

HP Client Automation Agent

for Windows® operating system

Software Version: 5.11.4 and 7.8.1

Agent Lockdown Mode Enablement Guide

Document Release Date: April 2010

Software Release Date: February 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

© Copyright 2010 Hewlett-Packard Development Company, L.P.

Trademark Notices

Linux is a registered trademark of Linus Torvalds.

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

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
Copyright Mihai Bazon, 2002, 2003

Documentation Updates

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

- Software Version number, which indicates the software version.
 - The number before the period identifies the major release number.
 - The first number after the period identifies the minor release number.
 - The second number after the period represents the minor-minor release number.
- 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 and to verify that you are using the most recent edition, visit:

<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.

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

Support

You can visit the HP Software support site at:

www.hp.com/go/hpsoftwaresupport

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

HP Software online software support provides customer self-solve capabilities. It provides a fast and efficient way to access the interactive technical support tools that are needed to manage your business. As a valued support customer, you can benefit by using the support 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 an active support contract. To find more information about support-access levels, go to:

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

To register for an HP Passport ID, go to:

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

Contents

1	Introduction	9
	HP Client Automation Agent.....	10
	Audience.....	11
	Background.....	11
	Entitlement Settings.....	12
	Machine Defaults (MACHDEF.EDM).....	12
	Potential Security Concerns	13
	Agent Lockdown Mode Overview	15
	Features	16
	Device Prerequisites	17
	Related Documents	17
	Data Isolation and use of HOME Directories.....	17
	Migration to Agent Lockdown Mode Environment.....	18
2	Installing and Customizing Agent Lockdown Mode	19
	System Requirements.....	20
	Platform Support.....	20
	Installation Prerequisite: The UPGRDMOINT File.....	20
	Installing the HPCA Agent.....	20
	New Installation of the HPCA Agent	21
	Migration from a Lower Version to HP OVCM 5.11.4 or HPCA 7.8.1	21
	Enabling the Secure Lockdown Mode	22
	setsecure.bat File.....	22
	Agent Lockdown Mode: HPCA Agent Directory Structure.....	24
	Directory Structure in a non-Agent Lockdown Mode	24
	Directory Structure in Agent Lockdown Mode.....	25
	Log and Data Directories	27
	IDMROOT Directory	27
	IDMSYS Directory.....	27

3	Configuring HPCA Agent Security	29
	Access Control Lists	30
	Ensuring Security with ACLs	30
	Setting ACLs	30
	Agent Lockdown Mode: Known Limitations	32
	Connect Types	32

1 Introduction

This chapter describes:

- The purpose of this guide, including:
 - Its intended audience and objective.
 - Some background information on agent security.
 - An overview of the approaches available for locking down the agent environment.
 - Prominent features of Agent Lockdown Mode.
- The HP Client Automation (HPCA) agent environment differences when Agent Lockdown Mode is enabled.
- Migration to and configuration of Agent Lockdown Mode.

HP Client Automation Agent

The HP Client Automation (HPCA) agent installed on a target device allows an HPCA administrator to:

- Automate deployment of applications
- Update, repair, and delete applications
- Inspect hardware and software

The HP Client Automation agent (HPCA Application Manager and HPCA Application Self-service Manager) runs on the agent computer. It communicates with the HPCA Configuration Server to gather information about the desired state of the agent computer, and compares that information to the actual state of the agent computer. Then, the HPCA agent makes adjustments to make the actual state match the desired state.

The HPCA agent has several sub-features that perform a variety of functions. [Table 1](#) lists and describes the HPCA agent's sub-features.

Table 1 HPCA agent sub-features


Sub-feature	Description
HPCA Application Manager	Use this sub-feature to distribute mandatory applications throughout the enterprise.
HPCA Application Self-service Manager	With this sub-feature, subscribers can install, remove, and update optional applications that are available to them in a service list.
HPCA Inventory Manager	This sub-feature allows you to collect hardware information and send it to the Inventory Manager for collection and reporting.
HPCA OS Manager	This sub-feature controls the provisioning of operating systems.
HPCA Patch Manager	This sub-feature analyzes and manages security patches.

If you install the HPCA Application Self-service Manager and HPCA Application Manager, you can decide whether an application is mandatory or optional, and specify who controls the installation of the application. By adding the Inventory Manager, you can also discover the hardware and software configurations of HPCA agent computers.

Audience and Objective

This guide is targeted at systems administrators who manage the HP Client Automation products in their corporate environment.

This guide presents core client security information and steps for HPCA administrators for locking down HPCA agents.

 This guide uses the terms **MACHINE** and **SYSTEM**. These terms are interchangeable, but their varied use is done to accurately reflect how they are used in a HPCA environment.

Background

The HPCA agent is used to deploy operating systems, software, patches, and monitor vulnerabilities and application usage on managed devices. The HPCA agent communicates with the HPCA Configuration Server to download the required information.

Typically, there is a machine (**SYSTEM**) mode and user mode on the HPCA agent. The machine mode runs with elevated privileges, whereas the user mode runs with potentially limited privileges. The machine mode is controlled by the site administrator who manages software deployment in the enterprise while user mode is controlled by the end user who logs into the system.

In a typical environment, a site administrator deploys all the standard applications to a device using the machine mode. A user who logs in to the system might deploy optional software that has been entitled to him/her by the site administrator.

To install applications on a system, the install process must run with elevated privileges. Since the end user can decide which entitled applications to deploy, the **MACHINE** mode needs to be available to the user and the site administrator.

The HPCA agent uses an object model to manage software on the systems. The object model is retrieved from the HPCA Configuration Server and stored on the target device as objects. These objects are accessed using SYSTEM or end user privileges. There are SYSTEM level objects such as installation programs which are used by the HPCA agent to control its processing and implementation specific information used during deployment. Conversely, there are USER level objects as well.

Entitlement Settings

In general, the HPCA administrators would have the following entitlement scenarios for deploying software into target devices:

- **Machine Only Entitlements:** These are applications, which are deployed using the SYSTEM context. These applications are owned by the machine level.
- **User Only Entitlements:** These are the applications, which are deployed using the user context. Hence, entitlements are done in per user per user based policy, and the application is owned by the end-user of the target devices.
- **Machine/User (Hybrid) Entitlements:** These are applications, which are partly deployed by the SYSTEM and partly deployed by the USER. Before running the first user connect, the Machine side has to run first. This is called **Priming Connect**. To facilitate the Priming Connects, there is a MACHDEF.EDM file, which will be created by collecting the Connect parameters from the HPCA administrator during the installation.

Machine Defaults (MACHDEF.EDM)

MACHDEF is an abbreviation for Machine Defaults. The MACHDEF.EDM file carries the Machine default parameters. [Table 2](#) lists the variables of MACHDEF.EDM along with their description and values.

Table 2 MACHDEF Variables

VARIABLE	DESCRIPTION	VALUE
STARTDIR	The directory under machine IDMLIB	SYSTEM, \$MACHINE, or \$USER

VARIABLE	DESCRIPTION	VALUE
UID	The value used for entitlement	\$MACHINE or \$USER
IP	The IP address of the HPCA Configuration Server	A valid IP address or IP name
COP	Client Operation Profile resolution enabled	Y or N
ASK	Prompt user	Y or N

When your HPCA environment has Radia Software Manager (RSM) with differing user entitlements and no machine entitlement, you should specify the values of MACHDEF variables as follows:

STARTDIR	\$USER
UID	\$USER

Similarly, when you want to entitle applications to machine and user and machine has all the user applications entitled, you should specify the values of MACHDEF variables as follows:

STARTDIR	SYSTEM
UID	\$MACHINE

After the product is installed, if you always run a Priming Connect for the machine side, where the machine has all the entitlements, you will not need a MACHDEF.EDM value to get all the default parameters.

Potential Security Concerns

HPCA administrators may have a variety of reasons for choosing not to deploy security lockdown restrictions on end users:

- Users may all be machine administrators
- Users may all be trusted users. Another means of security may be employed

Implementations that choose not to secure their HPCA managed devices folders may be exposed to a variety of issues, including:

Local Tampering of Data Store

The HPCA agent data store is a directory in which the user and the machine modes share objects. This is called `IDMROOT`. The user can influence the machine mode to do unauthorized operations by tampering with the object content.

A locked down HPCA agent resolves the tampering of the object content. When running in Agent Lockdown Mode, the HPCA agent segregates the user and the machine data stores so that the data objects are only accessible by its authorized processing context. The HPCA agent directory layout when running in Machine-only Lockdown Mode differs from Agent Lockdown Mode to ensure that the `MACHINE` and `USER` objects are isolated and can be secured independently.

Secure Environment Trust Issues

- Who is trusted?
- What is trusted?

Can the user or the remote site administrator that has contacted the HPCA Configuration Server be trusted to perform a task? Can the parameters that were passed from the user side to the machine side be trusted? Is the HPCA agent requesting to be connected to a valid device on the network or is it requesting access to a non-authorized HPCA Configuration Server?

These problems are solved by enabling the Agent Lockdown Mode HPCA agent. The HPCA agent only trusts IP addresses that are specified in secured locations (for example, `SAP` object) and cannot be modified by a non-privileged user. When a Client Operations Profile (COP) connect has run, there is a secure list of servers to which the HPCA agent is allowed to communicate.

Agent Lockdown Mode Overview

The goal of the HPCA agent with lockdown mode is to ensure the integrity, confidentiality, and availability of the content and methods that are stored and used by the management agent. The HPCA agent prevents non-privileged users from tampering with critical system-level content or breaching confidentiality by viewing content they should not have access to.

Agent Lockdown Mode extends Machine-only Lockdown Mode and when enabled, this feature allows HPCA agent processes running on behalf of a USER to run in a more secure manner. The context switching between USER and SYSTEM mode is kept to a minimum and occurs only when needed and with proper controls. As the context switching is kept to a minimum, you need not give higher access privileges to the USER to run the HPCA agent processing.

The directory structures on the managed device are changed to isolate SYSTEM and USER data to prevent local tampering of HPCA agent owned objects. In this mode, the SYSTEM and each user get their own private data stores. This prevents users from tampering with SYSTEM or each other's objects (for example USER Joe cannot access the data files and confidential information of USER Tom), as you could have users with different levels of privileges using the system.

In Microsoft Windows, the operating system allows defining HOME directories for each user. The HPCA administrator configures the user data store to use the HOME directory style approach. The HPCA processing methods and other objects are owned by the SYSTEM user. This is done intentionally so that migration is less disruptive to the SYSTEM mode for existing customers who might want to migrate to Agent Lockdown Mode.

To solve the "What to trust" issue, the HPCA agent does not trust any parameters that are passed from a USER request (for example, RADSKMAN command). The SYSTEM side uses predefined, trusted, and secure objects either at installation time or by performing a priming connection after installation to the HPCA Configuration Server to get the default parameters.

The implementation of security permissions is the responsibility of the HPCA administrator. Sample processing scripts are provided for setting Access Control Lists (ACLs), which isolate USERS from the SYSTEM and other USERS. A sample ACL batch file, `setsecure.bat`, is included on the HPCA media and can be referred to configure security in your environment. For more information, see [Access Control Lists](#) on page 30.



Be wary of the “Everyone” group on Windows operating systems. If you remove privileges for a specific user, be sure to remove access for the “everyone” group also, because the user is still part of that group and as such, can log into the machine.

Features

- The HPCA agent runs using the existing HPCA infrastructure. There are no changes required for the HPCA infrastructure with the exception of policy entitlements.
- USER directories are moved from the `IDMROOT` directory to `CSIDL_LOCAL_APPDATA\HPCA\Agent`.
- MACHINE privately owns all of `IDMROOT`. No read or write access by USERS.
- USERS get private `Log` and `Data` directories specific to each user.
- USERS can add a custom directory with their own script to set access permissions. USERS can use the sample statements from the `setsecure.bat` file to create a custom script that can be used to set access permissions after installation or upgrade of the HPCA agent.
- MACHINE’s `Log` and `Data` directories cannot be accessed by USERS.
- `IDMSYS\DEFAULTS` stores the priming objects that are needed to run a HPCA agent.
- `ZSYSACCT=Y` applications will be wholly owned by MACHINE; USERS cannot access the objects for the specified application.
- USERS have access to run some files from `IDMSYS`. However, SYSTEM methods (such as, `daemons`, `upgrdmaint`, and `radtimeq`) will be run by MACHINE only.
- USERS cannot create `TIMER` instances.
- MACHINE side implementations like HPCA Patch Manager and HPCA OS Manager, which are entirely owned by the SYSTEM, will keep working without any changes.
- USER MSI files will be stored in a separate directory.
- MACHINE side MSI files will not be accessible to USER.

Device Prerequisites

The following environmental conditions must be met in order to ensure the proper functioning of the HPCA agent.

- A Microsoft Windows NTFS-based configuration; setting security using **Access Control Lists (ACLs)** will not work with FAT16 or FAT32 file systems.

Related Documents


This section provides a list of documents that are related to the topics that are discussed in this guide.

- *HP Client Automation Application Manager and Application Self-service Manager Installation and Configuration Guide*
- *HP Client Automation Administrator User Guide*

Data Isolation and use of HOME Directories

For HPCA administrators who are enabling Agent Lockdown Mode, there are choices to be made on where to isolate and store the USER data. In Microsoft Windows, the operating system defines “home” directories for each user and inherently prevents unauthorized access to these directories.

There are several directories that can be used to separate user data. A typical implementation will have the HPCA administrator configure the user data store to use the home-directory approach. This results in an existing managed device’s data stores being exclusively owned and accessible by the SYSTEM. This approach facilitates the migration of an existing environment to Agent Lockdown enabled environment.

 If, in your environment, the applicable directory is hidden, use the operating system-specific “view hidden folders” procedure to access and view it.

For HP OVCN 5.11 and HPCA 7.80, the home directory is:

- **Windows 2000, Windows XP, and Windows 2003 Server:**

C:\Documents and Settings\username\Local Settings\
Application Data\HPCA\Agent

For HPCA 7.80, the home directory is:

- **Windows Vista, Windows 7 and Windows 2008 Server:**

C:\Users\username\AppData\Local\HPCA\Agent

Migration to Agent Lockdown Mode Environment

The HPCA administrator must be able to migrate from a HPCA agent non-lockdown enabled environment to a lockdown enabled environment. Agent Lockdown Mode enablement supports:

- New installations
- Existing installations

Once the Agent Lockdown mode is enabled:

- The Lockdown enabled HPCA agent runs using the same HPCA infrastructure. No infrastructure changes are required.
- The Lockdown enabled HPCA agent does not support USER-based TIMERS used during scheduling on a managed device. Only SYSTEM-based TIMERS are supported.
- The HPCA agent code no longer uses Microsoft Windows Registry or environment variables to determine the HPCA root directory location. Modify any customized scripts or other code that relied on this technique.
- NVD.INI has been moved from IDMROOT to IDMSYS.

For more information, see the sections [IDMROOT Directory](#) and [IDMSYS Directory](#), on page 27.

2 Installing and Customizing Agent Lockdown Mode

This chapter describes:

- The system requirements for the HPCA agent as well as the operating systems supported by HPCA.
- The installation prerequisites and configuration information that pertains to the UPGRDMAINT file.
- Deployment of patch.
- Enabling the Secure Lockdown mode.
- The installation of the HPCA agent to a new and clean device.
- The migration of a HPCA agent.
- A look at the HPCA agent directory structure, and how it changes when Agent Lockdown mode is enabled.



For HP OVCM 5.11.4 and HPCA 7.8.1, the base products are HP OVCM 5.11 and HPCA 7.80 respectively.




Before you perform the remove, repair, or modify operations for a HPCA agent installer, revert the ACL settings that you have applied on the HPCA agent directories.

System Requirements

To ensure the successful installation and operation of the security enhancements, following are the system requirements:

- Communications protocol: **TCP/IP** only
- Pentium processor (minimum): **120 MHz**
- Windows NTFS-based file system to ensure support for ACLs

 Only members of Administrator group can install the HPCA agent.

Platform Support

For information about the supported platforms, see the *Release Notes* document for the version of HPCA that is installed in your environment.

Installation Prerequisite: The UPGRDMAINT File

The UPGRDMAINT file contains configuration parameters with which you can customize the installation of the HPCA agent. The file also has parameters that will be applied to the HPCA agent after it is installed. This section focuses on and describes the Agent Lockdown Mode related parameters and settings of UPGRDMAINT.

Installing the HPCA Agent

This section details the installation of the HPCA agent security enhancement. Depending on the version of HPCA you are using, there are various ways for installing the HPCA agent in a Lockdown mode. This section describes the two scenarios, to install or to migrate to the HPCA agent Lockdown mode.

New Installation of the HPCA Agent

This section documents the installation on a device that does not host a previous version of the HPCA agent. If the device has a version of the HPCA agent already installed, uninstall the existing version of the HPCA agent, and install the latest version.

In this scenario, follow these steps:

1. Install the base product; HP OVCM 5.11 or HPCA 7.80.
2. Deploy the patch; HP OVCM 5.11.4 or HPCA 7.8.1 as required.
3. Enable the lockdown mode. For the steps to enable the Lockdown mode, see the section [Enabling the Secure Lockdown Mode](#) on page 22 in this chapter.
4. Restart the agent computer.

Migration from a Lower Version to HP OVCM 5.11.4 or HPCA 7.8.1

Consider a scenario where you are using the lower version of HPCA, say 4.2. Now, if you want to migrate to HP OVCM 5.11.4 or HPCA 7.8.1, follow these steps:

1. Uninstall the lower version of HPCA agent.
2. Install the base version, which is the normal agent mode. Restart the agent computer.
3. Deploy the patch; HP OVCM 5.11.4 or HPCA 7.8.1 as required. Restart the agent computer.
4. Enable the lockdown mode. For the steps to enable the Lockdown, see the section [Enabling the Secure Lockdown Mode](#) on page 22 in this chapter.
5. Run the `secure_migrate.tcl` file to move user objects from the `IDMROOT` folder to the private folder of the respective users. For information on the usage of `secure_migrate.tcl`, see [secure_migrate.tcl File](#) on page 22.
6. Restart the agent computer.

The HPCA agent is installed. If selected, a HPCA Application Self-service Manager icon is placed on the desktop.

secure_migrate.tcl File

Once the Agent Lockdown mode is enabled on the HPCA agent computer, you need to transfer the user data objects to the respective user profiles. The `secure_migrate.tcl` script automatically reads all the data objects in the `IDMROOT` folder, `C:\Program Files\Hewlett-Packard\HPCA\Agent\Lib`, for each user and moves them to the user profile set in the script.

From the command line, run the following command **nvdkit**
secure_migrate.tcl -idmusr *<User-Folder-path>* **-usrmsi**
<User-Msi-Folder-path>.

For Microsoft Windows Vista, Microsoft Windows 7, and Microsoft Windows 2008 Server the *<User-Folder-path>* is:

```
C:\Users\<username>\AppData\Local\HPCA\Agent
```

For Microsoft Windows 2000, Microsoft Windows XP, and Microsoft Windows 2003 Server the *<User-Folder-path>* is:

```
C:\Documents and Settings\<username>\Local  
Settings\Application Data\HPCA\Agent
```

You can move the data objects of all the users at the same time by replacing *<username>* with the value `ZUSERID` in the above mentioned paths.

The *<User-Msi-Folder-path>* is the `IDMUSRMSI` path,

```
IDMUSRMSI="c:\Program Files\Hewlett-Packard\HPCA\Agent\usermsi"
```

Enabling the Secure Lockdown Mode

After deploying the HP OVCM 5.11.4 or the HPCA 7.8.1 patch, you need to enable the secure Lockdown mode in order to limit the access of several directories to the user. In addition, the user cannot create his/her own folders when the Lockdown is enabled.

setsecure.bat File

The `setsecure.bat` file is used for the following purpose:

- Enable the secure Lockdown mode.
- Set Access Control List (ACL) to the HPCA agent directories.

Enabling the Secure Lockdown Mode

In the command prompt on the HPCA agent computer, run the following command:

```
<HPCA Installed Folder>\Agent\setsecure.bat <Source Dir>  
<Target Dir>
```

<Source Dir> is the current installed directory path of the HPCA agent. Before the `setsecure.bat` file is run, make sure to copy it into the HPCA agent install directory.

<Target Dir> is the directory where the user data will be moved to once the secure Lockdown mode is enabled.

Example, <Source Dir> `setsecure.bat .`
`CSIDL_LOCAL_APPDATA\HPCA\Agent`

The Agent Lockdown mode has been enabled. You can also observe that the `NVD.INI` file, which was previously inside the `Lib` folder, is now moved to the HPCA agent installation folder `C:\Program Files\Hewlett-Packard\HPCA\Agent`. Once the file is moved, it is no longer available to the user. A user without administrative rights cannot access folders such as `Log` and `Lib` which they could access before enabling the Lockdown mode.

You can disable the Agent Lockdown mode by re-installing the HPCA agent on the managed device.

Setting Access Control List (ACL)

The `setsecure.bat` file contains sample statements which you can use to create a new script. This customized script can be used to set ACLs in the HPCA environment. Customizing the batch file is an optional task. If you do not customize the `setsecure.bat` file, ACLs will be set using the sample statements provided in the `setsecure.bat` file.

Agent Lockdown Mode: HPCA Agent Directory Structure

The directory structure of the HPCA agent has changed to ensure the security of SYSTEM files, as well as prevent one USER from gaining unauthorized access to another USER's files.

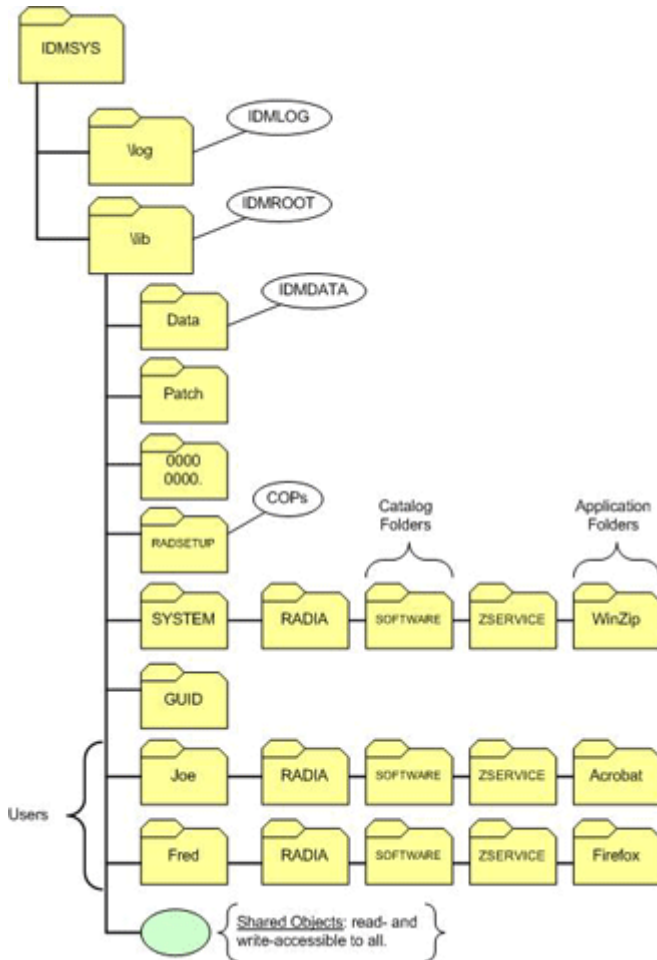


This guide uses the terms MACHINE and SYSTEM. These terms are interchangeable, but their varied use is done to accurately reflect how they are used in a HPCA environment.

Directory Structure in a non-Agent Lockdown Mode

Figure 1 illustrates the directory structure in a non-Agent Lockdown Mode. It is clear that SYSTEM directories are not isolated from USER directories. If the Machine-mode agent Lockdown is not enabled, they may be accessible to any user of the device. Also, various USER directories would be susceptible to unauthorized access, as well as unauthorized modifications.

