous version of SCS. In this case, the new SCS console will not display the migrated profiles in the left-side tree view.	You can view the profile information in profiles section on the right side of the SCS console.

Local agent software list and system message cannot be displayed after migration to the current release of Out of Band Management Software

Table 107 Migration issue for local agent message and list

Possible Cause	Solution
This is the normal behavior. If the software list and system message for the local agent are created and deployed in an earlier release of Out of Band Management Software, they are not available if you migrate to a later version.	Create and redeploy the local agent and system message in the current release. See Managing Agent Watchdogs on page 114 for details.

Incremental discovery performs full discovery when migrating to later release

Table 108 Device discovery performed when migrating to later release

Possible Cause	Solution
This is the expected behavior.	When you migrate from an earlier release, migrated devices will be listed in the HPCA Console. When you perform vPro discovery (full/updated discovery) for the first time, it performs a full vPro discovery (not an incremental update) since it is the first discovery performed in the current version of the console.

Backing up OOBM Data

It is always a good idea to backup your OOBM data on a regular basis. There are three types of files you will want to backup:

- Configuration Files
- Data Files
- Database

The default installation directory for HPCA is `C:\Program Files\Hewlett Packard\HPCA`. The default data directory for HPCA is `C:\Program Files\Hewlett Packard\HPCA\data`.

If you are uninstalling or upgrading HPCA and want to retain the OOBM configuration and data files for later use, you must use the migration scripts for the backup and restore of files. For more information on migration and restore, refer to the *HP Client Automation Starter and Standard Migration Guide* available on the distribution media under `Docs\migrate`.

Configuration Files

To back up the configuration files

The OOBM configuration files, namely `configuration.properties` and `config.properties` are located in `<HPCA_INSTALL_DIR>\oobm\conf`. Copy these two files to a location outside of the HPCA installation directory structure. You can copy them back to the original location if you reinstall the HPCA product and want to retain the existing configuration.

Data Files

To back up data files

All the vPro System Defense configuration information for filters, policies, heuristics, and watchdogs are located in `<HPCA_DATA_DIR>\oobm\datafiles` as XML files. Copy the `sd.xml` and `AgentPresence.xml` files to a location outside of the HPCA installation directory structure. You can copy them back to the original location if you reinstall the HPCA product and want to retain the existing vPro System Defense configuration information.

Database

To back up database

The OOBM database stores information about discovered devices, DASH credentials, and HPCA groups. This database is located in `<HPCA_DATA_DIR>\oobm\OOBMDB`. Copy the entire `OOBMDB` directory to a location outside of the HPCA installation directory structure. You can copy the directory back to the original location if you reinstall the HPCA product and want to retain this information.

Summary of Port Information

Out of Band Management uses several TCP ports for communication. If corporate or personal firewall software is installed, then the following port exclusions must be made on the HP CA Console server to allow for inbound and outbound traffic.

For Out of Band Management Service to vPro Device Communication:

- Port 16692 is used for web service traffic over TCP.
- Port 16693 is used for web service traffic over TLS (with client authentication).
- Port 9999 is used as the default starting port for communication between the SOL display applet and the server's web application. This is configurable.
- Port 16694 is used for SOL/IDE-R over TCP.
- Port 16695 is used for SOL/IDE-R over TLS (with client authentication).
- Port 162 is used for alert management.

For Browser to Server Communication:

- Port 9999 is used for applet to server socket communication for SOL. This port must also be available on the client browser system as well.
- Port 5900 is used for the VNC Viewer for KVM redirection on vPro devices.

For Out of Band Management Service to Local Agent Communication:

- Port 9998 is used for communication between Out of Band Management and the local agent during Remote Configuration of vPro devices.

For Out of Band Management Service with DASH devices:

- Port 623 is used for communication between Out of Band Management and DASH devices.

Checklist Questions

If you are still having problems with the Out of Band Management features in the HPCA Console, call HP support. Before calling, be sure you know the answers to the following questions. This information will expedite the support team’s ability to solve any problem you may be experiencing.

1 What is the operating system and service pack installed on your HPCA Console server?

2 What is the IIS version on the SCS Server?

3 Are SCS and the HPCA Console installed on the same machine?

4 Are SCS and the SQL server installed on the same machine?

5 Is Active Directory installed on your network?

6 Do you have a DNS and DHCP-enabled network?

7 Are you using the NTLM v2 protocol for authentication between the SCS server and the Out of Band Management Service on the HPCA Console (you can check in local policies to confirm)?

8 What user ID did you use when installing SCS regardless if it was a local or domain user?

9 Does that local or domain user have local administrator rights?

10 What authentication mode are you using to communicate with SQL (Windows authentication is recommended)?

11 Are you able to login to the HPCA Console?

12 Are any devices listed on the Devices tab in the HPCA Console?

13 Are the devices displayed but are disabled, that is, they appear grayed out and are not accessible?

14 Are any devices provisioned using SCS?

15 Are the provisioned devices listed in the SCS table?

16 For SCS login, are you using **http://IP/AMTSCS** or **https://IP/AMTSCS** as the URL?

Index

N

O

P

R

S

T

U

V

W

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click on the bookmark “Comments”.

In case you do not have the email client configured, copy the information below to a web mail client, and send this email to **ca-docfeedback@hp.com**

Product name:

Document title:

Version number:

Feedback: