

DICOM Integration Guide

Release: 8.0

190-0012 5.0

*HP Medical Archive
solution*

DISCLAIMER

While every reasonable effort has been made to achieve technical accuracy and completeness, information in this document is subject to change without notice and does not represent a commitment on the part of Bycast Inc., or any of its subsidiaries, affiliates, licensors, or resellers. There are no warranties, express or implied, with respect to the content of this document.

Features and specifications of Bycast® products are subject to change without notice.

This manual contains information and images about Bycast Inc., its fixed content storage systems, and its other products that are protected by copyright and furnished under terms of a license agreement.

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

Copyright ©2008 by Bycast Inc. All rights reserved.

Proprietary and Confidential

Bycast® and StorageGRID® are trademarks of Bycast Inc. Their related marks, images, and symbols are the exclusive properties of Bycast Inc.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation.

Adobe® and Acrobat® are registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

All other brands, product names, company names, trademarks, and service marks are the properties of their respective owners.

Copyright (c) 1991, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Contents

Preface	7
Purpose	7
Currency	7
Intended Audience	8
References	8
Using this Guide	9
Conventions	9
1 DICOM Integration Preparation	11
DICOM Integration Overview	12
Assumptions	12
Process Overview	12
Materials Checklist	13
2 Enable or Update DICOM Connections	15
Process Overview	16
Preparation	16
Enable the DICOM Option	17
Acquire Updated Deployment Grid Specification File	18
Provision the Grid	18
Enable DICOM	23
Enable DICOM Connections	23
Define the DICOM Application Entity	23
Enable DICOM AE TCP/IP Connection	26
Change an Existing DICOM Integration	27
Changing DICOM Entity Access	27
Deleting DICOM Access	28
3 Client DICOM AE Integration	31
Process Overview	32
Client Device Settings	33
AE Title (Client)	33
IP Address (Client)	33
Port (Client)	34
Grid Settings	34
AE Title (Grid)	34
IP Address (Grid)	34
Port (Grid)	34
Completion	35

4	DICOM Integration Verification	37
	Process Overview	38
	Test Setup	38
	Test Case Overview	40
	Completion	41
	DICOM Interoperability Testing Failure	41
	Test Cases	41
	1: C-ECHO SCU	41
	2: C-STORE SCU	42
	3: C-STORE SCU with Storage Commitment	42
	4: C-FIND SCU	43
	5: C-MOVE SCU and C-STORE SCP	44
A	Grid Access for Client Applications	45
	Overview	46
	Profiles	47
	IP Ranges	47
	Group ID	48
	Protocol Permissions	48
	Configuring an IP Range	49
	HTTP Configuration	50
	Overview of HTTP Configuration Process	50
	HTTP Advanced	51
	HTTP Entities	54
	DICOM Configuration	54
	Validating DICOM Associations	54
	DICOM Profiles	56
	Advanced Config Profiles	58
	DICOM Partitions	62
	DICOM Examples	64
	Overview of DICOM Configuration Process	64
	Configuring Access Using a Simple DICOM Profile	65
	Configuring Access Using a Complex DICOM Profile	70
	Configuring Access Using a Coerce Tag Profile	77
B	DICOM Device Test Report	81
	Results Summary	82
	DICOM Client Identification	82
	Test Results	82
	1: C-ECHO SCU Report	83
	Recorded Data	83
	Additional Comments	83
	Expected Results	83

2: C-STORE SCU Report	84
Recorded Data	84
Additional Comments	84
Expected Results	84
3: C-STORE SCU with Storage Commitment Report	85
Recorded Data	85
Additional Comments	85
Expected Results	85
4: C-FIND SCU Report	86
Recorded Data	86
Additional Comments	86
Expected Results	86
5: C-MOVE SCU and C-STORE SCP Report	87
Recorded Data	87
Additional Comments	87
Expected Results	87
C Connectivity	89
Service Laptop Requirements	90
Browser Settings	90
NMS Connection Procedure	91
Security Certificate	92
Log In	92
Enable Pop-ups	93
Log Out	93
Command Shell Access Procedures	93
Log In	93
Accessing a Server Remotely	94
Log Out	95
Glossary	97

Preface

Purpose

This document is intended to guide you through the process of integrating the HP Medical Archive solution system with client entities that use the DICOM protocol to connect, associate, and conduct data transactions. It covers the process for enabling access on the grid side, making settings on the remote DICOM Application Entity (AE), and verifying operation of the grid integrated with the client entity.

The specific operation of client DICOM AEs is beyond the scope of this guide. You are assumed to have in-depth knowledge of DICOM devices and can determine the procedure needed to execute the required operations. As well, you must understand the provisioning and expansion processes, as documented in the *Expansion Guide*.

The HP MAS is assumed to have been fully installed and integrated with the customer's network. Consult the *Installation Guide* and the *Administrator Guide* for details.

The objectives of this document are to enable trained technicians to:

- Deploy the DICOM option on a running grid (post-installation addition)
- Configure profiles and enable DICOM protocol connections to the HP MAS
- Configure client DICOM AEs to access the grid
- Verify the integration

Currency

This edition of the *DICOM Integration Guide* is **revision 5.0**.

The content is current with the HP MAS software **Release 8.0**.

To find the version number of the existing deployment:

1. Access the NMS interface using the “Vendor” account (see “[NMS Connection Procedure](#)” on page 91).
2. Go to **AN1-A-1 ▶ SSM ▶ Services ▶ Overview**.
3. Scroll to the bottom of the content frame to view the Packages section. The Version column for the storage-grid-release package indicates the installed suite version number.

If the grid deployment is a different release, update the deployment to Release 8.0 before proceeding to integrate DICOM clients or consult the revision of this guide that is current with your software. Consult the HP Software Depot for update information.

Intended Audience

The content of this guide is intended for trained HP technical staff and authorized agents responsible for field integration of the DICOM protocol on the HP MAS system.

You are assumed to have a general understanding of the HP MAS deployment and an in-depth understanding of the DICOM protocol and DICOM AEs. A fairly high level of computer literacy is assumed, including knowledge of networking using TCP/IP.

References

This document assumes familiarity with many terms related to computer operations and network communications. There is wide use of acronyms.

The *HP MAS DICOM Conformance Statement* should be consulted for information about how HP MAS conforms to the DICOM standard, including such details as supported SOP Classes.

Integration and verification requires knowledge of the HP MAS Network Management System (NMS) interface. For more information, see the *Administrator Guide*.

For information and procedures on the provisioning and expansion processes, see the *Expansion Guide*.

Hardware at the customer site is assumed to be installed, configured, and tested. The DICOM option must be included in the product purchase, either initially or as an add-on after purchase.

Using this Guide

Product guides are available in Adobe® Acrobat® Portable Document Format (PDF). You may print copies of the PDF editions for internal use but all copies must be treated as proprietary and confidential; *not* for general distribution.

Conventions

This guide adheres to conventions for terminology to avoid confusion or misunderstanding. There are also conventions for typography to enhance readability and usefulness of the text.

You may print copies of the PDF editions for internal use but all copies must be treated as proprietary and confidential and *not* for general distribution.

This guide uses the style conventions shown below.

Table 1: Style Conventions

Element	Meaning
Sans-serif	Field prompts, names of windows and dialogs, messages, and other literal text in the interface are shown in sans-serif, for example the LDR State menu, or the Log In window.
Bold	Items upon which you act are shown in bold. <ul style="list-style-type: none">• Sequences of selections from the navigation tree, tabs, and page options, for example: Go to LDR ► Configuration.• Buttons or check boxes, for example click Apply Changes or Acknowledge.• Keys, such as <Tab>. Where combinations are to be entered, they are noted as <Alt>+<F7>. Where key sequences are needed, they are noted without the "+", for example: <space>Y<Enter>.
<i>Italics</i>	Titles of other documents are shown in italics. Items that require emphasis also appear in italics.

Table 1: Style Conventions

Element	Meaning
Blue	Cross-references and hyperlinks are shown in blue.
Monospace	Coding samples or interactions with a command shell are shown in the fixed space font: <code><?xml version=1.0 ?></code>
<name>	Angle brackets indicate variable and parameter names.
Monospace Bold	<p>Commands issued in a command shell use a fixed space bold font, for example: Enter postinstall.sh start</p> <p>For such commands, you must press <Enter> after you have typed the command.</p>
<i>Monospace Bold Italics</i>	<p>Coding samples or terminal interactions may include variable elements intended to be replaced by actual data. In these cases, the variable elements are shown in italics as illustrated in this sample.</p> <div data-bbox="602 823 1349 974" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #f0f0f0;"> <pre># ssh <i>IPaddress</i> login as: <i>accountname</i> password: <i>password</i> Last login: Tue Aug 17 19:32:30 2004 ...</pre> </div>

DICOM Integration Preparation

Prerequisites and preview

Chapter Contents

DICOM Integration Overview	12
Assumptions	12
Process Overview	12
Materials Checklist	13

DICOM Integration Overview

Assumptions

This guide to the integration of an HP MAS grid with remote DICOM client entities assumes you are familiar with the product's general design, configurations, and options. The process further assumes that the hardware has been installed, connected, and configured to specifications.

If DICOM is being integrated as an add-on after purchase and initial installation, you must also be familiar with the provisioning and expansion processes as described in the *Expansion Guide*. You must acquire the DICOM integration details from the customer and then send the Grid Specification file, exported from the NMS, to Support. A Grid Configuration package is returned via e-mail. From this, the grid is provisioned, and a SAID package and grid task to enable DICOM are generated. For more information on provisioning and expansion, see the *Expansion Guide*.

This document guides you through the process of DICOM integration, using the SAID package generated during provisioning, and verification of the integration.

Process Overview

There are two possible routes that lead to the integration of DICOM clients:

- Adding DICOM clients as part of the initial HP MAS installation.
- Adding the DICOM option or additional clients to an established installation.

Adding DICOM to an Existing HP MAS Grid

When adding the DICOM option, you must provision the grid and generate a SAID package. This will create a new Grid Task (`enable-dicom.txt`) that when run enables the DICOM option.

Adding or Changing an Existing DICOM Integration

Adding or changing the integration of DICOM client entities to an existing deployment also involves provisioning the grid and generating a new SAID package.

Preparation

This guide assumes that HP MAS software has already been installed.

To prepare for a DICOM integration you must acquire a new Grid Configuration package. After acquiring a new Grid Configuration package, provision the grid, and then perform DICOM integration and verification. For more information, see [“Acquire Updated Deployment Grid Specification File”](#) on page 18.

You may want to photocopy report forms from [Appendix B](#) of this guide for use in verifying the integration. Copy one set for each entity being integrated and verified.

Materials Checklist

Before leaving for the customer site, ensure you have:

- The service laptop
- Customer Questionnaire
- Access to the two Provisioning USB flash drives used during the original installation process to provision the grid

These USB flash drives should be available at the customer site. It is suggested that you confirm access to these USB flash drives before leaving for the customer site. If you cannot reuse these USB flash drives, you must provide two new USB flash drives (at least one GB in size).

- The *Expansion Guide*.
- The *Administrator Guide*.
- This guide.

Take these items to the customer’s site to perform the integration.

Enable or Update DICOM Connections

Chapter Contents

Process Overview.....	16
Preparation.....	16
Enable the DICOM Option.....	17
Acquire Updated Deployment Grid Specification File ...	18
Provision the Grid.....	18
Enable DICOM.....	23
Enable DICOM Connections	23
Define the DICOM Application Entity.....	23
Enable DICOM AE TCP/IP Connection.....	26
Change an Existing DICOM Integration	27
Changing DICOM Entity Access	27
Deleting DICOM Access.....	28

Process Overview

This chapter covers the two processes that take place on the HP MAS side of the integration:

- enabling DICOM
- enabling DICOM connections

The first process is for deployments that do not yet have the DICOM option enabled.

The second process defines the DICOM Application Entities (AEs) that are permitted to use the HP MAS. This chapter describes how to create a DICOM Application Entity (AE) definition for each DICOM AE that is permitted to use HP MAS. This definition takes two parts: the connection permission to establish a TCP/IP connection with the grid, and the permission profile the entity has for DICOM transactions.

The mechanism that enables DICOM access is controlled by the Grid Management ► Grid Configuration ► IP Ranges and Grid Management ► Grid Configuration ► DICOM components. To understand the workings of these components, and to see examples of how to configure a custom profile, consult [Appendix A](#) of this guide. You should be familiar with the concepts of connection permissions and profiles before starting any of these activities.



WARNING **Altering connection configurations and creating custom profiles are considered highly advanced activities that should not be undertaken casually.**

Preparation

Any change to a client integration requires a grid configuration request to Bycast that references the customer's Grid ID and includes an updated Customer Questionnaire and the latest Provisioned Grid Specification file copied from the Admin Node hosting the CMN service. A new Deployment Grid Specification file is returned.

To facilitate future maintenance, you must update the Customer Questionnaire.

Field	Element	Data Type	Description
Client Info #n	Description	Text	Descriptive name for the DICOM client entity
	AE Title	Text	AE Title of remote DICOM client device
	IP	IP Address	IP address of remote DICOM client
	Port	Numeric	TCP port used by remote DICOM client
	Access	Text	Client permissions to access the grid

To make changes to a client integration you need:

- Printed copies of:
 - The Passwords.txt file.
 - The Configuration.txt file.
 - The Customer Questionnaire.
- A service laptop computer equipped as noted in [“Connectivity” on page 89](#).
- The *Administrator Guide*.
- This guide.

Enable the DICOM Option

Follow the instructions in this section to enable the DICOM option.

For detailed procedures on how to work with grid tasks, consult the *Administrator Guide*.

To enable the DICOM option:

1. Acquire an updated Deployment Grid Specification file. For more information, see [“Acquire Updated Deployment Grid Specification File” on page 18](#).
2. Provision the Grid. For more information, see [“Provision the Grid” on page 18](#).

3. Enable DICOM. For more information, see “Enable DICOM” on page 23.

Acquire Updated Deployment Grid Specification File

Copy Provisioned Grid Specification File

Copy the Provisioned Grid Specification file from the Admin Node hosting the CMN service and send it along with the Customer Questionnaire to Bycast. Bycast updates this grid specification file and returns a new Deployment Grid Specification file.

To copy the Provisioned Grid Specification file:

1. Log into a command shell session on the Admin Node. Press **<Alt>+<F1>** from the Server Manager console to access a new command shell session on the server. Use the account name `root` and the password for the node provided in the `Passwords.txt` file.
2. Insert a USB flash drive into the Admin Node server.
3. Copy the latest version of the Provisioned Grid Specification file to the USB flash drive. Enter:

```
copy-grid-spec
```

The Provisioned Grid Specification file is copied to the USB flash drive.
Optionally, you may specify a directory other than the USB flash drive to which the Provisioned Grid Specification file can be saved:

```
copy-grid-spec <directory>
```
4. Transfer the Provisioned Grid Specification file from the USB flash drive to the service laptop.
5. Send the Provisioned Grid Specification file along with the Customer Questionnaire to Bycast.
The Provisioned Grid Specification file is updated to include DICOM and a Deployment Grid Specification file is returned via e-mail.
6. When the Deployment Grid Specification file is returned, save it to the service laptop and begin the provisioning process.

Provision the Grid

Before enabling DICOM, you must provision the grid and generate a new SAID package. Generating a new SAID package creates a new grid task which is used to enable DICOM.

To provision the grid:

1. Update the Provisioning USB flash drive. For more information, see “Update Provisioning USB Flash Drive” on page 19.
2. Run the Provision script. For more information, see “Run Provision Script” on page 20.
3. Confirm Provisioning. For more information, see “Confirm Provisioning” on page 21.
4. Back up the Provisioning USB flash drive. For more information, see “Back Up Provisioning USB Flash Drive” on page 22.

Update Provisioning USB Flash Drive

When the Deployment Grid Specification file is returned, confirm its filename and save it to the Provisioning USB flash drive.

To update the Provisioning USB flash drive:

1. Save the Deployment Grid Specification file to the root directory of the Provisioning USB flash drive created during the original installation of the grid.

2. When saving the Deployment Grid Specification file, confirm its filename. The following naming convention is used:

GID<grid_ID>_REV<revision_number>_GSPEC.xml

For example, GID1234_REV2_GSPEC.xml

Where REV<revision_number> refers to the revision number of the Deployment Grid Specification file. The revision number must be the <revision_number> plus one of the Provisioned Grid Specification file sent to Bycast for updating. For example, if the Provisioned Grid Specification <revision_number> was one (REV1) then the <revision_number> of the returned Deployment Grid Specification file must be two (REV2). Any other revision number will result in the failure of provisioning.

3. Delete any other grid specification files from the root directory of the Provisioning USB flash drive.

The Provisioning USB flash drive must only contain the Deployment Grid Specification file that is configured for grid expansion.



CAUTION

The USB flash drive must only contain one Deployment Grid Specification file at the root level. If more than one Deployment Grid Specification file is detected, an error occurs and provisioning will fail.

Run Provision Script

Provisioning the grid creates a SAID package that must be saved to the Provisioning USB flash drive.

To provision the grid:

1. Log onto the Admin Node hosting the CMN service.
1. Enter:
`provision`
2. When prompted, insert the Provisioning USB flash drive containing the Deployment Grid Specification file.



CAUTION It is critical to the successful creation of the SAID package and thus installation of the grid that data in the Grid Specification file is correct and complete.

3. When prompted, enter the gpt repository passphrase and press **<Enter>**.

A deployment-specific SAID package and encrypted repository backup are generated and saved to the Provisioning USB flash drive. Grid provisioning is complete. When provisioning is complete, "Provisioning complete" is displayed.

The gpt repository passphrase was created during the original provisioning of the grid. This passphrase should have been documented during the original provisioning of the grid.

4. Store the Provisioning USB flash drive in a safe and secure place.

NOTE The Provisioning USB flash drive is left on-site with the customer to store in a safe and secure location.

5. After provisioning the grid, confirm provisioning. For more information, see "[Confirm Provisioning](#)" on page 21.

NOTE If provisioning ends with an error message, see the "Troubleshooting" section in the *Expansion Guide*.

Confirm Provisioning



CAUTION It is **IMPERATIVE** that you confirm that the configuration of your Grid Specification file and that the SAID package is correct before proceeding. If errors occur contact Support.

After provisioning has completed, confirm provisioning by evaluating the generated SAID package against data contained the Customer Questionnaire.

To confirm provisioning:

1. Insert the Provisioning USB flash drive into your service laptop.
2. Copy the zipped SAID package (GID<grid_ID>_REV<rev_number>_SAID.zip) to your service laptop.
3. Extract the zipped SAID package.
4. Confirm the successful generation of the SAID package by checking the contents of the Customer Questionnaire against the Grid Configuration pages available in the doc directory of the generated SAID package.

To open the Grid Configuration pages, double-click the index.html file.

5. If after examining the SAID package and the Grid Configuration pages, you discover an error in your provisioning data:
 - a. Remove the provisioning data from the grid. Enter:
`remove-revision`
 - b. Cancel the pending Grid Tasks for this provisioning. Go to the **CMN ► Grid Tasks ► Configuration** tab. From the **Actions** drop-down menu, select **Cancel** and click **Apply Changes**.
 - c. Update your Deployment Grid Specification file and save it to the root directory of the Provisioning USB flash drive.
 - d. Generate a new SAID package and re-provision the grid. For more information, see [“Provision the Grid” on page 18](#).
 - e. After re-provisioning the grid, confirm provisioning.
6. Back up the Provisioning USB flash drive. For more information see [“Back Up Provisioning USB Flash Drive” on page 22](#).
7. Remove the Provisioning USB flash drive and store it in a safe and secure place.



CAUTION It is critical that you store the Provisioning USB flash drive in a safe secure place, such as a locked cabinet or safe. The Provisioning USB flash drive contains encryption keys and passwords that can be used to obtain data from the grid.

Back Up Provisioning USB Flash Drive

After grid provisioning is complete and confirmed, back up the Provisioning USB flash drive to a second USB flash drive. This backup copy of the Provisioning USB flash drive can be used to restore the grid in the case of an emergency or during an upgrade or grid expansion.



CAUTION It is critical that you store this backup copy of the Provisioning USB flash drive in a safe and secure place, such as a locked cabinet or safe. Store this backup copy of the Provisioning USB flash drive separately from the Provisioning USB flash drive. This backup copy of the Provisioning USB flash drive contains encryption keys and passwords that can be used to obtain data from the grid.

To back up the Provisioning USB flash drive:

1. Insert a USB flash drive in the server.
The flash drive used during the original installation of the grid to back up the Provisioning USB flash drive can be used.
2. Enter:
`backup-to-usb-key`
The latest SAID package and gpt repository (gpt_backup directory) are saved to the backup Provisioning USB flash drive.
3. Remove the backup copy of the Provisioning USB flash drive and store it in a safe and secure place.

NOTE The backup copy of the Provisioning USB flash drive is left on-site with the customer to store in a safe and secure location.

4. After creating a backup copy of the Provisioning USB flash drive, enable DICOM.

Enable DICOM

Grid tasks that are Paused can be resumed. If you Cancel a grid task you cannot restart it while it is in the Historical List. For more information, see the *Administrator Guide*.

To enable the DICOM option:

1. Go to the **CMN ► Grid Tasks ► Configuration ► Main** page.
2. In the **Actions** pull-down menu adjacent to the Enable DICOM grid task, select **Start**.
3. Click **Apply Changes**.

The grid task moves from the Pending list to the Active list. You must wait for the NMS page to auto-refresh before the change is visible. Do not submit the change again.

The task continues to execute until it completes, is paused or aborted manually.

When the task completes successfully, it moves to the Historical list with the description Successful in the Status field. If the task fails, it moves to the Historical list with a description of the error in the Status field.

Wait until the grid task completes before continuing.

If the grid task fails, report the issue to Support to determine the cause of the failure. The integration process must be postponed and a new Grid Task generated. This means provisioning the grid again and generating a new SAID package.

Following the successful execution of the task, you may proceed to integrate DICOM entities.

Enable DICOM Connections

This section assumes that the DICOM option has been enabled on the HP MAS grid. This section outlines how to configure the HP MAS grid to accept DICOM connections from DICOM entities that are enabled to access the grid.

Define the DICOM Application Entity

To enable a DICOM entity to access the HP MAS deployment, you must adjust settings in Grid Management ► Grid Configuration ► DICOM Advanced so that the grid recognizes the DICOM Application Entity (AE). Only the "Vendor" account can make changes in Grid Management ► Grid Configuration.

To define the DICOM Application Entity:

1. Access the NMS interface using the “Vendor” account. (See “[NMS Connection Procedure](#)” on page 91.)
2. Check to see if there are predefined DICOM profiles for the grid:
 - a. Go to **Grid Management ▶ Grid Configuration ▶ DICOM Advanced ▶ Overview**.
 - b. Check to see if there are DICOM profiles defined.
 - c. If there are no suitable profiles defined, create profiles using the instructions in “[Configuring Access Using a Simple DICOM Profile](#)” on page 65. The following standard profiles are useful for most grids:
 - **READ_WRITE**: Commonly used for PACS and modality integration. Provides full DICOM functionality on the grid. That is, S (store), R (retrieve), F (find), M (move), and C (storage commitment) are selected.
 - **READ_ONLY**: Commonly used for diagnostic stations. Provides access to data stored on the grid, but does not allow storing content (that is, R (retrieve), F (find), and M (move) are selected).

These predefined profiles do *not* use:

- a Behavioral Profile (used for integration with specific PACS only, and described in “[Behavioral Profile Name](#)” on page 58)
- a Coerce Tag Profile (used to create a DICOM partition, as explained in “[DICOM Partitions](#)” on page 62)
- an Advanced Configuration Profile (required if the DICOM AE uses a private SOP class, or if some of the entities’ presentation contexts present problems that require you to limit supported SOP classes or change their transfer syntax usage, as described in “[Advanced Config Profiles](#)” on page 58.)

If any of these are required, you must build a custom profile.



WARNING **Creating a custom profile is considered a highly advanced capability that should not be undertaken casually. Consult with HP technical support for assistance.**

3. Go to **Grid Management ▶ Grid Configuration ▶ DICOM ▶ Configuration** tab.






Description	AE Title	IP Range	Port	Via LDR	GRID AE	Profile Name	Actions
				<input type="checkbox"/>			  

Figure 1: No DICOM Entities Enabled

4. Click **Edit**  (if this is the first entry) or **Add**  to add a new DICOM AE.
5. Define a new DICOM AE entry within HP MAS, using the settings defined in the Customer Questionnaire for the site:
 - a. Enter the Description provided for of the entity.
 - b. Enter the AE Title of the entity.
The AE title is case-sensitive. Enter it exactly as shown the Customer Questionnaire.
 - c. Enter the IP address assigned to the entity on the customer network into the IP Range field.
 - d. Enter the Port the entity uses to listen for DICOM connections from the grid.
 - e. For HP MAS, leave Via LDR deselected (unchecked).

NOTE Leaving “Via LDR” unchecked is required for the HP MAS to route data traffic from the grid to the DICOM device via the CLB service.

- f. Enter **HPMA_DICOM** for the GRID AE setting.
- g. Select the access specified for the entity from the Profile Name pull-down menu. For example:
 - **READ_WRITE** – typically defined for PACS and modality AEs, or
 - **READ_ONLY** – typically defined for diagnostic station AEs, or
6. Repeat this process from step 4 to add definitions for all DICOM clients listed in the Customer Questionnaire Document.
7. Click **Apply Changes** to add the DICOM AE definitions to the HP MAS.

The entities now have permission to use the grid, but cannot yet make TCP/IP connections. These definitions are entered first, so that when a connection is made, the grid has the required permission settings to establish a DICOM association for the calling AE.

Enable DICOM AE TCP/IP Connection

Having defined DICOM AE entries in the Grid Management ► Grid Configuration ► DICOM component, you must now enable permission for the entity to make a TCP/IP connection to the HP MAS system. This is handled through the Grid Management ► Grid Configuration ► IP Ranges component.

To enable the DICOM AE TCP/IP connection:

1. Go to **Grid Management ► Grid Configuration ► IP Ranges ► Configuration** tab.

There is a default definition in place for the File System Gateway (FSG) to use the grid.

IP Range Name	IP Range	Group ID	DICOM	HTTP	Actions
192.168.130.61	192.168.130.61	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	[Edit] [Add] [Delete] [Refresh]
192.168.130.54	192.168.130.54	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	[Edit] [Add] [Delete] [Refresh]
192.168.170.41	192.168.170.41	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	[Edit] [Add] [Delete] [Refresh]

Figure 2: Default IP Ranges

2. Click **Add** to create a new row in Allowable IP Ranges.
3. Define a new connection entry for the DICOM entity using the settings defined in the Customer Questionnaire:
 - a. Enter the Description of the entity into the IP Range Name field.
 - b. Enter the IP address assigned to the entity into the IP Range field.
 - c. Enter the Group ID to which the entity belongs.
 - d. Leave the **DICOM** check box selected to enable the DICOM protocol for the entity.
 - e. Deselect (uncheck) the HTTP check box to disable use of HTTP by the DICOM entity.
4. Repeat this process from step 2 to add definitions for all DICOM clients listed in the customer questionnaire.

5. Click **Apply Changes** to add the new IP range definitions to the HP MAS.

This completes the integration of the DICOM clients on the HP MAS side of the connection. Proceed to configure the DICOM client entities to connect with the grid.

6. Click **Logout** to close the NMS interface session. The NMS is not needed for client-side integration.

Change an Existing DICOM Integration

Changes to an existing DICOM integration can be made at any time. You should be familiar with the concepts of connection permissions and profiles before starting any of these activities.

Changing DICOM Entity Access

Should the need arise to alter the permissions or behavior of an entity within the HP MAS, changes can be made using the CMN service. Only the “Vendor” account can access the CMN configuration pages of the NMS interface.

Changes include activities such as:



- Altering transaction permission (store, retrieve, move, find, and storage commit)
- Restricting SOP classes
- Restricting transfer syntax

Transaction permission within a DICOM association for any given AE is governed by profiles defined in the Grid Management ► Grid Configuration ► DICOM Advanced component. These profiles are then applied to the connecting AE through the Grid Management ► Grid Configuration ► DICOM component.

To alter the permissions for a DICOM AE requires you to define a profile of the desired permissions.

NOTE Determining the profile settings needed for any particular behavior is beyond the scope of this procedure. Consult [Appendix A](#) for more information.

To change DICOM entity access:

1. Access the NMS interface using the “Vendor” account (see [“NMS Connection Procedure” on page 91](#)).
2. Go to **Grid Management ▶ Grid Configuration ▶ DICOM Advanced ▶ Overview** tab.
3. View the defined DICOM Profiles to determine if there is a profile already defined for the behavior you want to set. If so, note the Profile Name and skip to step 5.
4. Define a new profile with the desired settings:
 - a. Click the **Configuration** tab.
 - b. If a new Advanced Config Profile is needed to control SOP class or transfer syntax behavior, you must add that profile first. Consult [“DICOM Configuration” on page 54 of Appendix A](#) for details.
 - c. Follow steps **d** through **f** to add the required advanced profile.
 - d. Add a new DICOM Profile by following steps **d** through **f**.
 - e. Select the **Insert**  button to create a new line in the section.
 - f. Enter the required profile settings.
 - g. Click **Apply Changes** to add the profile to the system.
5. Assign the profile to the DICOM AE:
 - a. Go to **Grid Management ▶ Grid Configuration ▶ DICOM ▶ Configuration** tab.
 - b. Locate the DICOM AE title to be modified.
 - c. Click the **Edit**  button in the row for the entity to enable fields for data entry.
 - d. Change the Profile Name to the name of the desired profile.
 - e. Click **Apply Changes** to commit the change.

The entity now takes on the new behavior profile for all associations established from this point onward.


Deleting DICOM Access

Access to the grid from a DICOM AE Title can be disabled temporarily (for troubleshooting or security investigation) or deleted outright.

Disabling Access

In cases where a DICOM AE or IP address is suspected of either a security violation or of causing other problems on the grid, the address can be disabled from establishing DICOM associations. When the issues are resolved, access can be easily re-enabled.

To disable DICOM access for a defined IP address:


1. Access the NMS interface using the “Vendor” account (see “[NMS Connection Procedure](#)” on page 91).
2. Go to **Grid Management** ► **Grid Configuration** ► **IP Ranges** ► **Configuration** tab.
3. Locate the IP address in the IP Range column.
4. Click the **Edit**  button in the row for the entity’s IP address to enable fields for data entry.
5. Deselect the **DICOM** check box for the entity to disable access to DICOM operations on the grid.
6. Click **Apply Changes** to commit the change.

Connections from the IP address can still establish TCP/IP with the grid’s CLB service, however they cannot use the DICOM protocol for transactions.

When the issue is resolved, DICOM access can be re-enabled using the same process; this time enabling the DICOM check box for the IP address.

Deleting Access

To delete a DICOM AE Title integration:

1. Access the NMS interface using the “Vendor” account (see “[NMS Connection Procedure](#)” on page 91).
2. Go to **Grid Management** ► **Grid Configuration** ► **DICOM** ► **Configuration** tab.
3. Locate the AE Title in the list and note the IP Address of the entity.
4. Click the **Delete**  button in the row for the entity.
A confirmation dialog appears, “Are you sure you want to delete this entry?”
5. Click **OK** to mark the entry for deletion and close the dialog. The entry disappears from the list, but is not yet fully deleted.


6. Click **Apply Changes** to commit the deletion.

At this point the DICOM AE can no longer establish DICOM associations with the HP MAS. Depending on how the entity was granted TCP/IP access, there may be another entry to delete.

Look for any other instances of the IP address noted in step 3. If the address is used by other entities, you are finished the deletion process. If no other entities use that address, you may be able to delete the address from TCP/IP connectivity:

7. Go to **Grid Management ► Grid Configuration ► IP Ranges ► Configuration** tab.
8. Look for the IP address noted in step 3. If the address is entered explicitly (that is, it is not just an element within a range of addresses), you can remove the IP Range entry for the entity. If the address does not appear as an explicit entry, then the deletion process is complete.

To delete the TCP/IP access for the DICOM entity:

1. Click the **Delete**  button in the row for the entity's IP address.
A confirmation dialog appears, "Are you sure you want to delete this entry?"
2. Click **OK** to mark the entry for deletion and close the dialog. The entry disappears from the list, but is not yet fully deleted.
3. Click **Apply Changes** to commit the deletion.

At this point, the DICOM AE can no longer make a TCP/IP connection with the HP MAS grid. The deletion process is complete.

Client DICOM AE Integration

Configuration of the DICOM device

Chapter Contents

Process Overview	32
Client Device Settings	33
AE Title (Client)	33
IP Address (Client)	33
Port (Client)	34
Grid Settings	34
AE Title (Grid)	34
IP Address (Grid)	34
Port (Grid)	34
Completion	35

Process Overview

After the HP MAS has been configured to recognize the DICOM AE, configure the DICOM device to communicate with the grid.

Configuration and verification of a DICOM client device requires knowledge of the specific device operation, which is beyond the scope of this guide. This guide provides a list of the settings that must be made at the client device, but cannot provide details of how to enable the settings on the device.

The device must be configured to use specific values and settings that match those in the customer questionnaire. Specifically, settings for the following items must be made on the client device:

	Item	Setting
Client	AE Title	The client AE Title provided by the customer and recorded in the customer questionnaire file. This is the title the device uses to identify itself.
	IP Address	The IP address of the DICOM client device on the customer network.
	Port	The port used by the client device to receive DICOM connections.
HP MAS Grid	AE Title	HPMA_DICOM is the AE title of the HP MAS grid.
	IP Address	The customer network IP address assigned to the Gateway Node GN1-A-1.
	Port	5104 for Read, Find, and Move (the standard READ_ONLY profile). 5105 for Store and Storage Commitment (the standard READ_WRITE profile)

The HP MAS grid imposes a “friends only” policy in granting a TCP/IP connection. The IP address of the device must match that enabled in the Grid Management ► Grid Configuration ► IP Ranges component of the NMS interface (“[Enable DICOM AE TCP/IP Connection](#)” on page 26) to establish a connection.

Additionally, the HP MAS grid only accepts the DICOM association if the device’s IP address and AE title, along with the destination AE title

match an entry in the Grid Management ► Grid Configuration ► DICOM component (“[Define the DICOM Application Entity](#)” on page 23).

The settings made in the previous chapter are taken from the customer questionnaire. These same values must be used at the client device side to enable a TCP/IP connection and DICOM association.

Client Device Settings

These settings describe the client device, and have usually been set at the DICOM client device before HP MAS integration begins. This information should have been provided to Bycast during deployment of your grid or your expansion site. Verify that the settings are entered correctly into the NMS, as outlined in the previous chapter. Verify the settings at the device match those in the customer questionnaire.

In the event there is a discrepancy between existing client settings at the device and those entered in the NMS, corrective action is needed. The first choice is to adjust the settings at the device to match the CMN settings. If the customer cannot accommodate a change to the local device settings, the settings made in the NMS in the previous chapter can be adjusted to match the actual settings of the device.

AE Title (Client)

The DICOM device must identify itself using an AE title. In most deployments, the AE title was already set in the device, and that title was provided to Bycast.

This is the single most common item that causes problems during integration. If the title at the device does not match exactly the value in the NMS, the device should be re-titled (if possible).

AE titles are case sensitive and must match exactly.

IP Address (Client)

The IP address assigned to the client device must match that noted in the NMS.

Port (Client)

Most transfers of data from the grid to the client device are handled using the C-MOVE operation. This instructs the grid to establish a new association—from the grid to the client device—over which the data is transferred. For the grid to make this connection, it must have the port number of the client device.

Ensure the device is listening on the port specified in the NMS. The standard port for DICOM is 5100, however the device may use a different port. If the entity is not used for retrieval, the port may be set to zero. Ensure the setting used for the device matches the information in the customer questionnaire.

Grid Settings

These settings provide a description of the HP MAS system for the DICOM client. These settings are made at the DICOM client device, and enable the device to initiate a connection with the grid by connecting to the CLB on the Gateway Node server.

AE Title (Grid)

The DICOM client requests an association with a specific AE title at the HP MAS system. This title must be set to: HPMA_DICOM.

AE titles are case sensitive. Ensure the entry matches exactly.

IP Address (Grid)

The client device must be provided with the IP address and port to use when calling the HP MAS system.

The address to provide is the Customer Network IP address for the Gateway Node server (**GN1-A-1**) as noted in the Configuration.txt file.

Port (Grid)

The port number to use depends on the action:

- to find and retrieve data from the grid (for example, using the standard READ_ONLY profile): 5104
- to write data to the grid (for example, using the standard READ_WRITE profile): 5105

The grid closes connectivity on port 5105 if all Storage Nodes in the grid become full. This is intended to deny C-STORE activity when the grid has insufficient free capacity for new content.

C-FIND and C-MOVE are always supported on port 5104. You are strongly encouraged to configure the DICOM AE to direct write requests to 5105 and query /retrieve requests to 5104. If this is not possible, the client system should be connected to 5105 and the customer advised to administer the grid to prevent exhausting all storage. Reconfiguration of the client system to port 5104 for read-only operations may otherwise be required.

Completion

When the above items have been set and verified, the device's integration with the HP MAS system can be tested. A sample test plan is provided in the next chapter.

Generally, it is more efficient to integrate and test each device before moving on to integrate another device.

DICOM Integration Verification

Chapter Contents

Process Overview	38
Test Setup	38
Test Case Overview	40
Completion	41
DICOM Interoperability Testing Failure	41
Test Cases	41
1: C-ECHO SCU	41
2: C-STORE SCU	42
3: C-STORE SCU with Storage Commitment	42
4: C-FIND SCU	43
5: C-MOVE SCU and C-STORE SCP	44

Process Overview

To complete the integration, you must verify that the customer's DICOM clients can access the grid, store content, and retrieve content. This verification should be performed by the customer system administrator with your assistance.

NOTE Specific verification steps depend on the device being integrated and are beyond the scope of this guide. This is a sample test plan only.

This chapter provides a high-level test plan that can be used to perform interoperability testing between the grid and a DICOM device. This test plan should be executed for every DICOM device that has been configured to access the HP MAS grid.

[Appendix B: "DICOM Device Test Report"](#) contains a summary test report template that you can use to record the results of this DICOM integration testing.

The HP MAS grid is usually configured with the following DICOM profiles:

- A read-only (READ_ONLY) profile that allows retrieve, find, and move from the grid.
- A read-write (READ_WRITE) profile that includes all READ_ONLY operations as well as store to grid and storage commitment.

Test Setup

The NMS interface is used to monitor the results of transactions with the HP MAS system. The NMS can be accessed using the service laptop or one of the customer's workstations as best suits the location.



WARNING This test procedure could effect grid availability. Test first against a Modality Tester and correct any problems before integrating the DICOM device with HP MAS.

HP MAS Configuration

The DICOM client connects to the Gateway Node. The CLB on the Gateway Node, in turn, directs the connection to an LDR on a Storage Node where the DICOM association is established. The CLB uses internal logic to select the most efficient of all available LDRs to provide data services. The LDR on the Storage Node grid handles the actual data transaction.

To enable monitoring of associations needed to verify the results of integration tests, you need to know which LDR the connection is routed to. To achieve this, the HP MAS system must be configured so that only one Storage Node has the DICOM service online.

For this test, SN1-A-1 is used to monitor DICOM transactions. All other Storage Nodes must have their LDR ► DICOM service taken offline.

NOTE Restricting LDR DICOM services does not impact normal data replication or FSG access to storage services, so it does not affect storage or retrieval of files via NFS or CIFS. However, it may reduce the performance of ingestion of DICOM studies

To disable the DICOM services of all but one LDR:

1. Using the NMS interface, navigate to **SN2-A-1 ► LDR ► DICOM** component, **Configuration** tab.
2. Select **Offline** from the DICOM State pull-down menu.
3. Click **Apply Changes** to commit the state change.

Taking the DICOM component offline triggers the major ⚠ alarm MSTE for the LDR. This can be disregarded during testing.

4. Repeat these steps for all other Storage Nodes in the grid, remembering to leave DICOM online for the Storage Node being used for the test.

DICOM Device Configuration

The DICOM device under test must be configured to communicate directly with the Gateway Node GN1-A-1 as defined in the previous chapter. The device must also be configured to allow connections originating from the HP MAS grid to enable support of retrieving data via the C-MOVE command.

Network Connectivity

Prior to running any tests, you should verify that there is TCP/IP network connectivity between the DICOM device under test and the Gateway Node of the HP MAS system.

The exact method used to achieve this depends on the DICOM device and is beyond the scope of this guide.

Test Case Overview

This chapter lists five test cases. Devices with an access profile that permits reading and writing data (such as the standard READ_WRITE profile) should run all five tests. Those with the an access profile that permits only reading data (like the standard READ_ONLY profile) need run only three tests (as noted in [Table 2](#) below).

For a device with a read-only access profile, ensure that there is content in the HP MAS grid prior to executing these test cases. That is, execute the interoperability test on a DICOM device that uses a read write profile *before* executing on a device that uses a read-only profile.

The table below lists each test in the test plan.

Table 2: Test Case Summary

Test Case	Description	R/W	R/O
1: C-ECHO SCU	Verifies that a DICOM association can be established and that the HP MAS responds to the DICOM client.	✓	✓
2: C-STORE SCU	Verifies the DICOM client can store data to the grid.	✓	✗
3: C-STORE SCU with Storage Commitment	Verifies the DICOM client can store data and receive positive acknowledgement that the data was stored in the grid.	✓	✗
4: C-FIND SCU	Verifies the DICOM client can perform queries on stored content.	✓	✓
5: C-MOVE SCU and C-STORE SCP	Verifies the DICOM client can support the move operation as a Service Class User and store data retrieved from the grid as a Service Class Provider.	✓	✓

Completion

To enable the DICOM services of all LDR services in the HP MAS system:

1. Using the NMS interface, navigate to **SN2-A-1 ► LDR ► DICOM** component, **Configuration** tab.
2. Select **Online** from the DICOM State pull-down menu.
3. Click **Apply Changes** to commit the state change.
This clears the MSTE alarm on the Storage Node.
4. Repeat these steps for all other Storage Nodes in the grid.
5. Ensure there are no MSTE major alarms in the grid. This alarm indicates the DICOM component is still offline.

DICOM Interoperability Testing Failure

If there are DICOM interoperability failures (such as an increase in the count of “Inbound C-Moves - Failed”), contact Support.

Test Cases

This section details each test case that can be used to verify interoperability with the DICOM device. Note that each test case title refers to the SOP class of the DICOM device.

NOTE Appendix B: “DICOM Device Test Report” contains a series of forms that you can use to record the results of these tests.

1: C-ECHO SCU

This test verifies that the DICOM device supports using the DICOM ping-like service provided by the HP MAS grid.

Procedure

1. Using the NMS interface, navigate to **SN1-A-1 ► LDR ► DICOM** component, **Overview** tab.
2. Note the attribute value of “Inbound C-Echoes - Successful”.
3. At the DICOM client, perform a **C-ECHO** operation to the grid.

4. Confirm that the DICOM device received a C-ECHO response.
5. At the NMS interface, confirm that the number of “Inbound C-Echoes - Successful” has increased as expected.

2: C-STORE SCU

This test verifies that the DICOM device supports using the DICOM store service provided by the HP MAS grid.

Preparation

If the DICOM device will be used to generate DICOM studies, select one or more representative studies in preparation for sending.

Procedure

1. Using the NMS interface, navigate to **SN1-A-1 ► LDR ► DICOM** component, **Overview** tab.
2. Note the attribute value of “Inbound C-Stores - Successful”.
3. Send a study to the grid. Initiate a **C-STORE** operation from the DICOM device to the grid.
4. At the NMS interface, confirm that the number of “Inbound C-Stores - Successful” has increased as expected.

3: C-STORE SCU with Storage Commitment

This test verifies that the DICOM device supports using the DICOM store and storage commitment services provided by the HP MAS grid.

Preparation

If the DICOM device will be used to generate DICOM studies, select one or more representative studies in preparation for sending.

Procedure

1. Using the NMS interface, navigate to the **SN1-A-1 ► LDR ► DICOM** component, **Overview** tab.
2. Note the attribute value of the “Inbound Storage Commitment - Successful” attribute.
3. Send a study to the grid. Initiate a **C-STORE** operation from the DICOM device to the grid.

4. Send a **storage commitment request** to the grid.
5. Confirm that the DICOM device successfully received a storage commitment response.
6. At the NMS interface, verify that the number of the “Inbound Storage Commitment - Successful” attribute has increased as expected. This confirms the data was stored by the HP MAS system.

4: C-FIND SCU

This test verifies that the DICOM device supports using the DICOM find service provided by the HP MAS grid.

Preparation

One of the test cases to store content must have successfully placed content that can be searched.

Procedure

1. Using the NMS interface, navigate to the **SN1-A-1 ► LDR ► DICOM** component, **Overview** tab.
2. Note the attribute value of “Inbound C-Finds - Successful”.
3. From the DICOM device, perform an unconstrained query of the studies available on the grid. Note the response from the DICOM device.
4. Perform a query constrained by patient ID. Note the response from the device.
5. Perform a query constrained by modality. Note the response from the device.
6. Perform a query constrained by accession number. Note the response from the device.
7. Perform a query constrained by patient name. Note the response from the device.
8. At the NMS interface, confirm that the number of “Inbound C-Finds - Successful” has increased by five (5) as expected.
9. Perform a query constrained by any other metadata field as required. Note the response from the device.
10. Confirm that the DICOM device received the expected list of studies for each query performed.

5: C-MOVE SCU and C-STORE SCP

This test verifies that the DICOM device supports using the DICOM move service provided by the HP MAS grid. This test also verifies that the device provides a DICOM store service that the HP MAS grid can use.

Procedure

1. Using the NMS interface, navigate to the **SN1-A-1 ► LDR ► DICOM** component, **Overview** tab.
2. Note the attribute value of “Inbound C-Moves - Successful”.
3. Note the attribute value of “Outbound C-Stores - Successful”.
4. Perform a query of the studies available on the grid from the DICOM device.
5. Retrieve a selection of studies, noting the presentation syntax (both the abstract syntax and transfer syntax) of each study retrieved.
6. Confirm that the selected studies were retrieved by the DICOM device.
7. At the NMS interface, confirm that the number of “Inbound C-Moves - Successful” has increased as expected.
8. Confirm that the number of “Outbound C-Stores - Successful” has increased as expected.

Grid Access for Client Applications

Understanding the connection process, and configuring access profiles

Chapter Contents

Overview	46
Profiles	47
IP Ranges	47
Group ID	48
Protocol Permissions	48
Configuring an IP Range	49
HTTP Configuration	50
Overview of HTTP Configuration Process	50
HTTP Advanced	51
HTTP Entities	54
DICOM Configuration	54
Validating DICOM Associations	54
DICOM Profiles	56
Advanced Config Profiles	58
DICOM Partitions	62
DICOM Examples	64
Overview of DICOM Configuration Process	64
Configuring Access Using a Simple DICOM Profile	65
Configuring Access Using a Complex DICOM Profile	70
Configuring Access Using a Coerce Tag Profile	77

Overview

Access to the grid for external applications is configured in the NMS via the Grid Management ► Grid configuration menu, using the IP Ranges, HTTP, HTTP Advanced, DICOM, and DICOM Advanced components.

The grid applies security checks and enforces access permissions to prevent remote entities from making unauthorized access. To understand these attributes and configuration options, you need to understand the layers of connectivity and a little about the protocols used to communicate with the grid.

This appendix contains this background information, as well as example procedures for configuring profiles.



WARNING **Altering connection configuration is considered a highly advanced capability and should not be undertaken casually. Contact Support for assistance with configuration.**

At the top level, connections to the grid are made using TCP/IP. Before a TCP/IP connection is opened, the grid checks to see if the remote entity is on its list of “friendly” IP addresses. If the connection request does not originate from a listed IP address, the connection request is ignored; the caller is not aware that there was any device at the called address.

DICOM is optional.

Assuming a TCP/IP connection is permitted, the grid further restricts the caller to the enabled protocols: HTTP or DICOM. There are configurations for each protocol that grant or decline permission for a remote entity to carry out specific operations. These permissions are defined in “profiles” that can be allocated to individual or groups of calling entities, based on the caller’s IP address.

Some DICOM modalities are limited in their ability to handle particular actions or data transfer formats (syntax). Configurations can be set to restrict activities of these entities to a subset of operations or transfer formats. Setting these types of restrictions requires you to be familiar with the DICOM standard.

Profiles

In general, a profile is a named definition of capabilities or behaviors that can be assigned to one or more remote entity groups. By defining a profile with a given set of permissions, that set of permissions can then be granted to a group of entities by referencing the profile name. The same profile can be assigned to any number of entity groups.

A profile definition may take more than one line in a table. All lines using the same (case sensitive) profile name are part of the profile. The sequence in the table is significant; the table is processed from the top downward. Therefore it is possible to specify specific exceptions to a general rule by listing the exceptions closer to the top of the table, and then specifying the general rule that applies to all remaining entities.

IP Ranges

To open a TCP/IP connection to a grid service, the caller's IP address must be on the list of addresses configured in Grid Management ► Grid Configuration ► IP Ranges. If the caller is not on the list, the request is ignored.

Provided a connection is permitted, the grid can improve performance by knowing which grid server group the remote entity is associated with. This helps the grid route data more efficiently by using services that operate at a lower "cost". To achieve this, the configuration includes a group identifier for each external entity.

Configuration: Grid Configuration - IP Ranges
Updated: 2008-04-25 10:31:52 PDT

Allowable IP Ranges (1 - 4 of 4)

IP Range Name	IP Range	Group ID	DICOM	HTTP	Actions
HP Medical Archive	14.0.0.0/8	50	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
PACS_Client	192.168.130.10	50	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Show 10 Records Per Page Refresh Previous « 1 » Next

Figure 3: Sample IP Range Configuration

Additionally, the configuration table can be used to grant or withhold permission to use particular protocols. At least one check box must be selected to be able to carry out any operations on the grid. If neither box is checked, the caller can make a TCP/IP connection and get a response but cannot access grid content.

IP Ranges are specified using one of the following:

- a single IP address
- a hyphenated list of IP addresses (e.g. 174.182.91.00-174.182.91.64)
- a range of IP addresses specified using CIDR notation (e.g. 192.168.120.0/27)
- an IP address in the form A.B.C.D, where at least one of A, B, C, or D is zero.

If D is 0, then IPs between A.B.C.0 and A.B.C.255 will be in range. If C and D are both 0, then IPs between A.B.0.0 and A.B.255.255 will be in range. If B, C, and D are all 0, then IPs between A.0.0.0 and A.255.255.255 will be in range. If A, B, C, and D are all 0, then all IPs will be in range.

Multiple IP Range Matches

It is possible that a caller's IP address may match more than one of the ranges specified in the IP Range table. When the grid is validating the caller, it searches the table from the top downward. The first match found is used to assign the protocol permissions to the caller.

Group ID

At the time the grid deployment is configured, the services are allocated to logical groups; typically these are numbered: 1, 2, 3, and so on. The main Overview page for each service includes the Group ID attribute, the group to which the service belongs.

An analysis of the network connectivity between these groups is used to derive a "cost" factor (a number from 0 – 100) used by the grid to optimize traffic flow. Entities (IP addresses) within the same group are assumed to have a zero cost. Communication between groups has a cost assigned when the configuration plan is created for your enterprise.

Each remote entity listed in the IP Ranges table is allocated to one of these groups. You cannot create new groups using this configuration table. If no group is assigned, or the group ID specified is not known to the grid, the connection cost to that location is assumed to be zero.

Protocol Permissions

DICOM is optional.

The check boxes in the IP Range table enable the protocols that a remote entity is permitted to use when contacting the grid. You add



some additional protection to the grid by selecting only the protocol supported by the remote entities.

If no protocols are selected, the remote entity can only establish a TCP/IP connection with the grid. With only a TCP/IP connection, the remote entity is aware that there is some form of network node at the called address, but it cannot access grid content. You could deselect both the HTTP and DICOM protocols for an IP range to temporarily disconnect remote entities because of security concerns, for example, then easily restore connectivity later when the issues are resolved.

Configuring an IP Range

This procedure enables access to the grid from devices using specified IP addresses.

Once permission is granted for a particular IP address (or range of IP addresses), connections can be made from any device in that range that uses the specified protocol.

1. Go to **Grid Management ► Grid Configuration ► IP Ranges ► Configuration ► Main**.
2. Define a set of IP ranges permitted to access the grid:
 - a. In the **Allowable IP Ranges** table, click **Edit**  (if this is the first entry) or **Add**  to add a new IP range.
 - b. Enter a name for the range. The IP range name can be anything meaningful; it is not referenced elsewhere in the configuration.
 - c. Enter the IP address or range of IP addresses permitted to access the grid.

If specifying a range, use one of:

- a hyphenated list of IP addresses (e.g. 174.182.91.00-174.182.91.64)
- a range of IP addresses specified using CIDR notation (e.g. 192.168.120.0/27)
- an IP address in the form A.B.C.D, where at least one of A, B, C, or D is zero.

If D is 0, then IPs between A.B.C.0 and A.B.C.255 will be in range. If C and D are both 0, then IPs between A.B.0.0 and A.B.255.255 will be in range. If B, C, and D are all 0, then IPs between A.0.0.0 and A.255.255.255 will be in range. If A, B, C, and D are all 0, then all IPs will be in range.

- d. Enter a group ID for the remote entity.
Associate the remote entity with an existing group ID of servers within the grid to ensure that the grid operates efficiently. Select the group ID of the servers that are geographically or logically “close” to the remote entity. (For example, you may want to add the remote entity to the server group of the Gateway Node that it saves data to.) Consult the Customer Questionnaire Document for your grid if you are not sure which group ID to use. Note that if you do not set a group ID or the group ID is not known to the grid, the entity effectively belongs to all grid groups.
- e. Select the protocol or protocols (HTTP or DICOM or both) that can be used by devices that connect from within this IP range.
- f. Click **Apply Changes**.
Any device using the specified protocol, within the specified IP address range can now access the grid.
- g. Repeat for each IP range permitted to access the grid.

HTTP Configuration

NOTE Performing HTTP Configuration is not required in order to integrate DICOM devices with HP MAS.

The HP MAS uses one HTTP definition to enable internal HTTP connections (on the 14.0.0.0 private network). No other HTTP connections are needed.

To permit remote entities to access the grid using HTTP, you must create a profile that assigns permissions to perform activities on the grid, and assign this profile to the entity. Without this, the entity cannot access grid content.

Overview of HTTP Configuration Process

To permit a remote entity to access the grid via HTTP:

1. Use the Grid Management ► Grid Configuration ► HTTP Advanced component to define a profile that outlines the activities that the entity is permitted to perform.

2. Use the HTTP component to assign an IP range to the activities' permission profile.
3. Grant the IP range permission to access the grid, via the IP Ranges component.

More information about each of these steps is described below.

HTTP Advanced

HTTP access to grid content takes place in one of four “namespaces”. A namespace is a logical division within which all file names are unique. In brief, specific activities over HTTP are dependent on the namespace in which content is exchanged:

- /CBID supports content retrieval. Content can only be deleted from this namespace by the business rules of the grid.
- /UUID permits ingestion, retrieval, and deletion of content. Deletion in this namespace removes a handle to the content so that it can no longer be accessed. The grid business rules determine what happens to content that no longer has a UUID pointer to it.
- /DICOM supports ingestion of new DICOM content. This is only used if the DICOM option is installed.
- /GRID supports queries about grid nodes or services by a custom-developed client application. It is also used to enable the saving of audit messages by a custom-developed client application.

Each namespace can have any number of defined profiles, each with a unique user-defined (and case sensitive) name. To grant an entity permissions in more than one namespace, the same profile name is repeated in each namespace as needed. The check boxes enable specific activities. For more information about the namespaces and the options listed, see the *HTTP API Reference Guide*.

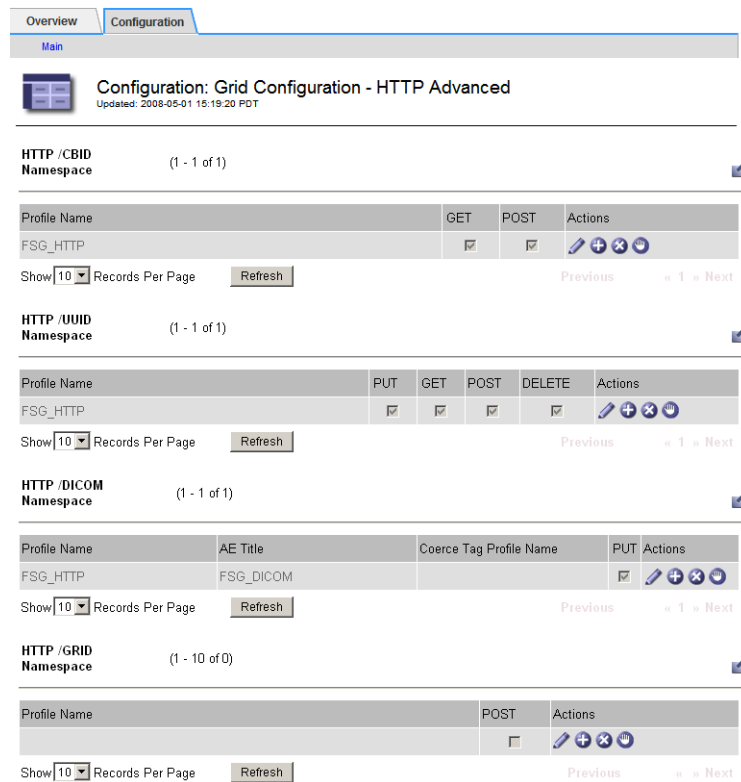


Figure 4: Sample HTTP Advanced Profiles Configuration

/CBID Namespace

The Content Block ID (CBID) namespace is owned by the grid and is used *within* the HP MAS system software. The content referenced by a CBID may be deleted by the grid (according to grid business rules) at any time.

External use of the CBID namespace is deprecated in favor of the use of the /UUID namespace.

/UUID Namespace

The Universal Unique ID (UUID) namespace is the preferred namespace used to store, access, and delete (hide) data using a unique identifier. This UUID provides an abstracted primary key (handle) for stored content that can be assigned by a third-party application, as long as the standard for generating unique identifiers is followed.

The Delete option can be overridden by configuring Grid Management ► Grid Configuration ► Configuration tab.

/DICOM Namespace

The Digital Imaging and Communications in Medicine (DICOM) namespace is used to store data in grids where the DICOM option has been purchased and configured.

/DICOM AE Title

DICOM objects must be saved to the grid with the AE title of the sending device. However, when using the HTTP interface, you do not establish a DICOM association between the grid and the device sending the object. Therefore the sender cannot provide an AE title when it submits an object. Instead, you must specify the AE title of the sending device in the Grid Management ► Grid Configuration ► HTTP Advanced ► HTTP /DICOM Namespace table. This field is used to assign an AE title to all content submitted by an entity assigned this profile.

/DICOM Coerce Tag Profile Name

This is a reference to another configuration profile that is used for DICOM transactions. When an entity assigned this HTTP profile submits a DICOM file, the behavior associated with the Coerce Tag Profile named here is also applied. See [“DICOM Partitions” on page 62](#) for more information on this feature. This field can be left blank if no partitioning is applied to entities with the profile.

/GRID Namespace

The GRID namespace is used to query the grid for information about nodes and the services they provide. The GRID namespace is used by custom applications developed to store or retrieve grid content via the UUID or DICOM namespaces. In this release, enabling POST in the grid namespace also enables a custom application to store custom audit messages supplied by the application. For more information, see the *HTTP API Reference*.

HTTP Metadata Indexing

This table lists the custom metadata defined for use with this grid via the HTTP API. For more information, consult the *HTTP API Reference Guide*.

HTTP Entities

Returning to the Grid Management ► Grid Configuration ► HTTP component, entities are now enabled to use HTTP by applying profiles to them. The IP Ranges specified here can be subsets of the addresses from the IP Ranges component. This enables a workgroup to be broken down into particular activity profiles on the grid.

Description	IP Range	Profile Name	Actions
14.1.1.19 FSG	14.1.1.19	FSG_HTTP	[Edit] [Add] [Delete] [Refresh]
14.1.1.17 FSG	14.1.1.17	FSG_HTTP	[Edit] [Add] [Delete] [Refresh]
14.2.1.19 FSG	14.2.1.19	FSG_HTTP	[Edit] [Add] [Delete] [Refresh]

Show 3 Records Per Page Refresh Previous 1 2 3 4 5 Next

Figure 5: Sample HTTP Entities Configuration

Any entities intending to use HTTP that do not have an assigned profile cannot access grid content. Ensure that all IP addresses of entities intended to use HTTP appear somewhere on this list.

You cannot assign a profile here before creating it in the HTTP Advanced component.

DICOM Configuration

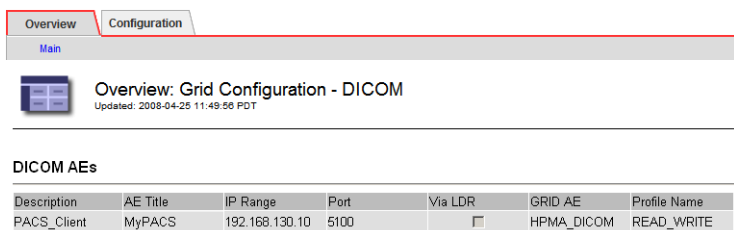
Validating DICOM Associations

DICOM transactions are carried out when a DICOM association has been established between two Application Entities (AEs). Each modality (device) has its own AE title which must be known in advance to configure the connection permission. The HP MAS software also has its own AE title (HPMA_DICOM); in fact, it could have several depending upon your installation.

The process of establishing a DICOM association includes validating that the calling entity has permission to use DICOM on the grid, and validating that the entity has permission to perform the requested activities. To configure the grid to give an entity these permissions,

settings must be made in both the Grid Management ► Grid Configuration ► DICOM and Grid Management ► Grid Configuration ► DICOM Advanced components.

Validation is a multi-layered handshake process. The first layer is to validate that the caller is permitted to associate with the grid. This requires that the caller (which has already established a TCP/IP connection via the IP range validation) is on the list of DICOM AEs in the Grid Management ► Grid Configuration ► DICOM component.



The screenshot shows a web application interface with a navigation bar containing 'Overview' and 'Configuration' tabs. Below the navigation bar is a 'Main' section. The main content area displays the title 'Overview: Grid Configuration - DICOM' and a timestamp 'Updated: 2008-04-25 11:49:56 PDT'. Below this is a section titled 'DICOM AEs' which contains a table with the following data:

Description	AE Title	IP Range	Port	Via LDR	GRID AE	Profile Name
PACS_Client	MyPACS	192.168.130.10	5100	<input type="checkbox"/>	HPMA_DICOM	READ_WRITE

Figure 6: Sample DICOM AE Entry

The caller must match both the caller AE Title and the IP address, and must also be attempting to associate with the matching GRID AE title. If there is a mismatch on any of these, the next entry in the DICOM AEs table is tested. If no entry matches, the association fails.

Assuming the calling AE is validated, the list of requested activities is then individually validated against the permitted activities as specified by a DICOM profile. That profile itself may contain references to additional profiles for controlling behavior and selecting transfer syntax. All of this is part of the handshake that establishes the parameters of an association.

DICOM Profiles

Profile Name	S	R	F	M	C	Coerce Tag Profile Name	Advanced Config Profile Name	Behavioral Profile Name
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			

Coerce Tag Profiles

Coerce Tag Profile Name	Tag	Tag Value	Query	Ingest	Description
			<input type="checkbox"/>	<input type="checkbox"/>	

Advanced Config Profiles

Advanced Configuration Profile Name	Behavior	SOP Class	Preferred Transfer Syntax	Required Transfer Syntax

Figure 7: Default DICOM Advanced Settings

GRID AE Titles

The GRID AE entry is a user-defined AE title for the grid to which the remote entity can associate. Remember that an association profile is assigned based on the unique combination of:

- Remote AE title
- Remote IP address
- Grid AE title
- Port number (used only for outbound associations from the grid)

By using different GRID AE titles, a single remote entity can connect to the grid using different profiles. The profile used for a connection is selected by selecting the Grid AE title the entity associates with.

This can be viewed as a form of data partitioning. For example: when an entity associates with the grid using GRID AE “A” using profile “Owner”, it may have all DICOM permissions; when it associates with GRID AE “B” using profile “Guest”, it may only have permission to query and get content. (This is more clearly understood when profiles include a Coerce Tag Profile as discussed in [“DICOM Partitions”](#) on page 62.)

DICOM Profiles

The DICOM profile definitions are used to grant permission to a remote Application Entity (AE) to perform various actions on the grid.

An association request includes a list of the activities intended to be performed during the association. The association handshake process allows the grid to accept or reject each activity individually.

Table 3: Permission options for DICOM Profiles

DICOM Option	Description
S	Send to GRID – indicates an entity with this profile can store DICOM files to the grid.
R	Receive from GRID – indicates an entity with this profile can retrieve DICOM files from the grid. (Note that retrievals are made using a C-MOVE request.)
F	Find on GRID – indicates an entity with this profile can issue query commands for DICOM content.
M	Move – indicates an entity with this profile can issue a DICOM command for the grid to open another association to relay an object to the device.
C	Storage Commit – indicates an entity with this profile can query for acknowledgement that an object was stored.

There are additional settings for:

- Coerce tag profile reference
- Advanced configuration profile reference
- Behavioral Profile name

Coerce Tag Profile Name

This profile is not related to the DICOM association handshake, but is used to manage logical partitions of DICOM data on the grid. See “DICOM Partitions” on page 62 for information.

Advanced Config Profile Name

To manage some DICOM entities that have unique behavior for particular actions or a limited ability to handle specific transfer syntax (data formats), an advanced configuration profile can be used to complete the association handshake.

This profile is optional. It is used for entities that have known compatibility issues, including the use of Private SOP storage classes that are not otherwise supported by HP MAS (as described in the *HP MAS DICOM Conformance Statement*).

Behavioral Profile Name

Some DICOM clients expect specific DICOM behavior that is different than the default behavior implemented by HP MAS software. In these cases, when configuring access for these clients you can select a pre-configured DICOM Behavioral Profile that customizes the grid's default behavior to match that expected by the client. Current values are:

- Xcelera A (for Xcelera Release 1.2 L4 SP1)
- syngo Dynamics A (for syngo Dynamics version 5.0)

Advanced Config Profiles

Handshaking a DICOM association is also governed by an optional Advanced Config Profile configuration. If this profile is assigned to an Application Entity, the requested activities and transfer syntax options are also reviewed against the following parameters defined in the Advanced DICOM Configuration profile.

Behavior

The Behavior (either "Allow" or "Disallow") is applied to the SOP class named in the profile. If the entity requests an activity using the named SOP Class, and that class is disallowed, then that activity is declined. This does not fail the association, only the particular intended activity within the association. By default all activities permitted by the primary DICOM profile are permitted.

This feature can be used to selectively allow or disallow actions with an AE assigned to the profile. By entering multiple lines with the same (case sensitive) profile name, a list of permitted or excluded activities can be built.

If you wish to disallow a minority of actions, enter one line per SOP Class to prohibit and set the Behavior to "Disallow".

Should the allowable set be in the minority, enter one line per SOP Class to enable and set the Behavior to "**Allow**". Then enter a line with the Behavior set to "**Disallow**" and the SOP Class set to an asterisk "*", the wildcard for all classes. The system searches the profiles from the top of the list downward. By ending the list with an entry to disallow all, only those allowed classes higher in the list are enabled.

SOP Class

The Advanced configuration profile is applied only to the SOP class named in the Profile.

If the SOP class entered here is a supported SOP class (as listed in the *HP MAS DICOM Conformance Statement*), then the Advanced Configuration Profile is used to restrict the activities permitted by the AE using this class, or to customize the Transfer Syntax used.

If the SOP class is a private or unsupported SOP class (which does not have a prefix of “1.2.840.10008”, or is not listed as a supported class in the *HP MAS DICOM Conformance Statement*), the Advanced DICOM Configuration Profile permits the grid to accept associations that use this class and to perform all activities permitted by the profile. The profile can also optionally be used to customize the Transfer Syntax used for the SOP class.

Note that configuring an Advanced Configuration profile for a private or unsupported SOP class does not guarantee that all activities using that SOP class will succeed on the grid. For example, a particular private SOP class may use an encoding that the grid is unable to parse.

Preferred and/or Required Transfer Syntax

For each requested data transaction, the caller lists the transfer syntax options it is capable of supporting for that activity. Some particular device entities do not handle some formats very well. The Advanced Config Profile can impose rules on selecting the syntax for a transaction during the association handshake process.

NOTE The “required” format is a check that the entity has *included* the format within its options, *not* a requirement to use that transfer syntax for a given action.

The “preferred” format is used when it is included in the caller’s list of supported options. You may specify more than one “preferred” format by including a comma-separated list of preferred transfer syntaxes. If no preferred option is specified, the grid selects either the required format, the first format in the caller’s list, or the grid’s preferred option of “Little Endian Implicit” (LEI) format.

The application of rules is fairly complex and varies based on which of the two fields have entries and which are blank. The selection of a

transfer syntax (or the outright rejection of the activity) is determined according to the flowchart in [Figure 8](#).

The questions “Is Required Specified?” and “Is Preferred Specified?” are testing if the fields in the configuration profile have entries. If a field is left blank, the decision evaluates “No”.

The questions “Is Required in Options?” and “Is Preferred in Options?” are testing if the caller’s list of transfer syntaxes includes the one specified in the configuration profile. There is one case where the test for a required syntax is done across all actions in the association request, not just the specific action being validated.

Note that the Big Endian Explicit transfer syntax is not supported by the HP MAS software. If Big Endian Explicit is the only specified transfer syntax for an entity, or if it is the first specified transfer syntax (in the case that the decision tree shown in [Figure 8](#) evaluates such that First Format Listed is used for the association request) the association request fails.

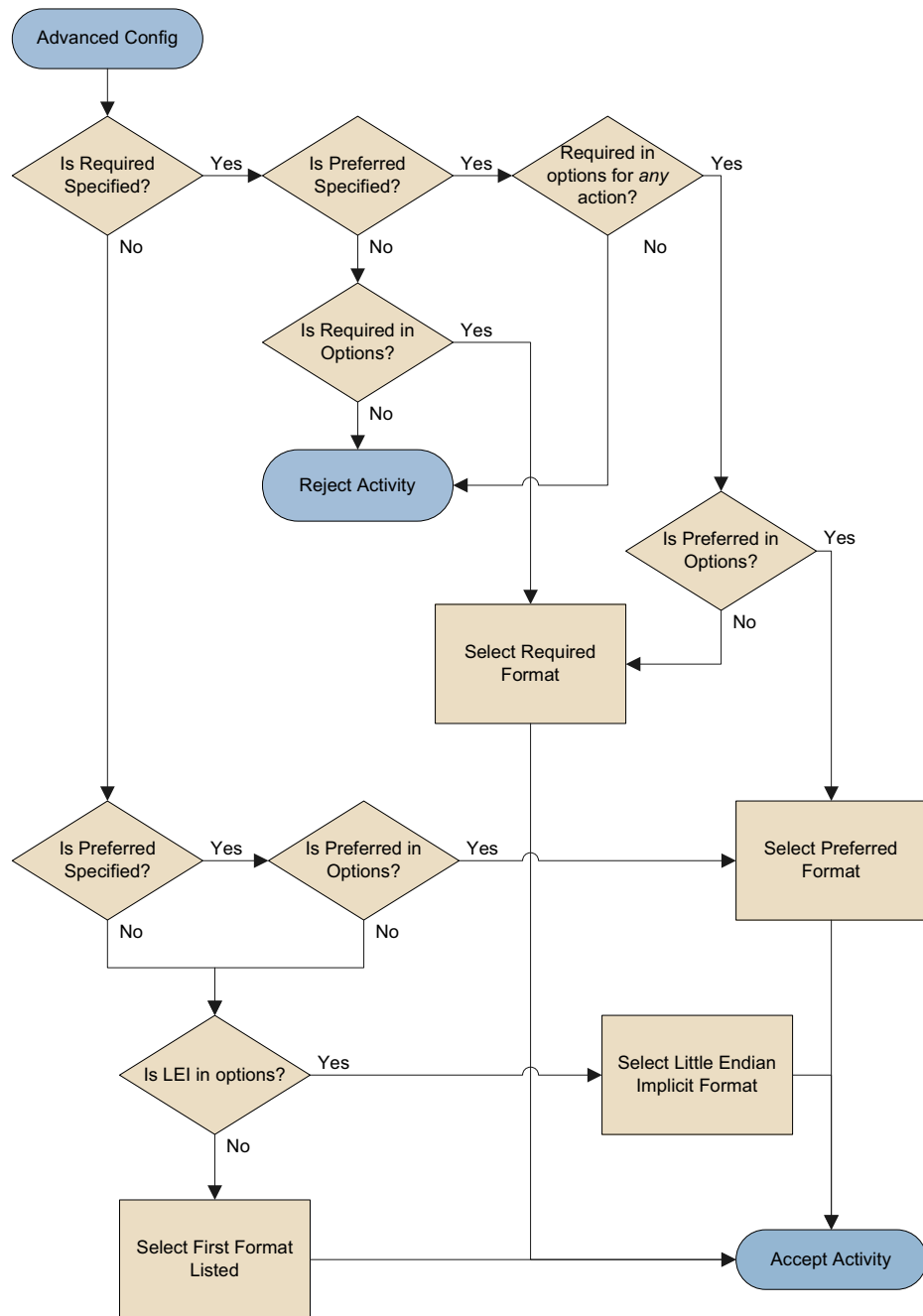


Figure 8: Advanced Configuration Flowchart

Combining SOP Class and Transfer Syntax

Because both SOP class and transfer syntax settings are included on each line of the profile table, you must make an entry for the SOP Class, even if you intend to allow all activities and only restrict file formats (transfer syntaxes). To set a profile for file formats only, ensure

the Behavior is set to “**Allow**” and the SOP Class field is set to an asterisk “*” to indicate that all supported SOP classes are permitted.

Note that setting the SOP class to an asterisk “*” applies settings only to the list of supported SOP classes found in the grid’s *DICOM Conformance Statement*. Advanced Configuration profiles that use “*” are not applied to private or unsupported SOP classes, even if profiles exist that permit associations using these classes.

Entries that allow a specific SOP class can optionally apply a transfer syntax rule. If a rule is included, the rule applies only to the named SOP class. To apply a rule to all allowed SOP classes, the transfer syntax rule must be entered on every line that contains an “Allow” behavior for that profile.

DICOM Partitions

The HP MAS software supports a feature that enables an enterprise to logically partition DICOM data. This can be used to restrict a remote entity so that it can access only a portion of the whole grid.

When a DICOM object arrives, it is stored in the grid and elements of its metadata are sent to the Content Management System (CMS) service. The CMS keeps a database of this metadata to facilitate queries. In addition to the file metadata, it is possible to add a DICOM private tag to assign the content to a logical partition; (0009,0080) has been selected by the HP MAS system for this purpose. That private tag is stored in the CMS database only, not with the actual DICOM file in the grid.

When an entity that has restricted access issues a query or data request, the private tag is automatically added to the criteria, thus limiting the responses to only those data objects within the logical partition.

You can restrict the access that an entity has to objects using the Coerce Tag Profiles table in the Grid Management ► Grid Configuration ► DICOM Advanced component.

Note that any DICOM profile that does not specify a Coerce Tag Profile has unrestricted access to all data saved to the grid, regardless of any coerce tags assigned to that data.

Coerce Tag Profiles

Defining a coerce tag requires knowledge of the DICOM standard. DICOM metadata consists of “tag:value” pairs. The coerce tag used to partition data *must* be the DICOM private tag (0009,0080). The value of the tag is any suitable name for the logical partition.

Coerce tags are stored with the grid metadata, not with the content object. The content object is never altered by the grid.

All profiles begin with a user-defined name for the profile. This is the reference name entered in entity configurations to assign the profile to entities accessing the grid. It is case-sensitive.

You can use multiple lines with the same profile name to assign more than one DICOM private tag to a profile. **Only** the (0009,0080) tag is supported to create partitions, although other private tags can be used to coerce settings if required.

Within a profile, the Coerce Tag must be unique. That is, you can only specify a single permitted value for each DICOM private tag. Therefore each profile can only be associated with a single logical partition. If a Coerce Tag is repeated within a profile, the first occurrence (from the top of the table downward) specifies the value. Any subsequent repeats of the Coerce Tag in a profile are ignored.

The Query check box is used to restrict the visibility of objects available to entities. When an entity with this profile issues a query, the CMS automatically adds the coerce tag to the query criteria. Therefore, the returned objects are restricted to those that have the tag value listed in the profile (that is, those that are a part of the logical partition created by the coerce tag).

The Ingest check box is used to enable the addition of the coerce tag to objects submitted from an entity assigned this profile. When the entity submits a DICOM object, the CMS adds the tag to its metadata database for that object. This is how data is allocated to partitions. If the profile has more than one line, multiple tags can be added.

NOTE To use coerce tags to enforce partitioning, the DICOM private tag "(0009,0080)" must be added to the DICOM Indexed Tags (ITAG) bundle. Contact Support for assistance.

DICOM Examples

This section provides step-by-step instructions for configuring access to the grid for a DICOM Entity.

The procedures described here use “backward configuration” — they start by defining the most specific part of the profile and end by defining the most general. Performing the configuration in this way avoids problems with dependencies, and ensures that clients cannot access the grid using the new profile until configuration is complete.

Overview of DICOM Configuration Process

The following configuration steps are needed to permit a remote entity to access the grid via DICOM:

1. Use the **Grid Management ► Grid Configuration ► DICOM Advanced** component to define a profile that outlines the activities that the remote entity is permitted to perform.
 - a. Optionally define an Advanced Config Profile to specify the details of allowed SOP classes and their preferred and required transfer syntaxes.
 - b. Optionally define a Coerce Tag Profile to partition data in the grid.
 - c. Define a DICOM Profile for the remote entity.

The DICOM Profile outlines the permitted activities that the remote entity may perform on the grid, and specifies which (if any) Advanced Config Profile, Coerce Tag Profile, and DICOM Behavioral Profile are to be used for associations with the remote entity.

2. Use the **Grid Management ► Grid Configuration ► DICOM** component to specify which entities can access the grid, and assign the DICOM Profile and Grid AE title they use when doing so.
3. Use the **Grid Management ► Grid Configuration ► IP Ranges** component to grant the IP addresses associated with the remote entity permission to access the grid.

Each of these steps is described in more detail in the DICOM examples below.

Configuring Access Using a Simple DICOM Profile



This section describes how to enable access to the grid for a DICOM device that does not require coerce tags or specialized access restrictions. This is the most common type of configuration.

DICOM Configuration Profile

The first step is to identify (or create) the DICOM Configuration Profile to be used by the DICOM device. The DICOM Configuration Profile defines the activities that a device that uses the profile is permitted to perform on the grid.

1. From the NMS, select **Grid Management ► Grid Configuration ► DICOM Advanced ► Overview**

A description of the activities that can be included in a device's profile are listed in [Table 3 on page 57](#).

2. If an existing profile meets your needs, note its name, and go on to ["DICOM AE Titles" on page 74](#).
3. Otherwise, create a custom DICOM profile:
 - a. Select **Grid Management ► Grid Configuration ► DICOM Advanced ► Configuration ► Main**
 - b. Click **Edit**  (if this is the first entry) or **Add**  to add a new DICOM Configuration Profile.
 - c. Type a meaningful Profile Name. This name is referenced later in the configuration process, so note that the name is case-sensitive. For example, type: **WRITE_ONLY**
 - d. Select the DICOM options needed for the entity. For a write only profile, select: **S** (Send to Grid) and **C** (Commit Storage)
 - e. Leave the entries for Coerce Tag Profile Name and Advanced Config Profile Name blank.

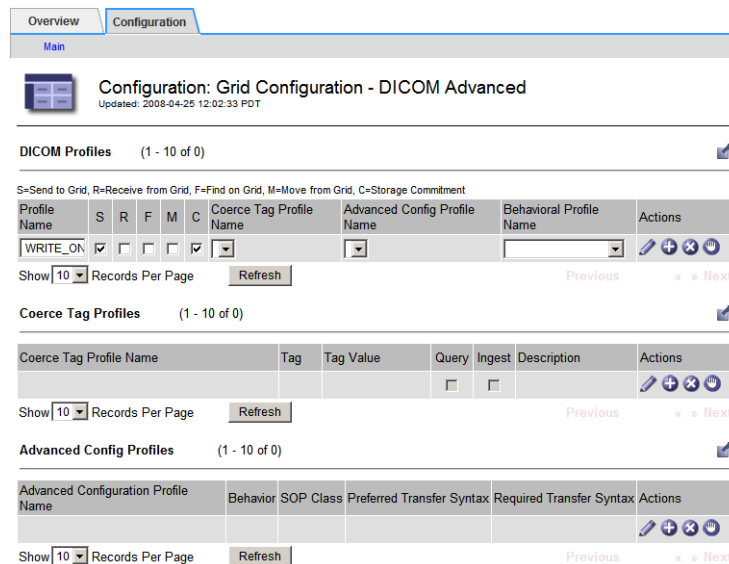




Figure 9: DICOM Configuration

- f. If the client that will use this profile is one that requires a change to the grid’s default DICOM behavior, select the appropriate Behavioral Profile Name from the drop down list. For more information, see “Behavioral Profile Name” on page 58.
- g. Click **Apply Changes**.

Next enter the DICOM AE Titles for devices that are to be given grid access using one of the defined DICOM Profiles.

DICOM AE Titles

After you have created the DICOM Configuration Profile using Grid Management ► Grid Configuration ► DICOM Advanced, define the DICOM AE Titles of the remote entities that are permitted to access the grid.

1. From the NMS, select **Grid Management ► Grid Configuration ► DICOM ► Configuration ► Main**
2. Click **Edit**  (if this is the first entry) or **Add**  to add a new DICOM AE.

Configuration: Grid Configuration - DICOM
Updated: 2008-04-25 12:51:41 PDT

DICOM AEs (1 - 10 of 0)

Description	AE Title	IP Range	Port	Via LDR	GRID AE	Profile Name	Actions
Bycasr StorageGRID		192.168.0.0/16	0	<input type="checkbox"/>			

Show 10 Records Per Page Refresh Previous Next

Figure 10: Grid Management ► Grid Configuration ► DICOM

3. Enter a Description of the DICOM device you are granting access to. This description can be anything meaningful; it is not used as a reference elsewhere in the configuration process. In this example, type: **MRI Clinic**
4. Enter the AE Title assigned to the remote DICOM entity. AE Titles are case-sensitive. In this example, type: **DICOM_MRI**
5. Enter the IP Range (or IP address) that the device can connect from. If specifying a range, use one of:
 - a hyphenated list of IP addresses (e.g. 174.182.91.00-174.182.91.64)
 - a range of IP addresses specified using CIDR notation (e.g. 192.168.120.0/27)
 - an IP address in the form A.B.C.D, where at least one of A, B, C, or D is zero. If D is 0, then IPs between A.B.C.0 and A.B.C.255 will be in range. If C and D are both 0, then IPs between A.B.0.0 and A.B.255.255 will be in range. If B, C, and D are all 0, then IPs between A.0.0.0 and A.255.255.255 will be in range. If A, B, C, and D are all 0, then all IPs will be in range.

In this example, enter: **192.168.120.54**

6. Enter the Port that the DICOM device uses to listen for connections from the grid. (This is the port number used for DICOM C-MOVE operations that send data from the grid to the device.) In this example, enter: **5000**
7. Do not select Via LDR

DICOM associations are generally initiated via a CLB. The CLB identifies a preferred LDR for the transaction, and passes the association from the remote entity on to that LDR. Selecting Via LDR directs the LDR to communicate directly with the remote entity once an association has been made. However, in an HP MAS grid that uses a private network the LDR is accessible only over the

internal private network, and cannot communicate directly with the remote entity.

8. Next, enter the GRID AE title.

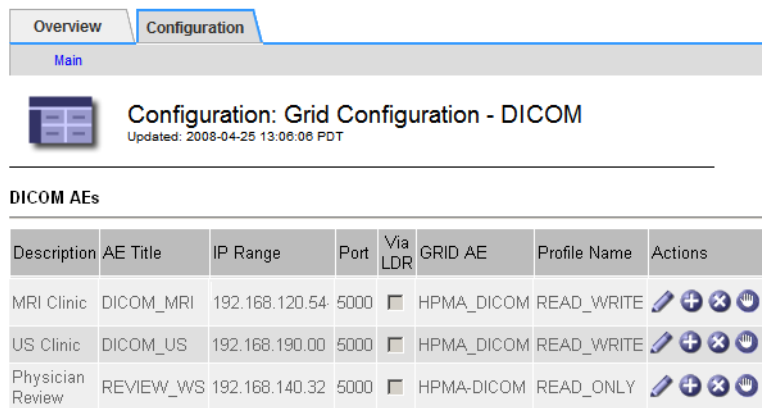


Figure 11: Grid Management ► Grid Configuration ► DICOM

The AE Title of the grid is an arbitrary, case-sensitive string of 16 characters or fewer. The grid may use more than one AE title, where each title is associated with a different DICOM configuration profile. In this example, enter: **HPMA-DICOM**

9. Select the Profile Name of the DICOM Configuration Profile that you defined or chose earlier (as described in “DICOM Configuration Profile” on page 65). In this example, select: **READ_WRITE**
10. Repeat from step 2 for each remote DICOM entity that needs to access the grid.

Note that the table is evaluated from the top down. If a table contains more than one match for a device AE title and IP address, the grid maps them to the first GRID AE and DICOM Profile that it finds in the table. Therefore, to specify exceptions to any general rule, first match specific IP addresses to the GRID AE Title and Profile that specify the exceptional case. Then match a broader range of IP addresses to the GRID AE title and Profile that express the more general rule for associations from that range.

11. If necessary, move a selected DICOM AE up or down in the list using the up and down arrows.
12. Click **Apply Changes**.

Next, enable grid access from the IP addresses of these DICOM devices.



Allowable IP Ranges

After you have configured the DICOM profile for the remote entity (“DICOM Configuration Profile” on page 73), and have associated this profile with a DICOM AE Title (“DICOM AE Titles” on page 74), enable the remote entity to access the grid by adding its IP address range to the allowed list.

Note that:

- If an IP range specified here (using the Grid Management ► Grid Configuration ► IP Ranges page) is more restrictive than the IP range specified when configuring the DICOM AE Title, only DICOM entities in the range specified here are permitted to access the grid.
- The IP Range table is evaluated from the top down. An IP address is granted the permissions associated with the first matching entry in the table. (Therefore, you should specify any exceptions to a general rule at the top of the table).

To grant grid access to a range of IP addresses:

1. From the NMS, select **Grid Management ► Grid Configuration ► IP Ranges ► Configuration ► Main**
2. Define a set of IP ranges permitted to access the grid:
 - a. In the **Allowable IP Ranges** table, click **Edit**  (if this is the first entry) or **Add**  if it is not.
 - b. Enter the IP Range Name. The IP range name can be anything meaningful; it is not referenced elsewhere in the configuration. In this example, enter: **radiology Subnet**
 - c. Enter the IP Range (or IP address) permitted to access the grid. If specifying a range, use one of:
 - a hyphenated list of IP addresses (e.g. 174.182.91.00-174.182.91.64)
 - a range of IP addresses specified using CIDR notation (e.g. 192.168.120.0/27)
 - an IP address in the form A.B.C.D, where at least one of A, B, C, or D is zero. If D is 0, then IPs between A.B.C.0 and A.B.C.255 will be in range. If C and D are both 0, then IPs between A.B.0.0 and A.B.255.255 will be in range. If B, C, and D are all 0, then IPs between A.0.0.0 and A.255.255.255 will be in range. If A, B, C, and D are all 0, then all IPs will be in range. In this example, enter: **192.168.120.54-192.168.120.56**

- d. Enter the Group ID for the device.

Group ID is used to determine optimal message routing and replication within the grid. Each group ID in the grid is associated with different link connection costs. You must choose a predefined group ID for your grid, or the value is ignored. For an HP MAS grid, the group ID for the Primary site is 101000 and 102000 for the DR site. Always place the device in the group for the Primary site. Enter: 101000

- e. Select **DICOM** to specify that the protocol can be used for connections.

- f. Click **Apply Changes**.

DICOM AE Titles from within the IP address range specified here can now access the grid.

Configuration: Grid Configuration - IP Ranges
Updated: 2008-04-25 13:15:30 PDT

Allowable IP Ranges

IP Range Name	IP Range	Group ID	DICOM	HTTP	Actions
Radiology Subnet	192.168.120.54-192.168.120.56	101000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Show 10 Records Per Page Refresh Previous « 1 » Next

Figure 12: IP Ranges

- g. Repeat for each IP range permitted to access the grid.

Once the IP addresses associated with the DICOM AE Titles identified earlier have been granted grid access, these DICOM entities can access the grid. The process of configuring access for a simple DICOM profile is complete.

Configuring Access Using a Complex DICOM Profile

This section provides step-by-step instructions for configuring access to the grid for a DICOM Entity.

The procedures described here use “backward configuration” — they start by defining the most specific part of the profile and end by defining the most general. Performing the configuration in this way avoids problems with dependencies, and ensures that clients cannot access the grid using the new profile until configuration is complete.

Advanced DICOM Configuration Profiles are generally necessary only for DICOM entities that have known compatibility issues, or to permit the use of private SOP classes.



Advanced DICOM Configuration Profile



The first step is to configure the Advanced DICOM Configuration Profiles needed to specify the access restrictions for the DICOM entity. You can build up a complex set of access restrictions by adding multiple lines to the table. When more than one entry is specified for a single Configuration Profile, the grid successively evaluates and applies the options specified in the table starting from the first entry and continuing to the last as described in “Advanced Config Profiles” on page 58.

Example 1

In this example, we will build an advanced profile that specifies a specific preferred transfer syntax for two SOP classes, and then sets the Preferred Transfer Syntax for all remaining SOP classes.

The profile is built by adding multiple entries with the same Profile Name to the Advanced Config Profile table. Given that the table is evaluated from the top down, we begin by specifying exceptions and end with specifying the most general case.

1. From the NMS, select **Grid Management ► Grid Configuration ► DICOM Advanced ► Configuration ► Main**
2. In the Advanced Config Profiles table, click **Add**  (or **Edit**  if this is the first entry in the table).
3. Enter a name for the Advanced Configuration Profile Name.
The name is case-sensitive, and must be repeated exactly on each line to ensure that all criteria belong to the same profile. For example, enter: `RemoteHospital`
4. Specify the preferred transfer syntax for MR Images and PET images to be DICOM JPEG Lossless Proc 14:
 - a. For the Advanced Configuration Profile Name, enter:
`RemoteHospital`
 - b. To set the preferred transfer syntax for MRI images, for SOP Class enter: `1.2.840.10008.5.1.4.1.1.4`
 - c. For Preferred Transfer Syntax, enter `1.2.840.10008.1.2.4.57` (the JPEG Lossless, non-hierarchical transfer syntax)
 - d. Ensure that the Behavior selected is **Allowed**.

- e. Click **Apply Changes**.
 - f. Click **Add**  to add another entry to the Advanced Config Profiles table.
 - g. Enter **RemoteHospital** for the Advanced Configuration Profile Name.
 - h. To set the preferred transfer class for PET images, for SOP Class, enter **1.2.840.10008.5.1.4.1.1.128**
 - i. For Preferred Transfer Syntax, enter **1.2.840.10008.1.2.4.57** (the JPEG Lossless, non-hierarchical transfer syntax)
 - j. Click **Apply Changes**.
5. Specify that all other SOP classes be allowed, and that they use Implicit VR Little Endian (1.2.840.10008.1.2) as their preferred transfer syntax.
- a. In the Advanced Config Profiles table, click **Add**  to add a new entry.
 - b. Enter **RemoteHospital** for the Advanced Configuration Profile Name.
 - c. For SOP Class, enter: *
 - d. For Preferred Transfer Syntax, enter **1.2.840.10008.1.2**
 - e. Click **Apply Changes**.

Advanced Config Profiles












Advanced Configuration Profile Name	Behavior	SOP Class	Preferred Transfer Syntax	Required Transfer Syntax	Actions
RemoteHospital	Allow	1.2.840.10008.5.1.4.1.1.4	1.2.840.10008.1.2.4.57		   
RemoteHospital	Allow	1.2.840.10008.5.1.4.1.1.128	1.2.840.10008.1.2.4.57		   
RemoteHospital	Allow	*	1.2.840.10008.1.2		   



Figure 13: Advanced Config Profiles

- 6. Next, create a DICOM Configuration Profile that uses this Advanced Configuration Profile.

Example 2

In this example, we will build an advanced profile that permits the use of a private SOP class that is not otherwise supported by the grid (according to its *DICOM Conformance Statement*).



- 1. From the NMS, select **Grid Management ► Grid Configuration ► DICOM Advanced ► Configuration ► Main**

2. In the Advanced Config Profiles table, click **Add**  (or **Edit**  if this is the first entry in the table).
3. Enter a name for the Advanced Configuration Profile Name.
The name is case-sensitive, and must be repeated exactly on each line to ensure that all criteria belong to the same profile. For example, enter: `PrivateClass`
4. Ensure that the Behavior selected is **Allowed**.
5. For SOP Class enter: `1.2.840.113619.4.27`
This is a private SOP class that does not fall into the standard DICOM hierarchy of classes (that begin with `1.2.840.10008`).
6. Leave the Preferred Transfer Syntax and Required Transfer Syntax fields blank to use the grid's preferred transfer syntax ("Little Endian Implicit").
7. Click **Apply Changes**.
8. Next, create a DICOM Configuration Profile that uses this Advanced Configuration Profile.

When you use the resulting DICOM Configuration Profile for an AE, the entity can now make associations and perform the permitted activities using this Private SOP class.

DICOM Configuration Profile

Create a DICOM Configuration Profile that includes the Advanced DICOM Config Profile that you have just defined. The following procedure uses the Advanced Configuration profile defined in Example 1 above.

1. From the NMS, select **Grid Management ► Grid Configuration ► DICOM Advanced ► Configuration ► Main**
2. In the DICOM Profiles table, **Edit**  (if this is the first entry) or **Add**  to add a new entry.
3. Type a meaningful Profile Name. For this example, enter: `RW_REMOT`
4. Select the DICOM options needed for the entity. In this example, we permit all activities. (See [Table 3: "Permission options for DICOM Profiles" on page 57](#) for more information on the options.)
5. For the Advanced Config Profile Name, enter: `RemoteHospital`
6. Select **Apply Changes**.

The screenshot displays the 'Configuration: Grid Configuration - DICOM Advanced' interface. It includes a navigation bar with 'Overview' and 'Configuration' tabs, and a 'Main' sub-tab. The main content area is titled 'Configuration: Grid Configuration - DICOM Advanced' and shows a legend for profile actions (S=Send to Grid, R=Receive from Grid, F=Find on Grid, M=Move from Grid, C=Storage Commitment). Below this are three tables:

Profile Name	S	R	F	M	C	Coerce Tag Profile Name	Advanced Config Profile Name	Behavioral Profile Name	Actions
READ_WRITE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				[Edit] [Add] [Delete] [Refresh]
READ_ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				[Edit] [Add] [Delete] [Refresh]
WRITE_ONLY	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				[Edit] [Add] [Delete] [Refresh]
R.W.REMOT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		RemoteHospital		[Edit] [Add] [Delete] [Refresh]

Below the first table is a 'Show 10 Records Per Page' dropdown and a 'Refresh' button. The second table, 'Coerce Tag Profiles (1 - 10 of 0)', has columns for Coerce Tag Profile Name, Tag, Tag Value, Query, Ingest, and Description. The third table, 'Advanced Config Profiles (1 - 3 of 3)', has columns for Advanced Configuration Profile Name, Behavior, SOP Class, Preferred Transfer Syntax, and Required Transfer Syntax.

Figure 14: DICOM Advanced

- Next enter the DICOM AE Titles for devices that are to be given grid access using this Profile.

DICOM AE Titles

This procedure defines a grid AE Title that specified remote entities may use to access the grid.

- From the NMS, select **Grid Management** ► **Grid Configuration** ► **DICOM** ► **Configuration** ► **Main**
- Click **Edit** (if this is the first entry) or **Add** to add the DICOM AE for the remote entity.
- Enter a Description of the DICOM device you are granting access to. In this example, enter: **CT at Hospital X**
- Enter the case-sensitive AE Title of the remote entity. In this example, enter: **CT_HOSX**
- Enter the IP Range (or IP address) that the device can connect from. In this example, enter: **174.182.91.00**
- Enter the Port that the remote DICOM device uses to listen for connections from the grid. In this example, enter: **5000**

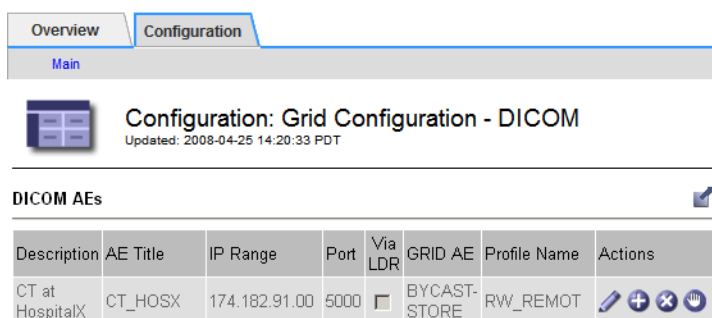
7. Do not select Via LDR.

DICOM associations are generally initiated via a CLB. The CLB identifies a preferred LDR for the transaction, and passes the association from the remote entity on to that LDR. Selecting Via LDR directs the LDR to communicate directly with the remote entity once an association has been made. However, in an HP MAS grid that uses a private network, the LDR is accessible only over the internal private network and cannot communicate directly with the remote entity.

8. Next, enter the GRID AE Title. In this example, enter: **BYCAST-STORE**

9. Select the DICOM Configuration Profile to associate with this GRID AE Title. In this example, select: **RW_REMOT**

10. Click **Apply Changes**.



The screenshot shows a web interface with tabs for 'Overview' and 'Configuration'. Under 'Configuration', there is a 'Main' section. Below that, a title 'Configuration: Grid Configuration - DICOM' is displayed with a timestamp 'Updated: 2008-04-25 14:20:33 PDT'. A section titled 'DICOM AEs' contains a table with the following data:

Description	AE Title	IP Range	Port	Via LDR	GRID AE	Profile Name	Actions
CT at HospitalX	CT_HOSX	174.182.91.00	5000	<input type="checkbox"/>	BYCAST-STORE	RW_REMOT	

Figure 15: Grid Management ► Grid Configuration ► DICOM

11. Next, enable grid access from the IP addresses that are used by the remote DICOM devices.

Allowable IP Ranges


This procedure enables devices using specified IP addresses to access the grid.

Note that:

- If an IP range specified here is more restrictive than the range specified for a DICOM AE Title, only DICOM entities in the range specified here are permitted to access the grid.
- The IP Range table is evaluated from the top down. An IP address is granted the permissions associated with the first matching entry in the table.

Once the IP addresses associated with the DICOM AE Titles identified earlier have been granted grid access, these DICOM entities can store

or retrieve data from the grid. The process of configuring access for a complex DICOM profile is complete.

1. From the NMS, select **Grid Management ► Grid Configuration ► IP Ranges ► Configuration ► Main**
2. Define a set of IP ranges permitted to access the grid:
 - a. In the **Allowable IP Ranges** table, click **Add**  to add a new IP range.
 - b. Enter the IP Range Name. In this example, enter: **Radiology Subnet**
 - c. Enter the IP Range (or IP address) permitted to access the grid. For this example, enter: **174.182.91.00-174.182.91.64**
 - d. Enter the Group ID. Enter: **101000**
 Group ID is used to determine optimal message routing and replication within the grid. Each group ID in the grid is associated with different link connection costs. In an HP MAS grid, 101000 is the standard group ID for devices at the Primary Site. You must use a predefined group ID.
 - e. Select **DICOM** and **HTTP** as the protocols permitted to make connections from within this IP range.
 - f. Click **Apply Changes**.

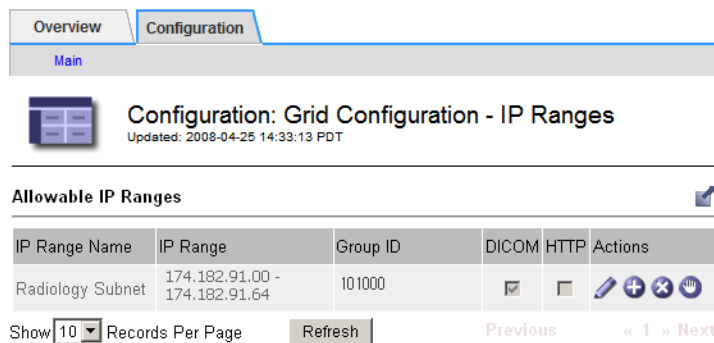


Figure 16: IP Ranges

DICOM AE Titles within the specified IP address range can now access the grid, using the DICOM Configuration Profile RW_REMOT, which in turn uses the Advanced DICOM Configuration Profile RemoteHospital.

Configuring Access Using a Coerce Tag Profile



This section provides step-by-step instructions for configuring a Coerce Tag Profile to partition DICOM data in the grid.


The procedure described here uses “backward configuration” —it starts by defining the most specific part of the profile and ends by defining the most general. Performing the configuration in this way avoids problems with dependencies, and ensures that clients cannot access the grid using the new profile until configuration is complete.

Before configuring a Coerce Tag Profile, consult the Solution Design document for your deployment to ensure that DICOM partitioning via Coerce Tags is required.

Coerce Tag Profile

The first step is to configure the Coerce Tag Profile needed to partition data for DICOM entities.

1. From the NMS, select **Grid Management** ► **Grid Configuration** ► **DICOM Advanced** ► **Configuration** ► **Main**
2. In the Coerce Tag Profiles table, click **Edit**  (if this is the first blank entry in the table) or **Add**  to add a new entry.
3. Enter a value for the Coerce Tag Profile Name.
The name is case-sensitive. For example, enter: **Hospital1**
4. Enter a value for the Tag. To partition data, enter the value:
(0009, 0080)
5. Enter a Tag Value. For example, enter: **PACS1**
6. Select **Query** and **Ingest**.
Selecting both options restricts data retrieved to data that has a (0009, 0080) tag with the value PACS1, and assigns a (0009, 0080) tag with the value PACS1 to all data saved by this device.
7. Enter a description for the profile. For example, enter: **Hospital 1 PACS**
8. Click **Apply Changes** to save the Coerce Tag Profile.

Coerce Tag Profiles 













Coerce Tag Profile Name	Tag	Tag Value	Query	Ingest	Description	Actions
Hospital1	(0009,0080)	PACS1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Hospital 1 PACS	   
Hospital2	(0009,0080)	PACS2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Hospital 2 PACS	   
Research	(0009,0080)	research	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Research Workstation	   


Figure 17: Coerce Tag Profiles

9. Repeat step 2 to step 8 to create a Coerce Tag Profile with the following values:
 - Coerce Tag Profile Name: **Hospital2**
 - Tag: **(0009, 0080)**
 - Tag Value: **PACS2**
 - **Query** and **Ingest** selected.
 - Description: **Hospital 2 PACS**
10. Finally, repeat step 2 to step 8 to create a Coerce Tag Profile with the following values:
 - Coerce Tag Profile Name: **Research**
 - Tag: **(0009, 0080)**
 - Tag Value: **research**
 - **Ingest** only selected
 - Description: **Research Workstation**

Note that the Research coerce tag applies a tag on ingest, but does not use tags on queries (as Query is not selected). This means that the Research coerce tag profile gives unrestricted read access to all grid data, regardless of the Coerce Tag assigned to the data at ingest.

After the Coerce Tag Profiles are created, use the procedure “Configuring Access Using a Simple DICOM Profile” on page 65 to:

- Create DICOM profiles that use these Coerce Tags. For example:

DICOM Profiles 

S=Send to Grid, R=Receive from Grid, F=Find on Grid, M=Move from Grid, C=Storage Commitment





















Profile Name	S	R	F	M	C	Coerce Tag Profile Name	Advanced Config Profile Name	Behavioral Profile Name	Actions
READ_WRITE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				   
RW_REMOT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		RemoteHospital		   
READ_ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				   
RW_HOSP1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Hospital1			   
RW_HOSP2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Hospital2			   

Figure 18: DICOM Profiles

- Assign the DICOM profiles to DICOM AE Titles
- Grant access to the IP ranges of these DICOM AEs

The end result is that entities assigned the RW_HOSP1 DICOM profile can save data to the grid, assigning it the Hospital1 coerce tag (that has the value PACS1). Entities assigned RW_HOSP1 can also access any data saved to the grid with the Hospital1 coerce tag profile. Therefore, the RW_HOSP1 DICOM profile is used by entities at the first hospital to save and retrieve data from that location. Entities using this profile can neither see nor retrieve data saved using other DICOM profiles (unless these profiles also use the Hospital1 coerce tag profile).

Likewise, entities assigned the RW_HOSP2 DICOM profile can access only data saved to the grid from the second hospital.

The remaining DICOM profiles do not specify a Coerce Tag Profile. Therefore, entities using the remaining DICOM profiles can access all data saved to the grid, regardless of the value of any assigned coerce tags, or whether the data had a coerce tag assigned at the time of ingest.

DICOM Device Test Report

Chapter Contents

Results Summary	82
DICOM Client Identification	82
Test Results	82
1: C-ECHO SCU Report	83
2: C-STORE SCU Report	84
3: C-STORE SCU with Storage Commitment Report	85
4: C-FIND SCU Report	86
5: C-MOVE SCU and C-STORE SCP Report	87

Results Summary

DICOM Client Identification

Record the device-specific information for the device under test.

DICOM Device Information
Make
Model
Software Version
AE Title
IP Address
Port

Test Results

Fill in this section after all recommended tests have been run. Enter one of:

- PASS
- FAIL
- N/A

Test Case	Result
1: C-ECHO SCU	
2: C-STORE SCU	
3: C-STORE SCU with Storage Commitment	
4: C-FIND SCU	
5: C-MOVE SCU and C-STORE SCP	
Overall Test Result	

1: C-ECHO SCU Report

Successful completion of this test confirms that the DICOM device supports using the DICOM ping-like service provided by the HP MAS system.

Recorded Data

Start of Procedure

Inbound C-Echoes - Successful

End of Procedure

Inbound C-Echoes - Successful

Additional Comments

Expected Results

Y **N**

The DICOM device received a C-ECHO response.

The number of "Inbound C-Echoes - Successful" increased as expected.

Test Result (PASS/FAIL):

2: C-STORE SCU Report

Successful completion of this test confirms that the DICOM device supports using the DICOM store service provided by the HP MAS system.

Recorded Data

Start of Procedure

Inbound C-Stores - Successful

End of Procedure

Inbound C-Stores - Successful

Additional Comments

Expected Results

The HP MAS system successfully received the study.

Y

N

The number of "Inbound C-Stores - Successful" increased as expected.

Test Result (PASS/FAIL):

3: C-STORE SCU with Storage Commitment Report

Successful completion of this test confirms that the DICOM device supports using the DICOM store and storage commitment service provided by the HP MAS system.

Recorded Data

Start of Procedure

Inbound Storage Commitments - Successful

End of Procedure

Inbound Storage Commitments - Successful

Additional Comments

Expected Results

	Y	N
The HP MAS system successfully received the study.	<input type="checkbox"/>	<input type="checkbox"/>
The DICOM device successfully received a storage commitment response.	<input type="checkbox"/>	<input type="checkbox"/>
The number of "Inbound Storage Commitments - Successful" increased as expected.	<input type="checkbox"/>	<input type="checkbox"/>

Test Result (PASS/FAIL):

4: C-FIND SCU Report

Successful completion of this test confirms that the DICOM device can utilize the DICOM find service provided by the HP MAS system.

Recorded Data

Start of Procedure

Inbound C-Finds - Successful

End of Procedure

Inbound C-Finds - Successful

Additional Comments

Expected Results

	Y	N
The DICOM device successfully received the expected list of studies for each query performed.	<input type="checkbox"/>	<input type="checkbox"/>
The number of "Inbound C-Finds - Successful" increased as expected.	<input type="checkbox"/>	<input type="checkbox"/>

Test Result (PASS/FAIL):

5: C-MOVE SCU and C-STORE SCP Report

Successful completion of this test confirms that the DICOM device supports using the DICOM move service provided by the HP MAS system. This result also confirms that the device provides a DICOM store service that the HP MAS system can use.

Recorded Data

Start of Procedure

Inbound C-Moves - Successful

Outbound C-Stores - Successful

End of Procedure

Inbound C-Moves - Successful

Outbound C-Stores - Successful

Additional Comments

Note the presentation syntax of the studies retrieved on the back of this sheet.

Expected Results

	Y	N
The selected studies were retrieved.	<input type="checkbox"/>	<input type="checkbox"/>
The number of "Inbound C-Moves - Successful" increased as expected.	<input type="checkbox"/>	<input type="checkbox"/>
The number of "Outbound C-Stores - Successful" increased as expected.	<input type="checkbox"/>	<input type="checkbox"/>

Test Result (PASS/FAIL):

Connectivity

Connection requirements for the NMS interface and the server command shell

Chapter Contents

Service Laptop Requirements	90
Browser Settings	90
NMS Connection Procedure.....	91
Security Certificate	92
Log In	92
Enable Pop-ups	93
Log Out.....	93
Command Shell Access Procedures	93
Log In	93
Accessing a Server Remotely.....	94
Log Out.....	95

Service Laptop Requirements

The requirements for the service laptop used to connect to the NMS interface are:

- Microsoft® Windows® operating system.
- Network Interface Card (NIC) adapter for connection to the customer's network. You should also have a cable in case one is not readily available at the customer's site.
- CD drive (to read the Software Activation backup CD)
- Microsoft Internet Explorer v6.0 SP2 or Microsoft Internet Explorer v7.0
JavaScript and cookies *must* be enabled.

Browser Settings

Internet Options Settings

You need to verify that the Internet Explorer settings for temporary internet files, security and privacy are set correctly.

To verify the Internet Explorer settings:

1. Go to **Tools ► Internet Options ► General**
2. In the Temporary Internet files box, click **Settings**.
3. In the Check for newer versions of stored pages section, verify that **Automatically** is selected.

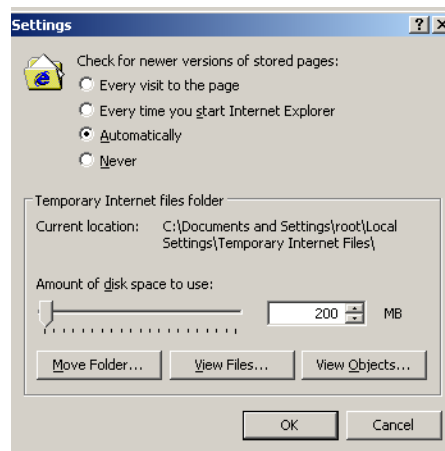


Figure 19: Temporary Files Setting

4. Go to **Tools ► Internet Options ► Security ► Custom Level** and ensure that the Active Scripting setting is Enable

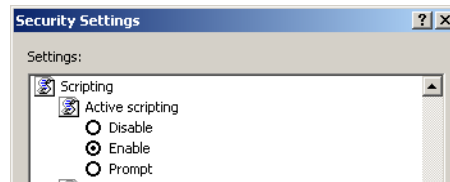


Figure 20: Active Scripting Setting

- Go to **Tools ► Internet Options ► Privacy** and ensure that the privacy setting is Medium or lower (cookies must be enabled).

NMS Connection Procedure

Connecting to the NMS interface at the customer site requires access to the customer's network in close proximity to the HP MAS cabinets.

To connect to the NMS interface:

1. Work with the customer system administrator to establish the physical network connection to the service laptop. Using the customer's network rather than a direct connection within the cabinet verifies that the interface is accessible using the same infrastructure the customer uses.
2. Insert the Software Activation backup CD, and open:
 - Configuration.txt
 - Passwords.txt
3. From the Configuration.txt file, note the IP address of the Admin Node on the customer network. This is needed to access the NMS interface.
4. From the Passwords.txt file, note the NMS password for the Vendor account or the Admin account.
5. Launch the web browser.
6. Open the address **https://<IP_address>**
 where <IP_address> is the address of the Admin Node hosting the CMN service on the customer network specified in the Configuration.txt file.

Security Certificate

Depending on your version of Windows and web browser, you may be prompted with a Security Alert window when you access the NMS URL.

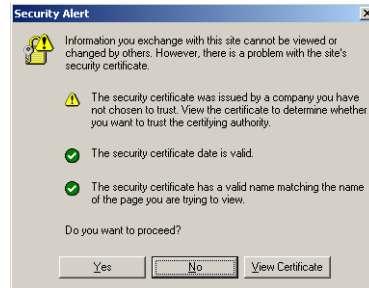


Figure 21: Security Alert Window

If this appears, you can either:

- Click **Yes** to proceed with this session. The alert will appear again the next time you access this URL.
- Click **View Certificate** and install the certificate using the installation wizard so that you no longer receive the alert.

Log In

You are presented with the NMS login window.



Figure 22: NMS Login Window

To log in:

1. Enter the username **Vendor** for full access to the NMS. If you are not making grid-wide configuration changes, you can also use the **Admin** account. For more information, see the *Administrator Guide*.
2. Enter the password for the NMS specified in the Passwords.txt file.

Enable Pop-ups

To make any changes to passwords, you must ensure that Internet Explorer has the Pop-up Blocker turned *off*.

To enable pop-ups:

- Select **Tools ► Pop-up Blocker ► Turn off Pop-up Blocker** from the Internet Explorer main menu to open the Pop-up Blocker Settings dialog.

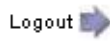
NOTE Note that the menu option is a toggle. If the blocker was already disabled, the menu option is to Turn on the Pop-up Blocker.

You may now use the NMS Account Management feature to change access passwords.

Log Out

When you have finished your NMS session, log out to keep the system secure.

To log out:

1. Click **Logout**  located at the top right corner of the screen. The logging out message appears.
2. You may safely close the browser or continue using other applications.

NOTE Failure to log out may give unauthorized users access to your NMS session. Simply closing your browser is *not* sufficient to log out of the session.

Command Shell Access Procedures

Log In

To log in at the console of a server:

1. Press **<Alt>+<F1>** to access a command shell.
2. Enter the account name `root`

3. Enter the password for the server listed in the Passwords.txt file.

Accessing a Server Remotely

There are two ways to access a server remotely using SSH:

- from the primary Admin Node using the SSH key password
- from any server using the remote server password

By default, the Admin Node that hosts the CMN service acts as an SSH access point for the grid. When passwordless access is enabled, you can SSH to other servers from the Admin Node without entering their password. The procedure to enable passwordless access to grid nodes is described in the Network Configuration chapter of the *Administrator Guide*.

To access a remote server using the SSH key password:

1. Log in to the Admin Node hosting the CMN service.
2. Enter: `ssh <IP_address>`

where `<IP_address>` is the IP address of the remote server.

— or —

Enter: `ssh <hostname>`

where `<hostname>` is the name of the server.

If the remote server was added as a result of a grid expansion, use the server IP address instead of the hostname.

3. When prompted, enter the SSH private key password listed in the SSH Access Password section of the Passwords.txt file.

You may now execute commands on the remote server as if you were logged in to that server directly.

To access a remote server using the remote server password:

1. Log in to any local server.
2. Enter: `ssh <IP_address>`

where `<IP_address>` is the IP address of the remote server.

— or —

Enter: `ssh <hostname>`

where `<hostname>` is the name of the server.

If the remote server was added as a result of a grid expansion, use the server IP address instead of the hostname.

3. When prompted, enter the password for the remote server listed in the Passwords.txt file.

You may now execute commands on the remote server as if you were logged into that server directly.

Log Out

To log out of a command shell session:

1. Enter `exit` to close the current command shell session.
2. Press `<Alt>+<F7>` to return to the Server Manager GUI.

Glossary

- ACL** Access control list—Specifies what users or groups of users are allowed to access an object and what operations are permitted, for example read, write, and execute.
- ADC** Administrative Domain Controller—A software component of the HP MAS product. The ADC service maintains topology information, provides authentication services, and responds to queries from the LDR, CMS, and CLB. The ADC service is found on the Control Node.
- ADE** Asynchronous Distributed Environment—Proprietary development environment used as a framework for grid services within the HP MAS system.
- Admin Node** A building block of the HP MAS product. The Admin Node provides services for the web interface, grid configuration, and audit logs.
- AE title** Application Entity Title—The identifier of a DICOM node communicating with other DICOM AEs.
- AMS** Audit Management System—A software component of the HP MAS product. The AMS service monitors and logs all audited system events and transactions to a text log file. The AMS service is found on the Admin Node.
- API** Application Programming Interface—A set of commands and functions, and their related syntax, that enable software to use the functions provided by another piece of software.
- ARC** Archive—A software component of the HP MAS product. The ARC service manages interactions with archiving middleware that controls nearline archival media devices such as tape libraries. The ARC service is found on the Archive Node.
- Association** A connection protocol between two DICOM Application Entities (AEs), typically a local and remote AE. The AEs use the Association Establishment to negotiate the type of data to exchange and the format of data encoding.
- audit message** Information about an event occurring in the HP MAS system that is captured and logged to a file.

atom	Atoms are the lowest-level component of the container data structure, and generally encode a single piece of information. (Containers are sometimes used when interacting with the grid via the HTTP API).
AutoYaST	An automated version of the Linux installation and configuration tool YaST (“Yet another Setup Tool”), which is included as part of the SUSE Linux distribution.
BASE64	A standardized data encoding algorithm that enables 8-bit data to be converted into a format that uses a smaller character set, enabling it to safely pass through legacy systems that can only process basic (low order) ASCII text excluding control characters. See RFC 2045 for more details.
bundle	A structured collection of configuration information used internally by various components of the grid. Bundles are structured in container format.
Bycast Enablement Layer	The Bycast Enablement Layer CD is used during installation to customize the Linux operating system installed on each grid server. Only the packages needed to support the services hosted on the server are retained, which minimizes the overall footprint occupied by the operating system and maximize the security of each grid node.
cabinet	Used to house hardware components, a cabinet includes the physical rack and all power and network wiring required for an installation.
cabinet connectivity kit	Used to link cabinets. One Cabinet Connectivity Kit is required at Single Site installations that have more than one cabinet, and one is required at each site in a Single Site + DR installation. The Cabinet Connectivity Kit is installed in the Base Cabinet. See also: “WAN Connectivity Kit” .
CBID	Content Block Identifier—A 64-bit number that uniquely identifies a piece of content within the HP MAS system. CBIDs are represented as a zero-padded, 16-character, hexadecimal number when used to refer to a unique piece of content using the HTTP interface.
CIDR	Classless Inter-Domain Routing—A notation used to compactly describe a subnet mask used to define a range of IP addresses. In CIDR notation, the subnet mask is expressed as an IP address in dotted decimal notation, followed by a slash and the number of bits in the subnet. For example, 192.168.110.0/24.
CIFS	Common Internet File System—A file system protocol based on SMB (Server Message Block, developed by Microsoft) which coexists with protocols such as HTTP, FTP, and NFS.

CLB	Connection Load Balancer—A software component of the HP MAS product. The CLB service provides a gateway into the grid for clients connecting via DICOM and HTTP protocols. The CLB service is part of the Gateway Node.
CMN	Configuration Management Node— A software component of the HP MAS product. The CMN service manages system-wide configuration and grid tasks. The CMN service is found on the Admin Node.
CMS	Content Management System— A software component of the HP MAS product. The CMS service manages content metadata and content replication according to the rules specified by the ILM policy. The CMS service is found on the Control Node.
command	In HTTP, an instruction in the request header such as GET, HEAD, DELETE, OPTIONS, POST, or PUT. Also known as an HTTP method.
connectivity kit	See “ cabinet connectivity kit ” and “ WAN Connectivity Kit ”.
container	A container is a data structure used by the internals of grid software. In the HTTP API, an XML representation of a container is used to define queries or audit messages submitted using the POST command. Containers are used for information that has hierarchical relationships between components. The lowest-level component of a container is an atom. Containers may contain 0 to N atoms, and 0 to N other containers.
content block ID	See “ CBID ”.
Control Node	A building block of the HP MAS product. The Control Node provides services for managing content metadata and content replication.
C-STORE	A DICOM operation to send data between devices.
CSTR	Null-terminated, variable length string.
DC	Data Center.
DFSG	Distributed File System Gateway—A primary gateway cluster that uses the GPFS™ file system. Replication groups that include a DFSG also have a Secondary FSG that uses the XFS™ file system.
DICOM	Digital Imaging and COmmunications in Medicine—A standard developed by ACR-NEMA (an alliance of the American College of Radiology and the National Electrical Manufacturer’s Association) for communications between medical imaging devices.

DR	Disaster Recovery.
EVA	Enterprise Virtual Array—an HP product that uses virtual arrays to allocate SAN or Fibre Channel storage resources to different uses.
Fibre Channel	A networking technology primarily used for storage. The standard connection type for SAN.
FCS	Fixed Content Storage—a class of stored data where the data, once captured, is rarely changed and must be retained for long periods of time in its original form. Typically this includes images, documents, and other data where alterations would reduce the value of the stored information.
FSG	File System Gateway—A software component of the HP MAS product. The FSG service enables standard network file systems to interface with the grid. The FSG service is found on the Gateway Node.
FSG replication group	A replication group is a group of FSGs that provide grid access to a specified set of clients. Within each replication group, one FSG is a primary and all others are secondaries. The primary FSG allows clients read and write access to the grid, while storing file system information (stubs) for all files saved to the grid. The secondary FSG “replicates” file system information, and backs up this information to the grid on a regular schedule.
Gateway Node	A building block of the HP MAS product. The Gateway Node provides connectivity services for NFS/CIFS file systems and the HTTP and DICOM protocols.
GPFS	General Parallel File System™—A high-performance clustered file system developed by IBM.
grid node	The name of the HP MAS product building blocks, for example Admin Node or Control Node. Each type of grid node consists of a set of services running on a server.
Grid Specification File	An XML file that provides a complete technical description of a specific grid deployment. It describes the grid topology, and specifies the hardware, grid options, server names, network settings, time synchronization, and gateway clusters included in the grid deployment. The Deployment Grid Specification file is used to generate the files needed to install the grid.
Grid Task	A managed sequence of actions that are coordinated across a grid to perform a specific function (such as adding new node certificates).

Grid Tasks are typically long-term operations that span many entities within the grid. See also “[Task Signed Text Block](#)”.

- HP MAS** HP Medical Archive solution — Fixed-content grid storage system from Hewlett-Packard. The solution is sold under the HP brand and is serviced and supported by the HP services/support organization worldwide. The HP MAS Solution is powered by Bycast® StorageGRID® software.
- HTTP** Hyper-Text Transfer Protocol—A simple, text based client/server protocol for requesting hypertext documents from a server. This protocol has evolved into the primary protocol for delivery of information on the World Wide Web.
- HTTPS** Hyper-Text Transfer Protocol, Secure—URIs that include HTTPS indicate that the transaction must use HTTP with an additional encryption/authentication layer and often, a different default port number. The encryption layer is usually provided by SSL or TLS. HTTPS is widely used on the internet for secure communications.
- ILM** Information Lifecycle Management—A process of managing content storage location and duration based on content value, cost of storage, performance access, regulatory compliance and other such factors.
- inode** On UNIX/Linux systems, data structure that contains information about each file, for example, permissions, owner, file size, access time, change time, and modification time. Each inode has a unique inode number.
- instance** A DICOM term for an image. One or more instances for a single patient are collected in a “study”. For example, each “slice” of an MRI is an instance; together, the full set of slices is a study.
- KVM** Keyboard, Video, Mouse—A hardware device consisting of a keyboard, LCD screen (video monitor), and mouse that permits a user to control all servers in a cabinet.
- LAN** Local Area Network—A network of interconnected computers that is restricted to a small area, such as a building or campus. A LAN may be considered a node to the Internet or other wide area network. Contrast with WAN.
- latency** Time duration for processing a transaction or transmitting a unit of data from end to end. When evaluating system performance, both throughput and latency need to be considered. See also “[throughput](#)”.

LDR	Local Distribution Router—A software component of the HP MAS product. The LDR service manages the storage and transfer of content within the grid. The LDR service is found on the Storage Node.
metadata	Information related to or describing an object stored in the grid, for example file ingest path or ingest time.
namespace	A set whose elements are unique names. There is no guarantee that a name in one namespace is not repeated in a different namespace.
nearline	A term describing data storage that is neither “online” (implying that it is instantly available like spinning disk) nor “offline” (which could include offsite storage media). An example of a nearline data storage location is a tape that is loaded in a tape library, but is not necessarily mounted.
NFS	Network File System—A protocol (developed by SUN Microsystems) that enables access to network files as if they were on local disks.
NMS	Network Management System—A software component of the HP MAS product. The NMS service provides a web-based interface for managing and monitoring the HP MAS system. The NMS service is found on the Admin Node.
node ID	An identification number assigned to a grid service within the HP MAS system. Each service (such as an CMS or ADC) in a single grid must have a unique node ID. The number is set during system configuration and tied to authentication certificates.
NTP	Network Time Protocol—A protocol used to synchronize distributed clocks over a variable latency network such as the internet.
object store	A configured file system on a disk volume. The configuration includes a specific directory structure and resources initialized at system installation.
PACS	Picture Archiving and Communication System—A computerized system of patient records management responsible for short and long term (archival) storage of images.
presentation context	A combination of a DICOM SOP Class and a transfer syntax; the type and format of a DICOM transaction.
provisioning	The process of editing the Grid Specification File (if required) and generating or updating the SAID package. This is done on the Admin Node using the provision command. The new or updated

SAID package is saved to the Provisioning USB flash drive. See “[Grid Specification File](#)” and “[SAID](#)”.

- SAID** Software Activation and Integration Data—Generated during provisioning, the SAID package contains site-specific files and software needed to install a grid.
- Samba** A free suite of programs which implement the Server Message Block (SMB) protocol. Allows files and printers on the host operating system to be shared with other clients. For example, instead of using telnet to log into a Unix machine to edit a file there, a Windows user might connect a drive in Windows Explorer to a Samba server on the Unix machine and edit the file in a Windows editor. A Unix client called “*smbclient*”, built from the same source code, allows FTP-like access to SMB resources.
- SAN** Storage Area Network — A high-speed network connecting heterogeneous storage devices to servers.
- SATA** Serial Advanced Technology Attachment—A connection technology used to connect servers and storage devices.
- SCP** Storage Class Provider—A device that provides images (a storage class) to a DICOM compliant system. Contrast with “*SCU*”.
- SCSI** Small Computer System Interface — —A connection technology used to connect servers and peripheral devices such as storage systems.
- SCU** Storage Class User—A device that receives (uses) images (a storage class) from a DICOM compliant system. Contrast with “*SCP*”.
- server** Used when referring specifically to hardware.
- service** A unit of the HP MAS software such as the ADC, CMS or SSM.
- SLES** SUSE Linux Enterprise Server—A commercial distribution of the SUSE Linux operating system, used with the HP MAS system.
- SOP class** Service-Object Pair Class—The combination of an information object description (IOD) and the set of Services that are useful for a given purpose.
- SOP instance** Service-Object Pair (SOP) Instance—A specific occurrence of an Information Object.
- SQL** Structured Query Language— An industry standard interface language for managing relational databases. An SQL database is one that supports the SQL interface.

SSAM	IBM® System Storage™ Archive Manager.
ssh	Secure Shell— A Unix shell program and supporting protocols used to log in to a remote computer and execute commands over an authenticated and encrypted channel.
SSM	Server Status Monitor— A unit of the HP MAS software that monitors hardware conditions and reports to the NMS. Every server in the grid runs an instance of the SSM. The SSMS service is present on all grid nodes.
SSL	Secure Socket Layer— The original cryptographic protocol used to enable secure communications over the internet. See TLS.
Storage Node	A building block of the HP MAS product. The Storage Node provides storage capacity and services to store, move, verify, and retrieve objects stored on disks.
StorageGRID®	A registered trademark of Bycast Inc. for their fixed-content storage grid architecture and software system.
study	A DICOM term for a collection of images (instances) related to an individual patient or subject.
SUSE	See SLES— SUSE Linux Enterprise Server.
Archive Node	A building block of the HP MAS product. The Archive Node manages storage of data to nearline data storage devices such as such as tape libraries (via IBM Tivoli® Storage Manager).
Task Signed Text Block	A BASE64 encoded block of cryptographically signed data that provides the set of instructions that define a grid task.
TCP/IP	Transmission Control Protocol / Internet Protocol— A process of encapsulating and transmitting packet data over a network. It includes positive acknowledgement of transmissions.
throughput	The amount of data that can be transmitted or the number of transactions that can be processed by a system or subsystem in a given period of time. See also “latency”.
TLS	Transport Layer Security— A cryptographic protocol used to enable secure communications over the internet. See RFC 2246 for more details.
transfer syntax	The parameters, such as the byte order and compression method, needed to exchange data between systems.

TSM	Tivoli® Storage Manager — IBM storage middleware product that manages storage and retrieval of data from removable storage resources.
URI	Universal Resource Identifier—A generic set of all names or addresses used to refer to resources that can be served from a computer system. These addresses are represented as short text strings.
UTC	A language-independent international abbreviation, UTC is neither English nor French. It means both “Coordinated Universal Time” and “Temps Universel Coordonné”. UTC refers to the standard time common to every place in the world.
UUID	Universally Unique Identifier—Unique identifier for each piece of content in the HP MAS. UUIDs provide client applications with a content handle that permits them to access grid content in a way that does not interfere with the grid’s management of that same content. A 128-bit number which is guaranteed to be unique. See RFC 4122 for more details.
XFS	A scalable, high performance journaled file system originally developed by Silicon Graphics.
WAN	Wide Area Network—A network of interconnected computers that covers a large geographic area such as a country. Contrast with “LAN”.
WAN Connectivity Kit	Required for linking the primary and DR sites of an HP MAS deployment. The WAN Connectivity Kit is installed in the Base Cabinet at both locations. See also “ cabinet connectivity kit ”.
XML	eXtensible Markup Language—A text format for the extensible representation of structured information; classified by type and managed like a database. XML has the advantages of being verifiable, human readable, and easily interchangeable between different systems.