Figure 1 HPCA Agent Directory Structure in non-Agent Lockdown Mode

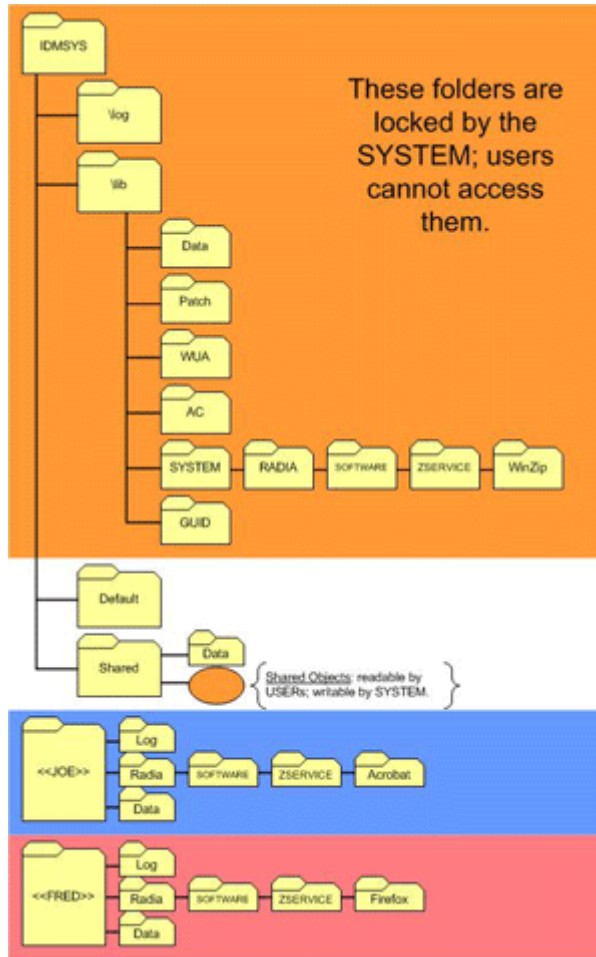


Directory Structure in Agent Lockdown Mode

Figure 2 illustrates the HPCA agent directory structure in Agent Lockdown Mode. The SYSTEM-based directories are no longer on the same “branch” as the USER directories. Therefore, SYSTEM data is secured and can no longer be accessed by any other user of the agent computer — they are accessible only to authorized administrators. Also, each user has its own (USER-

specific) directory, which again, is not on the same “branch” as another user. Hence, it is not susceptible to unauthorized access and modifications.

Figure 2 HPCA Agent Directory Structure in Agent Lockdown Mode



The location of the USER folders (**JOE**, **FRED**, and others) is determined at run time. It is based on the user that has logged in and by the value (in **NVD.INI**) of **IDMUSR=CSIDL_LOCAL_APPDATA\HPCA\Agent**. For example, for user **JOE**, this location would be:

For HP OVCM 5.11 and HPCA 7.80:

On **Windows 2000, Windows XP, and Windows 2003 Server**:
CSIDL_LOCAL_APPDATA is replaced with C:\Documents and Settings\Joe\Local Settings\Application Data.

For HPCA 7.80:

On **Windows Vista, Windows 7, and Windows 2008 Server**:


CSIDL_LOCAL_APPDATA is replaced with
C:\Users\Joe\AppData\Local\HPCA\Agent

Log and Data Directories

Each USER gets isolated and has a private Log and Data directories. These directories cannot be accessed by non-privileged users, thereby ensuring that their contents are also protected from unauthorized tampering. However, these directories can be accessed by HPCA administrators.

IDMROOT Directory

The IDMROOT directory stores the default objects that are created during installation. Although it was previously a shared directory, now its contents will be entirely owned by and exclusively accessible to the MACHINE.

 MACHINE side implementations that are owned by the SYSTEM (such as HPCA Patch Manager and HPCA OS Manager), will continue working without any changes.

The IDMROOT directory includes the scheduler object, ZTIMEQ. In Agent Lockdown Mode, this is owned by the MACHINE, which means that USER connects cannot write to ZTIMEQ or create timer instances.

IDMSYS Directory

The IDMSYS directory stores all the installer programs (.exe files), DLLs, the configuration file (NVD.INI), and shared lib files. IDMSYS\DEFAULTS stores the priming objects that are needed to run a HPCA agent. USERS have the authority to run some of the files from IDMSYS, but daemons, UPGRDMAINT, and RADTIMEQ will be run by MACHINE only.

See [Agent Lockdown Mode: Known Limitations](#) on page 32 for additional information.

3 Configuring HPCA Agent Security

This chapter describes:

- How to set Access Control Lists to enable Agent Lockdown Mode HPCA agent environment.
- The known limitations of the Agent Lockdown Mode.
- The various types of HPCA agent connections to the HPCA Configuration Server.

Access Control Lists

To enable Agent Lockdown Mode on the HPCA agent, an HPCA administrator needs to set the proper **Access Control List (ACL)** permissions, so that certain directories are not accessible by Microsoft Windows “Standard Users.” Use the sample batch file `setsecure.bat` to enable Agent Lockdown Mode. For more information, see the section [Enabling the Secure Lockdown Mode](#) on page 22.


Ensuring Security with ACLs

The ACLs need to be customized based on the environment. For example, if multiple users are included in an *Administrators* group on your devices, but you don’t want all of these users to have access to the secured folders, you must do one of the following:

- Revise the memberships of that Administrators group to include only the administrators who are authorized to access the secured folders.
- Remove access for that Administrators group and specify which individual administrators can access the secured folders.

Setting ACLs

The HPCA agent installer creates temporary environment variables, so that the batch script can access them.

 These variables are created to be used exclusively by the batch script and are automatically deleted when the HPCA agent is installed.

The script blocks access to the following services by standard users, who are not authorized to run them.

- `Radexecd`: This is the Notify Daemon.
- `Radsched`: This is the Scheduler Daemon.
- `Radstgms`: This is the MSI Redirector.

Only the `MACHINE` can access these modules.

The script also blocks access to the following two stand-alone applications by the standard users, who are not authorized to run them.

- Radtimeq
- Upgrdmaint

Only the MACHINE can access these modules.

Table 3 describes the access levels for the new directories, along with the applicable mnemonic from NVD.INI.

- SYSTEM access is read- and write-accessible for all these directories.
- USER access values are: read-only (**R**), read- and write-accessible (**RW**), no access (**N**).

Table 3 New Directory Access Levels

Mnemonic	USER Access	Example
IDMSHRDATA	R	C:\PROGRA~1\HEWLET~1\HPCA\Agent\SHAREDDATA
IDMPUBLIC	RW	C:\PROGRA~1\HEWLET~1\HPCA\Agent\PUBLIC
IDMUSR	RW	CSIDL_LOCAL_APPDATA\HPCA\Agent\
IDMUSRMSI	RW	C:\PROGRA~1\HEWLET~1\HPCA\Agent\USERMSI\
IDMSYS	R	C:\PROGRA~1\HEWLET~1\HPCA\Agent\
IDMLIB	N	C:\PROGRA~1\HEWLET~1\HPCA\Agent\Lib\
IDMLOG	N	C:\PROGRA~1\HEWLET~1\HPCA\Agent\Log\
IDMDATA	N	C:\PROGRA~1\HEWLET~1\HPCA\Agent\Lib\Data\
NONE-CACertificates	R	C:\PROGRA~1\HEWLET~1\HPCA\Agent\CACertificates\
NONE-DEFAULTS	R	C:\PROGRA~1\HEWLET~1\HPCA\Agent\DEFAULTS\

Agent Lockdown Mode: Known Limitations

Following are the known limitations of Agent Lockdown Mode. Note that some of these are intentional limitations to ensure the security aspect of the HPCA agent.

- Agent Lockdown Mode does not support FAT16 or FAT32 file systems because these do not support ACLs.
- USER connects cannot create TIMER instances. This is achieved by locking out ZTIMEQ as well as removing execute permissions to `radtimeq.exe`.
- Maintenance is entitled to MACHINE only; USERS cannot initiate HPCA agent maintenance.

Connect Types

The Agent Lockdown Mode enabled HPCA agent can support all of the various types of connects to the HPCA Configuration Server. The types of connects are:

- USER
- MACHINE
- MACHINE/USER

Also, the HPCA agent connect process runs several methods (such as `initmeth.rex` and `exbexit.rex`) in the proper (MACHINE or USER) context, thereby ensuring that existing customer-implemented customizations are not affected.

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: