HP Medical Archive solution

Software version: 8.1.0

DICOM Integration Guide

Document release date: May 2010
Software release date: November 2009

Legal notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted rights legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Licensing

The use of HP products is governed by the terms and conditions of the applicable End User License Agreement (EULA).

Copyright notices

Trademark notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Contents

About this document

References

NEMA DICOM Standard, PS 3.1 – 3.13, (1996 – 2003) – The DICOM Standard

Terminology

The following acronyms and abbreviations are used in this document:

AE	Application Entity
IOD	Information Object Definition
PDU	Protocol Data Unit
SCU	DICOM Service Class User
SCP	DICOM Service Class Provider
SOP	Service/Object Pair
UID	Unique Identifier (unique string in the entire network)

Related documentation

In addition to this guide, please refer to other documents for this product:

- *HP Medical Archive solution Release Notes* for 8.1.1
- *HP Medical Archive solution user guide*
- *HP Medical Archive solution audit message reference*
- *HP Medical Archive solution Siemens Integration Guide*
- *HP Medical Archive solution DICOM Conformance Statement*
- *HP Medical Archive solution IHE Integration Statement*

These and other HP documents can be found on the HP documents web site:

http://www.hp.com/support/

Documentation updates

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

- Software version number

  Indicates the software version.

- Document release date

  Changes each time the document is updated.

- Software release date

  Indicates the release date of this version of the software.

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

http://ovweb.external.hp.com/lpe/doc_serv/

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

You can also receive updated or new editions if you subscribe to the appropriate product support service. For details, contact your HP sales representative.

Subscription service

HP strongly recommends that customers sign up online using the Subscriber's choice web site:

http://www.hp.com/go/e-updates

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest versions of drivers, and firmware documentation updates as well as instant access to numerous other product resources.
- After signing up, you can quickly locate your products under Product Category.

Support

You can visit the HP Software Support web site at:

http://www.hp.com/go/hpsoftwaresupport

HP Software Support Online provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests

- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

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

For more information about HP Passport, go to:

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

1 DICOM Integration Preparation

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. You must acquire the DICOM integration details and then send the Grid Specification file, exported from the NMS MI, to HP 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.

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 the 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 (page 12).

You may want to photocopy report forms from Appendix B, DICOM Device Test Report 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).
- This guide.

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

2 Enable or Update DICOM Connections

This chapter covers the two processes that take place on the HP MAS system 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 system. This chapter describes how to create a DICOM Application Entity (AE) definition for each DICOM AE that is permitted to use the HP MAS system.

The mechanism that enables DICOM access is controlled by the Grid Management > Grid Configuration > DICOM Advanced 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, Grid Access for Client Applications 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 advanced activities. Review all documentation before beginning.

Preparation

Enabling or disabling DICOM on a grid requires you to make a request to HP Support that references the customer's Grid ID and includes an updated Customer Questionnaire and the latest Provisioned Grid Specification file copied from the primary Admin Node. A new Deployment Grid Specification file is returned.

To facilitate future maintenance, when you change the client integration 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:

- `Passwords.txt` file
- `Configuration.txt` file
- The Customer Questionnaire
- Service laptop computer equipped as noted in Connectivity (page 81)

Enable the DICOM Option

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

Acquire Updated Deployment Grid Specification File

Export the Provisioned Grid Specification file from the primary Admin Node and send it along with the Customer Questionnaire to HP Support. Support updates this grid specification file and returns a new Deployment Grid Specification file that you can use to enable DICOM.

To acquire an updated Deployment Grid Specification file:

1. Export the latest grid specification file from the grid, following the instructions in Export the Latest Grid Specification File (page 72).
2. Send the latest provisioned grid Specification file along with the Customer Questionnaire to HP Support.

   The Provisioned Grid Specification file is updated to include DICOM, and a Deployment Grid Specification file is returned via e-mail.
3. When the updated grid specification file is returned to you, save it to the service laptop and begin the provisioning process.

Provision the Grid

To enable DICOM, you must provision the grid with the updated grid specification file to generate a new SAID package, as described in Provision the Grid (page 75). Generating a new SAID package creates a new grid task which you use to enable DICOM.

Enable DICOM

Prerequisites

- Ensure that no grid tasks are running. The only exceptions are:
  - LDR content rebalancing grid task (LBAL)
  - ILM evaluation (ILME)
  - LDR foreground verification (LFGV)

These grid tasks can run concurrently with the grid task that removes cluster bindings. If any other grid tasks are running, wait for them to complete or release their lock, or abort them as appropriate. For more information on grid tasks and resource locking, contact HP Support.

Procedure

To enable the DICOM option:

1. Go to **CMN > Grid Tasks > Configuration > Main**.
2. In the **Actions** pull-down menu adjacent to the Enable DICOM grid task, select Start.

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.

3. Click **Apply Changes**.

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

   The task continues to run 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 HP 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 MI using the `Vendor` account. using the `Vendor` account. For more information, see NMS Connection Procedure (page 82).

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 (page 45). 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.

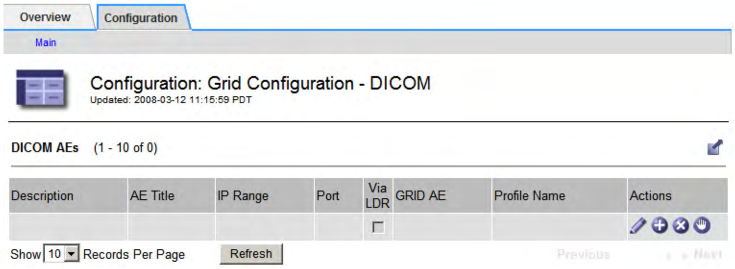
  — **READ_ONLY**: Commonly used for diagnostic stations. Provides access to data stored on the grid, but does not allow storing content (that is, R (retrieve), F (find), and M (move) are selected).

  The predefined profiles do *not* use any of the following features. If any of these are required, you must build a custom profile:

  - a Behavioral Profile–used for integration with specific PACS only, and described in Behavioral Profile Name (page 40).
  - a Coerce Tag Profile–used to create a DICOM partition, as explained in DICOM Partitions (page 43).
  - 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 (page 40).

⚠ WARNING! Creating a custom profile is an advanced activity. Review all documentation before beginning.

1 Go to **Grid Management > Grid Configuration > DICOM > Configuration**.



Configuration: Grid Configuration - DICOM
Updated: 2008-03-12 11:15:59 PDT

DICOM AEs (1 - 10 of 0)

Description	AE Title	IP Range	Port	Via LDR	GRID AE	Profile Name	Actions
				☐			

Show 10 Records Per Page Refresh

Figure 1 No DICOM Entities Enabled

2 Click **Edit** (if this is the first entry) or **Add** to add a new DICOM AE.

3 Define a new DICOM AE entry within the HP MAS system, 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 in 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

h Repeat this process from step 2 to add definitions for all DICOM clients listed in the Customer Questionnaire Document.

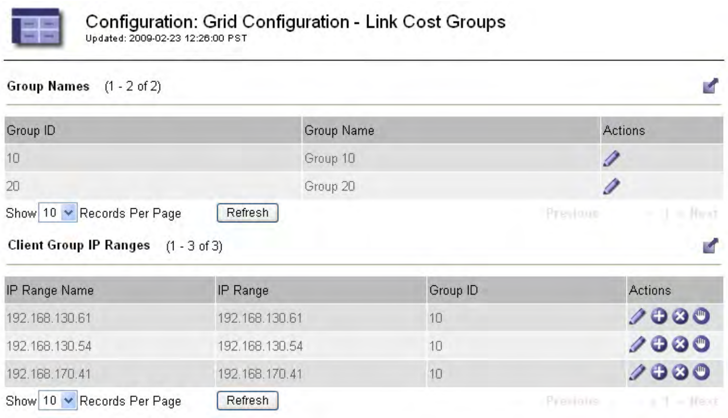
i Click **Apply Changes**.

The DICOM AE definitions is added to the HP MAS system.

The entities now have permission to use the grid.

4 Assign groups to the DICOM AE entries:

a Go to **Grid Management > Grid Configuration > Link Cost Groups > Configuration**.



Configuration: Grid Configuration - Link Cost Groups
Updated: 2009-02-23 12:26:00 PST

Group Names (1 - 2 of 2)

Group ID	Group Name	Actions
10	Group 10	✎
20	Group 20	✎

Show 10 Records Per Page Refresh Previous 1 Next

Client Group IP Ranges (1 - 3 of 3)

IP Range Name	IP Range	Group ID	Actions
192.168.130.61	192.168.130.61	10	✎ ⊕ ⊗ ⊖
192.168.130.54	192.168.130.54	10	✎ ⊕ ⊗ ⊖
192.168.170.41	192.168.170.41	10	✎ ⊕ ⊗ ⊖

Show 10 Records Per Page Refresh Previous 1 Next

Figure 2 Client Group IP Ranges

b In the **Client Group IP Ranges** table, click **Edit** ✎ (if this is the first entry) or **Insert** ⊕ to add a new IP range.

c Assign a group to the DICOM entity using the settings defined in the Customer Questionnaire:

- Enter a name for the range. The IP range name can be anything meaningful; it is not referenced elsewhere in the configuration.
- Enter the IP address assigned to the entity into the IP Range field.
- Enter the group ID for that IP range.

  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.

d Click **Apply Changes**.

e Repeat this process from step b to add definitions for all DICOM clients listed in the customer questionnaire.

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

5 Click **Logout** to close the NMS MI session.

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 grid, changes can be made using the CMN service. Only the Vendor account can access the CMN configuration pages of the NMS MI.

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 with the desired permissions.

NOTE Determining the profile settings needed for any particular behavior is beyond the scope of this procedure. For more information on determining profile settings, see Appendix A, Grid Access for Client Applications.

To change DICOM entity access:

1. Access the NMS MI using the `Vendor` account. For more information, see NMS Connection Procedure (page 82).
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. If there is no profile defined for the behavior you want to set, define a new profile with the desired settings.
   - — For more information on the general process, and for details of the kinds of behavior that can be specified via a DICOM profile, see DICOM Configuration (page 37) of Appendix A, Grid Access for Client Applications.
   - — For a detailed step by step example showing how to create an updated profile, see:

- Configuring Access Using a Simple DICOM Profile (page 45)

—or—

- Configuring Access Using a Complex DICOM Profile (page 49)

5 Assign the profile to the DICOM AE:

a Go to **Grid Management > Grid Configuration > DICOM > Configuration**.

b Locate the DICOM AE title to be modified.

c Click **Edit** ✎ 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

To delete a DICOM AE Title integration:

1 Access the NMS MI using the `Vendor` account. For more information, see NMS Connection Procedure (page 82).

2 Go to **Grid Management > Grid Configuration > DICOM > Configuration**.

3 Locate the AE Title in the list and note the IP Address of the entity.

4 Click **Delete** ⊗ 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.

3 Client DICOM AE Integration

After the HP MAS system 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[a]	5104 for Read, Find, and Move (the standard READ_ONLY profile). 5105 for Store and Storage Commitment (the standard READ_WRITE profile)

[a] You can verify the DICOM port numbers configured for your grid using the NMS MI. They are listed as the CLB DICOM ports on the Grid Management > Grid Configuration > Storage page. Do NOT use the LDR DICOM ports.

Additionally, the HP MAS system 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. For more information, see Define the DICOM Application Entity (page 14).

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.

Unrestrained Queries By a Client

When using a client application that retrieves images directly from the grid, avoid issuing unrestrained queries. That is, avoid queries that are equivalent to entering a wildcard value for all data fields such as patient name, study date, etc.

No results are returned for such queries. Depending upon the client, you may also receive a message such as “The Parameter is incorrect”, or “Peer aborted the association”.

Client Device Settings

These settings describe the client device, and have usually been set at the DICOM client device before grid integration begins. This information should have been provided to HP Support during deployment of your grid or your expansion site. Verify that the settings are entered correctly into the NMS MI, 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 MI, corrective action is needed. The first choice is to adjust the settings at the device to match the NMS MI settings. If the customer cannot accommodate a change to the local device settings, the settings made in the NMS MI 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 HP Support.

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 MI, 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 MI.

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 MI. 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. The following are the default ports configured on the grid for DICOM transactions[1]:

- 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

[1] You can verify the DICOM port numbers configured for your grid using the NMS MI. They are listed as the CLB DICOM ports on the Grid Management > Grid Configuration > Storage page. Do NOT use the LDR DICOM ports.

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.

4 DICOM Integration Verification

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 system.

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 system is usually configured with the following DICOM profiles:

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

Test Setup

The NMS MI is used to monitor the results of transactions with the HP MAS system. The NMS MI 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. Go to **SN2-A-1 > LDR > DICOM > Configuration**.
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 system 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 1).

For a device with a read-only access profile, ensure that there is content in the HP MAS system 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 (read-write R/W and read-only R/O) in the test plan.

Table 1 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.	✓	✓

Restore LDR to Service After Verification

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

1. Go to **SN2-A-1 > LDR > DICOM > Configuration**.
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 HP 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 C-ECHO service provided by the HP MAS system.

Preparation

Perform the steps in Test Setup (page 23) to prepare for the test.

Procedure

1. Go to **SN1-A-1 > LDR > DICOM > Overview**.
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. In the NMS MI, confirm that the number of “`Inbound C-Echoes - Successful`” has increased as expected.
6. After all tests are complete, ensure you perform the steps in Restore LDR to Service After Verification (page 25).

2: C-STORE SCU

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

Preparation

Perform the steps in Test Setup (page 23) to prepare for the test.

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

Procedure

1 Go to **SN1-A-1 > LDR > DICOM > Overview**.

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 In the NMS MI, confirm that the number of "`Inbound C-Stores - Successful`" has increased as expected.

5 After all tests are complete, ensure you perform the steps in Restore LDR to Service After Verification (page 25).

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

Perform the steps in Test Setup (page 23) to prepare for the test.

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

Procedure

1 Go to **SN1-A-1 > LDR > DICOM > Overview**.

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 In the NMS MI, 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.

7 After all tests are complete, ensure you perform the steps in Restore LDR to Service After Verification (page 25).

4: C-FIND SCU

This test verifies that the DICOM device supports using the DICOM C-FIND service provided by the HP MAS system.

Preparation

Perform the steps in Test Setup (page 23) to prepare for the test.

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

Procedure

1 Go to **SN1-A-1 > LDR > DICOM > Overview**.

1 Note the attribute value of "`Inbound C-Finds - Successful`".

2 Perform a query constrained by patient ID. Note the response from the device.

3 Perform a query constrained by modality. Note the response from the device.

4 Perform a query constrained by accession number. Note the response from the device.

5 Perform a query constrained by patient name. Note the response from the device.

6 In the NMS MI, confirm that the number of "`Inbound C-Finds - Successful`" has increased by five (5) as expected.

7 Perform a query constrained by any other metadata field as required. Note the response from the device.

8 Confirm that the DICOM device received the expected list of studies for each query performed.

9 After all tests are complete, ensure you perform the steps in Restore LDR to Service After Verification (page 25).

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 system. This test also verifies that the device provides a DICOM store service that the HP MAS system can use.

Preparation

Perform the steps in Test Setup (page 23) to prepare for the test.

Procedure

1 Go to **SN1-A-1 > LDR > DICOM > Overview**.

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. In the NMS MI, 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.
9. After all tests are complete, ensure you perform the steps in Restore LDR to Service After Verification (page 25).

A Grid Access for Client Applications

Access to the grid for external applications is configured in the NMS MI via the Grid Management > Grid configuration menu, using the Link Cost Groups, 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 an advanced capability. Review all documentation before beginning.

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.

Assuming a TCP/IP connection is permitted, the grid further restricts the caller to communicating with grid nodes that are in a specified group within the grid. (All grid nodes in a single geographic location are often assigned to a single group, but groups may also be used to recognize other logical partitions such as separate subnets or server racks.) After a TCP/IP connection is made, access to the grid is further restricted 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 collections of calling entities.

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.

HTTP Configuration

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

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:

- Go to **Grid Management > Grid Configuration > HTTP Advanced** and define a profile that outlines the activities that the entity is permitted to perform.
- Go to **Grid Management > Grid Configuration > HTTP** and assign an IP range to the activities’ permission profile.
- Go to **Grid Management > Grid Configuration > Link Cost Groups** and assign grid groups to the clients. The clients submit queries to the grid via these groups.

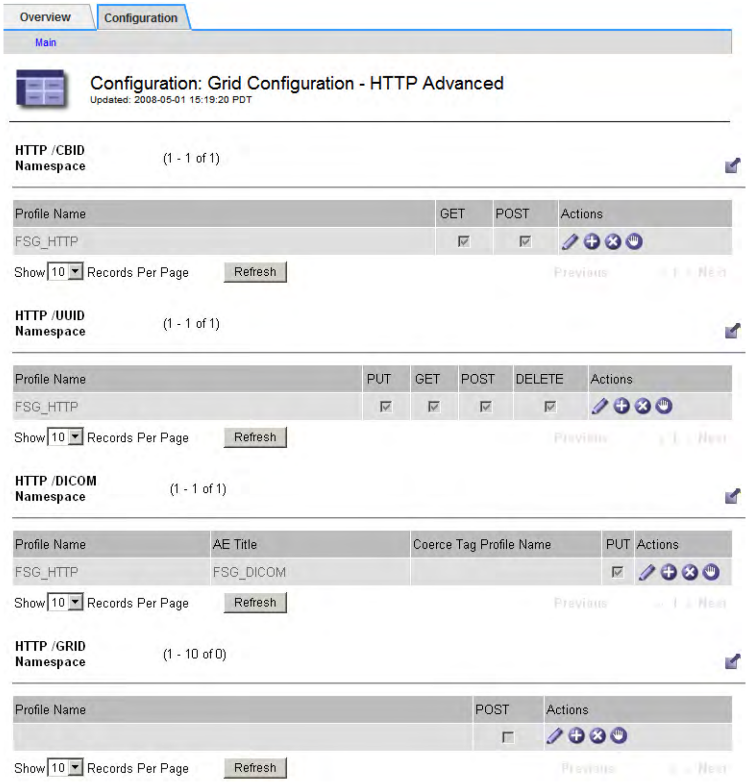
More information about each of these steps is described below.

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.



Configuration: Grid Configuration - HTTP Advanced
Updated: 2008-05-01 15:19:20 PDT

HTTP /CBID Namespace (1 - 1 of 1)

Profile Name	GET	POST	Actions
FSG_HTTP	☑	☑	

Show 10 Records Per Page Refresh

HTTP /UUID Namespace (1 - 1 of 1)

Profile Name	PUT	GET	POST	DELETE	Actions
FSG_HTTP	☑	☑	☑	☑	

Show 10 Records Per Page Refresh

HTTP /DICOM Namespace (1 - 1 of 1)

Profile Name	AE Title	Coerce Tag Profile Name	PUT	Actions
FSG_HTTP	FSG_DICOM		☑	

Show 10 Records Per Page Refresh

HTTP /GRID Namespace (1 - 10 of 0)

Profile Name	POST	Actions
	□	

Show 10 Records Per Page Refresh

Figure 3 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.

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.

- **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.
- **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. For more information, see DICOM Partitions (page 43). This field can be left blank if no partitioning is applied to entities with the profile.

/GRID Namespace

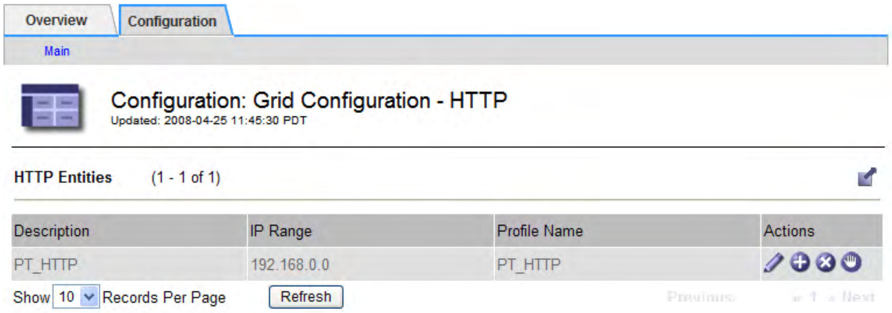
The GRID namespace is used to query the grid for information about nodes and the services they provide. The GRID namespace is used by custom applications developed to store or retrieve grid content via the UUID or DICOM namespaces. Enabling POST in the grid namespace is required to permit a custom application to store custom audit messages supplied by the application.

HTTP Metadata Indexing

This table lists the custom metadata defined for use with this grid via the HTTP API. For more information, contact HP Support.

HTTP Entities

Returning to the **Grid Management > Grid Configuration > HTTP** component, entities are now enabled to use HTTP by applying profiles to them.



Configuration: Grid Configuration - HTTP
Updated: 2008-04-25 11:45:30 PDT

HTTP Entities (1 - 1 of 1)

Description	IP Range	Profile Name	Actions
PT_HTTP	192.168.0.0	PT_HTTP	✎ ⊕ ⊗ ✋

Show 10 Records Per Page Refresh

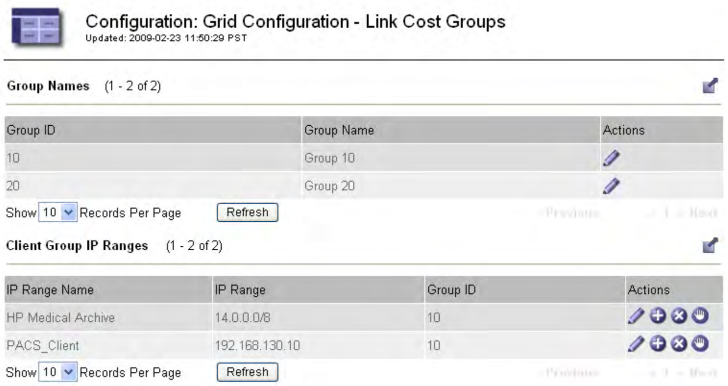
Figure 4 Sample HTTP Entities Configuration

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.

Client Group IP Ranges

Clients are then assigned to groups. 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 - Link Cost Groups
Updated: 2009-02-23 11:50:29 PST

Group Names (1 - 2 of 2)

Group ID	Group Name	Actions
10	Group 10	✎
20	Group 20	✎

Show 10 Records Per Page Refresh

Client Group IP Ranges (1 - 2 of 2)

IP Range Name	IP Range	Group ID	Actions
HP Medical Archive	14.0.0.0/8	10	✎ ⊕ ⊗ ✋
PACS_Client	192.168.130.10	10	✎ ⊕ ⊗ ✋

Show 10 Records Per Page Refresh

Figure 5 Sample IP Range Configuration

IP Ranges

IP Ranges are specified using one of the following:

- a single IP address

- a hyphenated list of IP addresses (for example, 174.182.91.00-174.182.91.64)
- a range of IP addresses specified using CIDR notation (for example, 192.168.120.0/27)

The following syntax for IP ranges is also supported to support legacy integrations. HP recommends that you use CIDR notation instead.

- IP ranges can be specified 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.

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 Client Group 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.

Assigning Groups to Client IP Ranges

To assign a group to an IP range:

1. Go to **Grid Management > Grid Configuration > Link Cost Groups > Configuration**.
2. Define a set of IP ranges for a group:
   - a In the Client Group 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.

If specifying a range, use one of:

- a hyphenated list of IP addresses (for example, 174.182.91.00-174.182.91.64)
- a range of IP addresses specified using CIDR notation (for example, 192.168.120.0/27)

For information on specifying an IP address in the form A.B.C.D, see IP Ranges (page 35).

d Enter a group ID for that IP range.

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.) 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 Click **Apply Changes**.

f Repeat for each IP range permitted to access the grid.

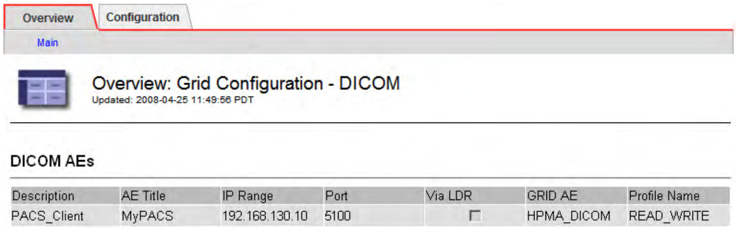
DICOM Configuration

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 is on the list of DICOM AEs in the Grid Management > Grid Configuration > DICOM component.



Overview: Grid Configuration - DICOM
Updated: 2008-04-25 11:49:56 PDT

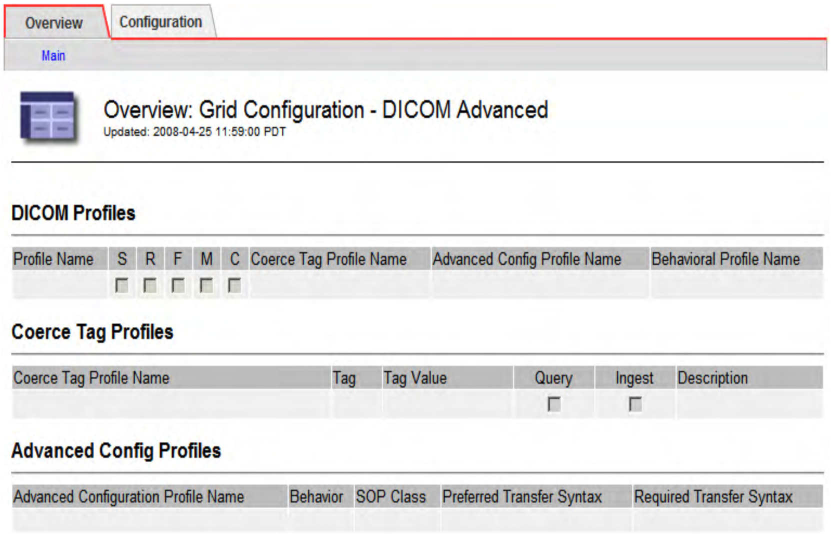
DICOM AEs

Description	AE Title	IP Range	Port	Via LDR	GRID AE	Profile Name
PACS_Client	MyPACS	192.168.130.10	5100	□	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.



Overview: Grid Configuration - DICOM Advanced
Updated: 2008-04-25 11:59:00 PDT

DICOM Profiles

Profile Name	S	R	F	M	C	Coerce Tag Profile Name	Advanced Config Profile Name	Behavioral Profile Name
	□	□	□	□	□			

Coerce Tag Profiles

Coerce Tag Profile Name	Tag	Tag Value	Query	Ingest	Description
			□	□	

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 (page 43).)

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 2 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. For more information, see DICOM Partitions (page 43).

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 or unsupported SOP storage classes that are not otherwise supported by the HP MAS system (as described in the *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 *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 *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.

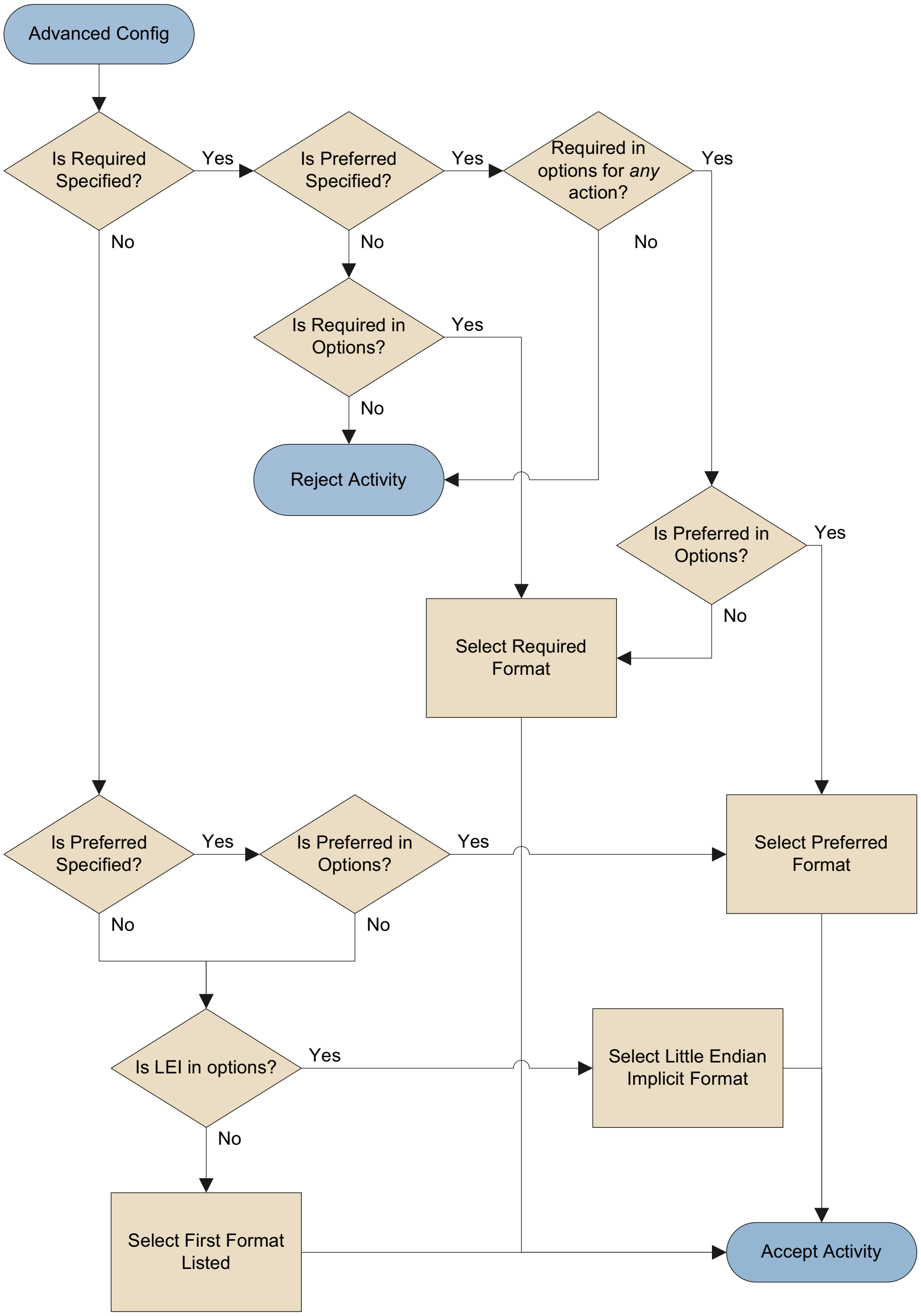


Figure 8 Advanced Configuration Flowchart

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 *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 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 HP 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 Go to **Grid Management > Grid Configuration > DICOM Advanced** and 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. Go to **Grid Management > Grid Configuration > Link Cost Groups** and assign grid groups to the clients. The clients submit queries to the grid via these groups.

3. Go to **Grid Management > Grid Configuration > DICOM** and specify which entities can access the grid, and assign the DICOM Profile and Grid AE title they use when doing so.

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. Go to **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 2 (page 39).

2. If an existing profile meets your needs, note its name, and go on to DICOM AE Titles (page 53).

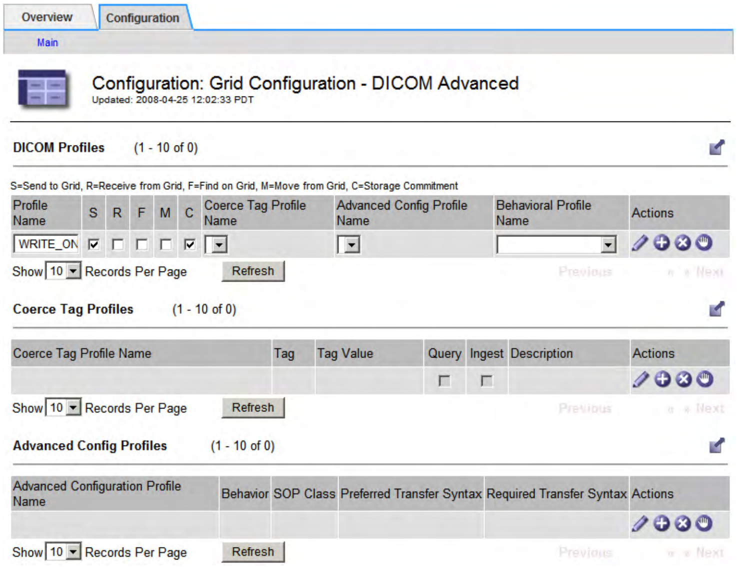
3. Otherwise, create a custom DICOM profile:

   a. Go to **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, enter: `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.



Configuration: Grid Configuration - DICOM Advanced
Updated: 2008-04-25 12:02:33 PDT

DICOM Profiles (1 - 10 of 0)

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
WRITE_ON	☑	□	□	□	☑				

Show 10 Records Per Page Refresh Previous « » Next

Coerce Tag Profiles (1 - 10 of 0)

Coerce Tag Profile Name	Tag	Tag Value	Query	Ingest	Description	Actions
			□	□		

Show 10 Records Per Page Refresh Previous « » Next

Advanced Config Profiles (1 - 10 of 0)

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

Show 10 Records Per Page Refresh Previous « » Next

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 (page 40).

g Click **Apply Changes**.

Next, assign groups to the IP addresses of the DICOM devices that will write to the grid.

Client Group IP Ranges

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 assign a group to an IP range:

1 Go to **Grid Management > Grid Configuration > Link Cost Groups > Configuration**.

2 Define a set of IP ranges for a group:

a In the Client Group 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).

If specifying a range, use one of:

- a hyphenated list of IP addresses (for example, 174.182.91.00-174.182.91.64)
- a range of IP addresses specified using CIDR notation (for example, 192.168.120.0/27)

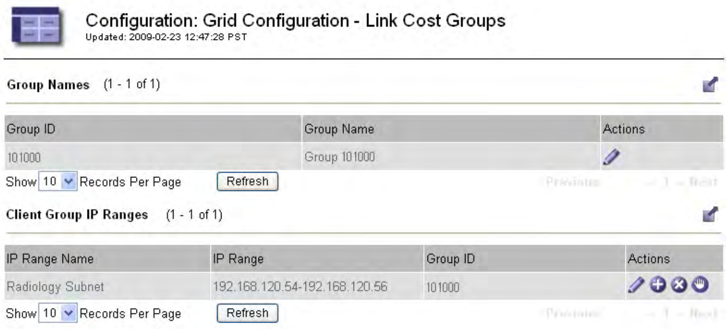
For information on specifying an IP address in the form A.B.C.D, see IP Ranges (page 35).

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 Click **Apply Changes**.



Configuration: Grid Configuration - Link Cost Groups
Updated: 2009-02-23 12:47:28 PST

Group Names (1 - 1 of 1)

Group ID	Group Name	Actions
101000	Group 101000	✎

Show 10 Records Per Page Refresh Previous 1 Next

Client Group IP Ranges (1 - 1 of 1)

IP Range Name	IP Range	Group ID	Actions
Radiology Subnet	192.168.120.54-192.168.120.56	101000	✎ ⊕ ⊗ ✋

Show 10 Records Per Page Refresh Previous 1 Next

Figure 10 Client Group IP Ranges

f Repeat for each IP range permitted to access the grid.

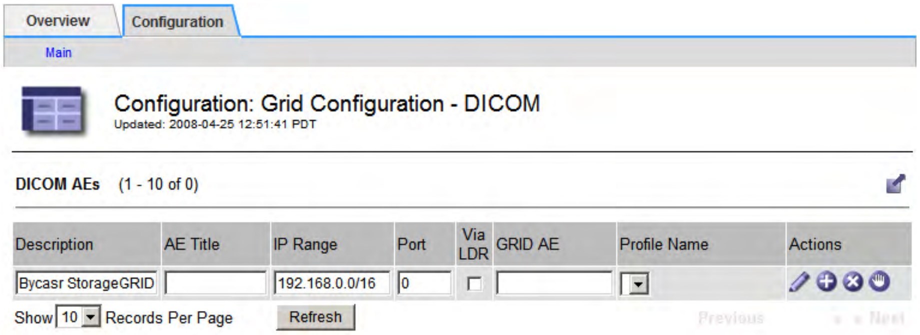
Next enter the DICOM AE Titles for devices that are to be given grid access using one of the defined DICOM Profiles.

DICOM AE Titles

After you have created the DICOM Configuration Profile using **Grid Management > Grid Configuration > DICOM Advanced**, and have given permission for entities with the appropriate IP addresses to access the grid via specified groups, define the DICOM AE Titles of the remote entities that are permitted to access the grid.

1 Go to **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	□			

Show 10 Records Per Page

Figure 11 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, enter: **`MRI Clinic`**

4 Enter the AE Title assigned to the remote DICOM entity. AE Titles are case-sensitive. In this example, enter: **`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 range of IP addresses (for example, 174.182.91.00-174.182.91.64)

— a range of IP addresses specified using CIDR notation (for example, 192.168.120.0/27)

For information on specifying an IP address in the form A.B.C.D, see IP Ranges (page 35).

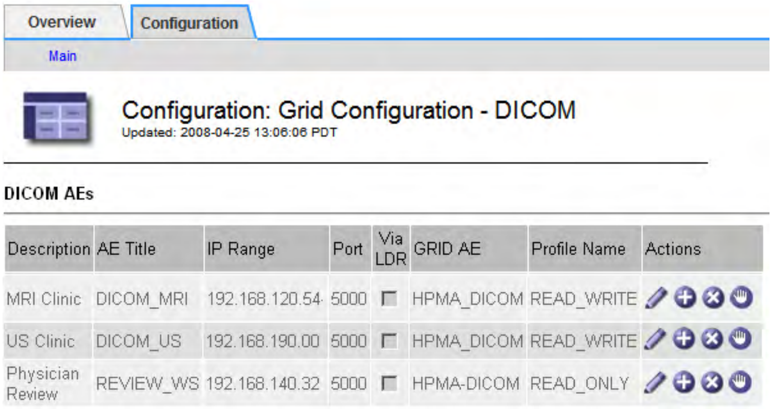
In this example, enter: **`192.168.120.54`**

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 Enter the GRID AE title.



Configuration: Grid Configuration - DICOM

Updated: 2008-04-25 13:06:06 PDT

DICOM AEs

Description	AE Title	IP Range	Port	Via LDR	GRID AE	Profile Name	Actions
MRI Clinic	DICOM_MRI	192.168.120.54·	5000	□	HPMA_DICOM	READ_WRITE	✎ ⊕ ⊗ ✋
US Clinic	DICOM_US	192.168.190.00	5000	□	HPMA_DICOM	READ_WRITE	✎ ⊕ ⊗ ✋
Physician Review	REVIEW_WS	192.168.140.32	5000	□	HPMA-DICOM	READ_ONLY	✎ ⊕ ⊗ ✋

Figure 12 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 (page 45). 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**.

Once you have assigned DICOM profiles to the DICOM AEs, 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 (page 40).

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. Go to **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.

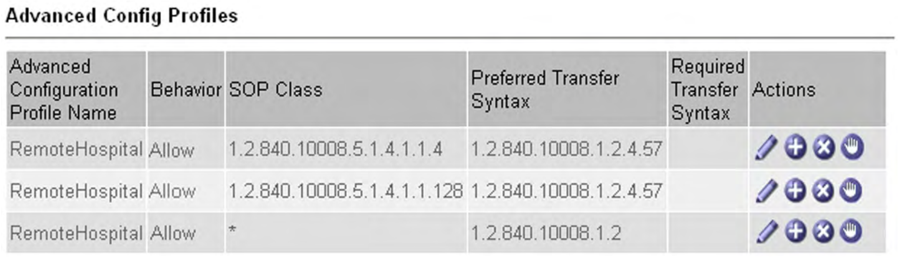
a In the Advanced Config Profiles table, click **Add** ⊕ to add a new entry.

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

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 or unsupported SOP class that is not otherwise supported by the grid (according to its *DICOM Conformance Statement*).

1 Go to **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 (page 50).

1 Go to **Grid Management > Grid Configuration > DICOM Advanced > Configuration > Main**.

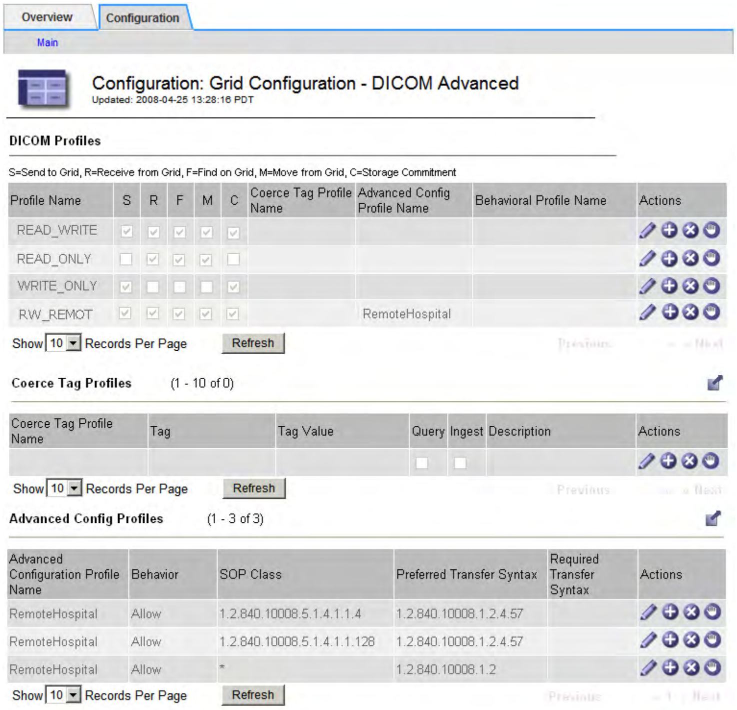
2 In the DICOM Profiles table, **Edit** ✎ (if this is the first entry) or **Add** ⊕ to add a new entry.

3 Type a meaningful Profile Name. For this example, enter: `RW_REMOT`

4 Select the DICOM options needed for the entity. In this example, all activities are permitted. For more information on options, see Table 2, Permission options for DICOM Profiles.

5 For the Advanced Config Profile Name, enter: `RemoteHospital`

6 Click **Apply Changes**.



Configuration: Grid Configuration - DICOM Advanced
Updated: 2008-04-25 13:28:16 PDT

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	☑	☑	☑	☑	☑				✎ ⊕ ⊗ ✋
READ_ONLY	□	☑	☑	☑	□				✎ ⊕ ⊗ ✋
WRITE_ONLY	☑	□	□	□	☑				✎ ⊕ ⊗ ✋
RW_REMOT	☑	☑	☑	☑	☑		RemoteHospital		✎ ⊕ ⊗ ✋

Show 10 Records Per Page Refresh Previous Next

Coerce Tag Profiles (1 - 10 of 0)

Coerce Tag Profile Name	Tag	Tag Value	Query	Ingest	Description	Actions
			□	□		✎ ⊕ ⊗ ✋

Show 10 Records Per Page Refresh Previous Next

Advanced Config Profiles (1 - 3 of 3)

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		✎ ⊕ ⊗ ✋

Show 10 Records Per Page Refresh Previous 1 Next

Figure 14 DICOM Advanced

Next, assign groups to the IP addresses of the DICOM devices that will access the grid.

Client Group IP Ranges

This procedure assigns groups to the IP addresses allowed 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.

1. Go to **Grid Management > Grid Configuration > Link Cost Groups > Configuration**.
2. Define a set of IP ranges for a group:

   a. In the Client Group IP Ranges table, click **Add** ⊕ to add a new IP range.

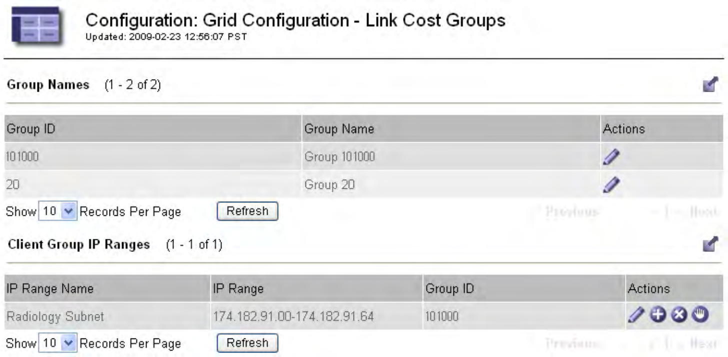
   b. Enter the IP Range Name. In this example, enter: **`Radiology Subnet`**

   c. Enter the IP Range (or IP address). 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. Click **Apply Changes**.



Configuration: Grid Configuration - Link Cost Groups
Updated: 2009-02-23 12:56:07 PST

Group Names (1 - 2 of 2)

Group ID	Group Name	Actions
101000	Group 101000	✎
20	Group 20	✎

Client Group IP Ranges (1 - 1 of 1)

IP Range Name	IP Range	Group ID	Actions
Radiology Subnet	174.182.91.00-174.182.91.64	101000	✎ ⊕ ⊗

Figure 15 Client Group IP Ranges

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.

1. Go to **Grid Management > Grid Configuration > DICOM > Configuration > Main**.

2 Click **Edit** ✎ (if this is the first entry) or **Add** ⊕ to add the DICOM AE for the remote entity.

3 Enter a Description of the DICOM device you are granting access to. In this example, enter: **`CT at Hospital X`**

4 Enter the case-sensitive AE Title of the remote entity. In this example, enter: **`CT_HOSX`**

5 Enter the IP Range (or IP address) that the device can connect from. In this example, enter: **`174.182.91.00`**

6 Enter the Port that the remote DICOM device uses to listen for connections from the grid. In this example, enter: 5000

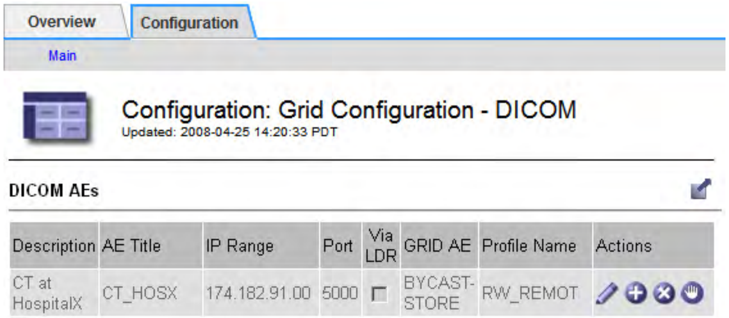
7 Do not select Via LDR.

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**.



Configuration: Grid Configuration - DICOM
Updated: 2008-04-25 14:20:33 PDT

DICOM AEs

Description	AE Title	IP Range	Port	Via LDR	GRID AE	Profile Name	Actions
CT at HospitalX	CT_HOSX	174.182.91.00	5000	□	BYCAST-STORE	RW_REMOT	✎ ⊕ ⊗

Figure 16 Grid Management > Grid Configuration > DICOM

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 Go to **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)`**

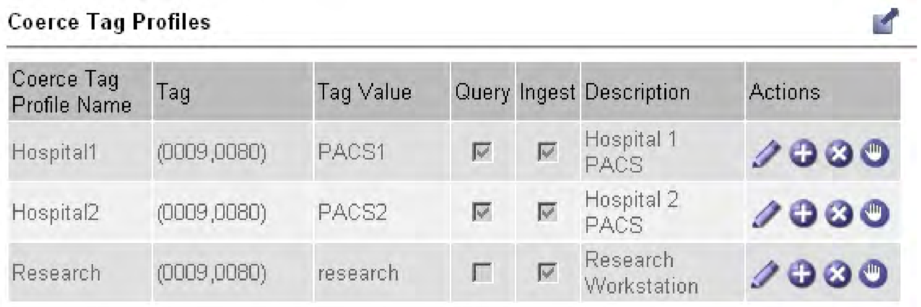
5 Enter a Tag Value. For example, enter: **`PACS1`**

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	☑	☑	Hospital 1 PACS	✎ ⊕ ⊗ ✋
Hospital2	(0009,0080)	PACS2	☑	☑	Hospital 2 PACS	✎ ⊕ ⊗ ✋
Research	(0009,0080)	research	□	☑	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

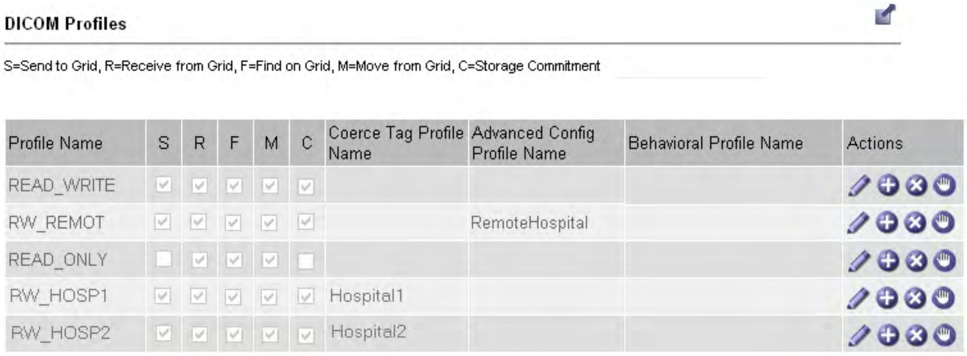
Ingest only selected

- 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 (page 45) 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	☑	☑	☑	☑	☑				✎ ⊕ ⊗ ✋
RW_REMOT	☑	☑	☑	☑	☑		RemoteHospital		✎ ⊕ ⊗ ✋
READ_ONLY	□	☑	☑	☑	□				✎ ⊕ ⊗ ✋
RW_HOSP1	☑	☑	☑	☑	☑	Hospital1			✎ ⊕ ⊗ ✋
RW_HOSP2	☑	☑	☑	☑	☑	Hospital2			✎ ⊕ ⊗ ✋

Figure 18 DICOM Profiles

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

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.

B DICOM Device Test Report

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

	Y	N
The HP MAS system successfully received the study.	□	□
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.	□	□
The DICOM device successfully received a storage commitment response.	□	□
The number of “Inbound Storage Commitments - Successful” increased as expected.	□	□

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.	□	□
The number of “Inbound C-Finds - Successful” increased as expected.	□	□

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.	□	□
The number of “Inbound C-Moves - Successful” increased as expected.	□	□
The number of “Outbound C-Stores - Successful” increased as expected.	□	□

Test Result (PASS/FAIL): □

C Grid Specification Files and Provisioning

Introduction

This appendix provides an introduction to:

- provisioning
- the SAID package
- grid specification files

It also contains procedures to:

- display grid specification files
- edit grid specification files for deployment at installation
- edit grid specification files for maintenance procedures
- provision the grid following changes to the grid specification file
- change the provisioning passphrase

Provisioning is the process of turning a grid design into the collection of files needed to create, expand, maintain, or upgrade the grid. That collection of files, referred to as the gpt (grid provisioning tool) repository, includes the SAID package.

The key input for provisioning is the grid specification file.

About the SAID Package

The Software Activation and Integration Data (SAID) package contains site-specific files for the grid. It is generated during the provisioning process and saved to the Provisioning USB flash drive as a zip file named `GID<grid_ID>_REV<revision_number>_SAID.zip`, for example, `GID1234_REV1_SAID.zip`. The SAID package contains the following:

Table 3 SAID Package Contents

Item	Description
Doc directory	Contains html files used to confirm provisioning.
Escrow_Keys directory	Encryption keys used by the data recovery tool.
Grid_Activation directory	Contains activation files, one for each server. Activation files are named `<`*`servername`*`>-autoinst.xml`. Activation files are keyed to work with the customer's hardware and a specific release of the HP MAS software.
Grid_Tasks directory	Contains files created by some types of changes to the grid specification file, such as adding a server or converting the grid to use metadata replication. Grid tasks are used to trigger various actions within the grid that are required to implement the specified changes to the grid.
Configuration.txt	Lists grid-wide configuration and integration data generated during the provisioning process.
Grid specification file	XML file that encapsulates the grid design. File name is `GID<`*`grid_ID`*`>_REV<`*`revision_number`*`>_GSPEC.xml`
Passwords.txt	Passwords used to access the grid.
Router_Configs	Contains files to configure the grid's network routers. This folder is empty if the deployment is a Single Site with only the Base Cabinet.

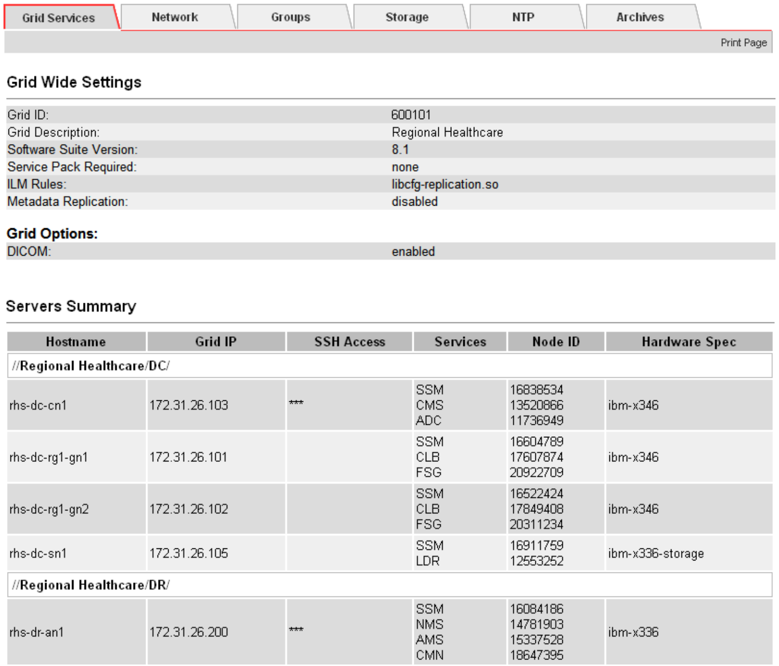
NOTE The SAID package contains highly confidential passwords and encryption keys. Only trained and authorized service personnel should have access to the `Passwords.txt` file.

Grid Configuration Files

The Doc directory of the SAID package contains html files documenting the configuration of the grid. Use these pages to confirm that the grid configuration is correct and complete.

To open the configuration pages:

- Click the `index.html` file. See Figure 19 for an example.



Grid Wide Settings

Grid ID:	600101
Grid Description:	Regional Healthcare
Software Suite Version:	8.1
Service Pack Required:	none
ILM Rules:	libcfg-replication.so
Metadata Replication:	disabled

Grid Options:

DICOM:	enabled

Servers Summary

Hostname	Grid IP	SSH Access	Services	Node ID	Hardware Spec
//**Regional Healthcare**/DC/					
rhs-dc-cn1	172.31.26.103	***	SSM CMS ADC	16838534 13520866 11736949	ibm-x346
rhs-dc-rg1-gn1	172.31.26.101		SSM CLB FSG	16604789 17607874 20922709	ibm-x346
rhs-dc-rg1-gn2	172.31.26.102		SSM CLB FSG	16522424 17849408 20311234	ibm-x346
rhs-dc-sn1	172.31.26.105		SSM LDR	16911759 12553252	ibm-x336-storage
//**Regional Healthcare**/DR/					
rhs-dr-an1	172.31.26.200	***	SSM NMS AMS CMN	16084186 14781903 15337528 18647395	ibm-x336

Figure 19 Index.html File

About Grid Specification Files

The grid specification file specifies grid topology, grid configuration, and networking. The grid specification file goes through a number of stages as the grid is designed and then installed:

- **Default grid specification file**—The default grid specification file describes the basic grid topology and grid configuration.
- **Deployment grid specification file**—The deployment grid specification file is created from the default grid specification file by replacing all factory-default values by customer-specific data, for example IP addresses.
- **Provisioned grid specification file**—The provisioned grid specification file is created when the provision command is run.

These stages are summarized in Figure 20.

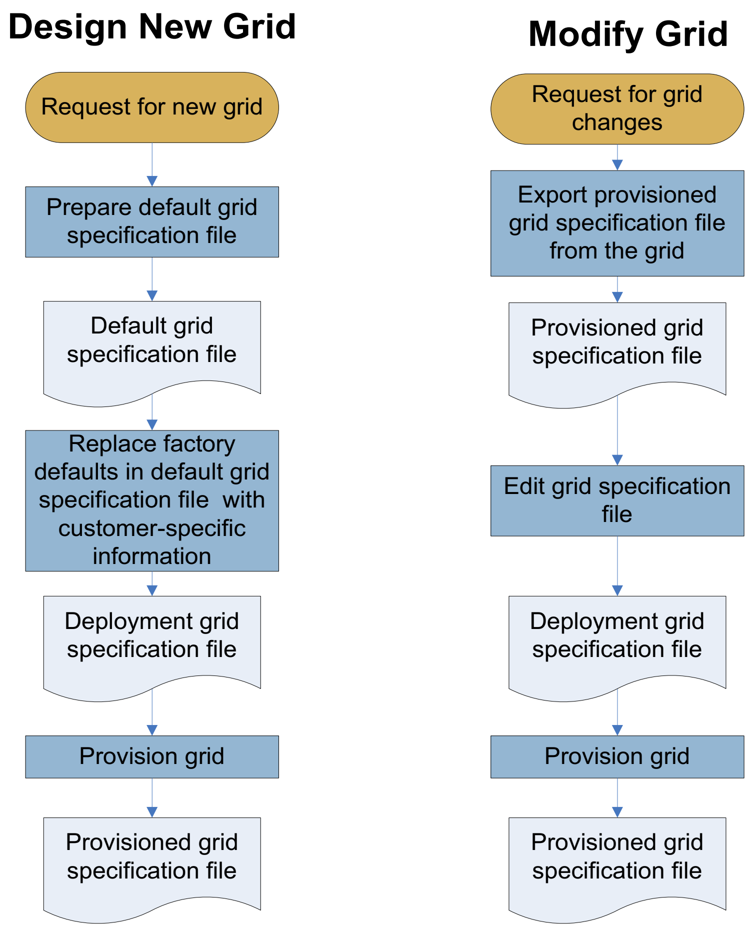

Design New Grid
Request for new grid
Prepare default grid specification file
Default grid specification file
Replace factory defaults in default grid specification file with customer-specific information
Deployment grid specification file
Provision grid
Provisioned grid specification file
Modify Grid
Request for grid changes
Export provisioned grid specification file from the grid
Provisioned grid specification file
Edit grid specification file
Deployment grid specification file
Provision grid
Provisioned grid specification file

Figure 20 Editing the Grid Specification File

Naming Convention

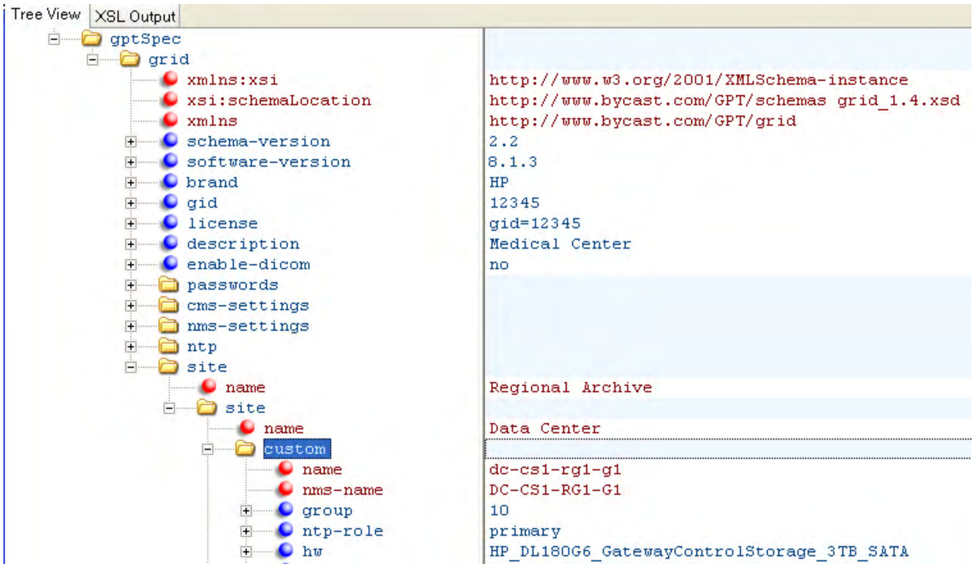
Grid specification files use the naming convention `GID`*`<grid_ID>`*`_REV`*`<revision_number>`*`_GSPEC.xml`, where *`<grid_ID>`* refers to the grid's unique identifier and *`<revision_number>`* refers to the revision number of the grid specification file, for example, `GID1234_REV1_GSPEC.xml`.

The default grid specification file has a *`<revision_number>`* of zero (REV0). The revision number is increased by 1 each time the grid specification file is modified, for example to add servers, change IP addresses, or refresh hardware.

For the initial installation of the grid, the revision number must be 1 (REV1). Any other revision number will cause provisioning to fail.

Grid Specification File Structure

The grid specification file is an XML file that encapsulates the grid design. See Figure 21 for an example. The file includes all the details about topology, servers, networking, and options for the grid.



```
gptSpec
  grid
    xmlns:xsi               http://www.w3.org/2001/XMLSchema-instance
    xsi:schemaLocation      http://www.bycast.com/GPT/schemas grid_1.4.xsd
    xmlns                   http://www.bycast.com/GPT/grid
    schema-version          2.2
    software-version        8.1.3
    brand                   HP
    gid                     12345
    license                 gid=12345
    description             Medical Center
    enable-dicom            no
    passwords
    cms-settings
    nms-settings
    ntp
    site
      name                  Regional Archive
      site
        name                Data Center
        custom
          name              dc-cs1-rg1-g1
          nms-name          DC-CS1-RG1-G1
          group             10
          ntp-role          primary
          hw                HP_DL180G6_GatewayControlStorage_3TB_SATA
```

Figure 21 Grid Specification File in XML Notepad 2007

Server Names

When editing the grid specification file manually, you must ensure that you select the right server. Table 4 lists the server tags. In addition, check the server name (`gptSpec>site>site>`*`server`*`>name`) to confirm that you are using the correct server.

Table 4 Server Tags

Server	XML Tag
Admin Node	admin
Gateway Node	gateway
Control Node	control
Storage Node	storage
Control/Storage Node	control-storage
Tape Node	archive
Combined Gateway/Control/Storage Node	two-server-primary
Combined Admin/Gateway/Control/ Storage Node	two-server-secondary
Server with other combinations of grid nodes	custom

Tags

Table 5 lists the XML tags of the attributes most likely to be updated.

Table 5 Common Changes to Grid Specification Files

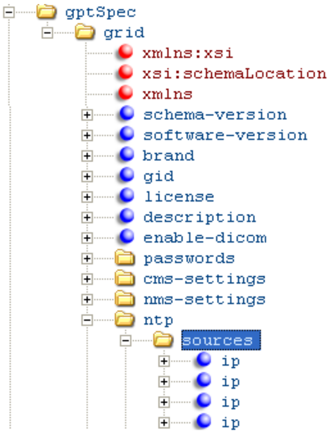
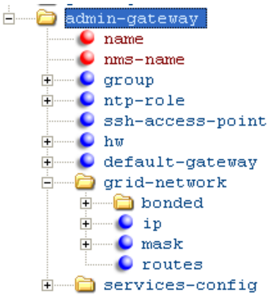
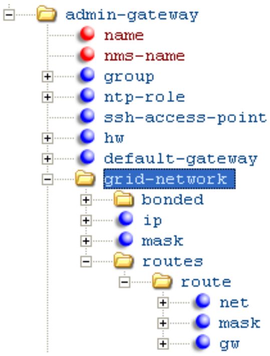
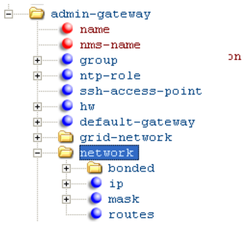
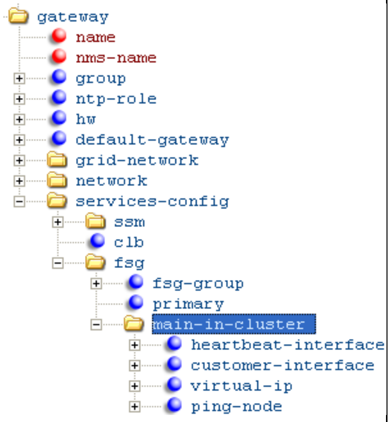
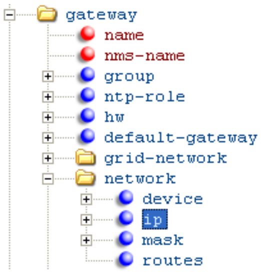
Settings	XML Tag	Notes
External NTP time sources  gptSpec grid xmlns:xsi xsi:schemaLocation xmlns schema-version software-version brand gid license description enable-dicom passwords cms-settings nms-settings ntp sources ip ip ip ip	gptSpec>grid>ntp>sources> ip	To provide a stable time source, specify four NTP time servers. External time sources must use the NTP protocol and not the SNTP protocol. In particular, do not use the Windows Time Service: it does not provide enough synchronization accuracy because it uses SNTP.
Networking information in a grid that does not have a private network  admin-gateway name nms-name group ntp-role ssh-access-point hw default-gateway grid-network bonded ip mask routes services-config	gptSpec>grid>site>site> *server*>default-gateway	
	gptSpec>grid>site>site> *server*>grid-network>ip	
	gptSpec>grid>site>site> *server*>grid-network>mask	
	gptSpec>grid>site>site> *server*>grid-network>routes	
Networking information for grid communication in grid with a private network  admin-gateway name nms-name group ntp-role ssh-access-point hw default-gateway grid-network bonded ip mask routes route net mask gw	gptSpec>grid>site>site> *server*>default-gateway	
	gptSpec>grid>site>site> *server*>grid-network>ip	
	gptSpec>grid>site>site> *server*>grid-network>mask	
	gptSpec>grid>site>site> *server*>grid-network>routes	

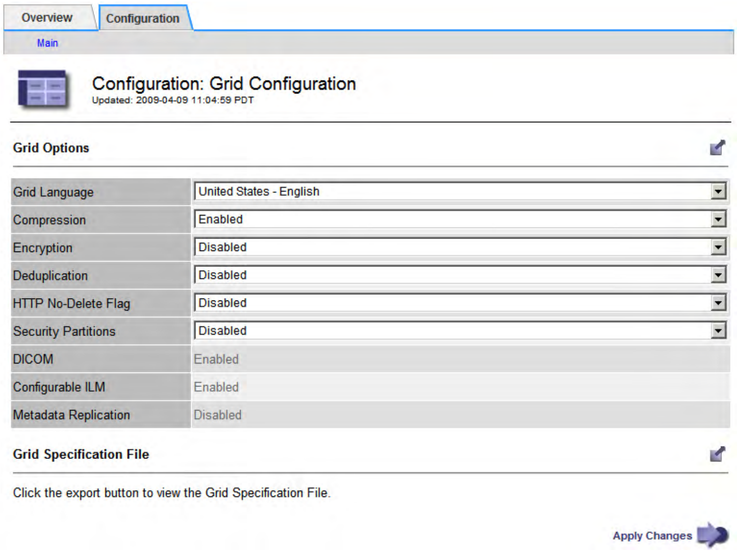
Table 5 Common Changes to Grid Specification Files *(continued)*

Settings	XML Tag	Notes
Networking information for client access in a grid with a private network  admin-gateway name nms-name group ntp-role ssh-access-point hw default-gateway grid-network network bonded ip mask routes	gptSpec>grid>site>site>*server*>default-gateway	Servers that have client-side IP addresses are Admin Nodes, Gateway Nodes, and Tape Nodes.
	gptSpec>grid>site>site>*server*>network>ip	
	server>grid>site>site>*server*>network>mask	
	gptSpec>grid>site>site>*server*>network>routes	
Virtual IP address of Gateway Node cluster  gateway name nms-name group ntp-role hw default-gateway grid-network network services-config ssm clb fsg fsg-group primary main-in-cluster heartbeat-interface customer-interface virtual-ip ping-node	gptSpec>grid>site>site>gateway>services-config>fsg>main-in-cluster>virtual-ip	Virtual IP addresses are used with high availability and DFSG clusters.
Heartbeat IP addresses  gateway name nms-name group ntp-role hw default-gateway grid-network network device ip mask routes	gptSpec>grid>site>site>gateway>network>ip	Heartbeat IP addresses are only used with high availability gateway clusters. They do not need to be modified unless they conflict with another network. If necessary, substitute the 10.1.1.x network with another unused non?routeable network.

View Grid Specification Files

Follow this procedure if you need to check quickly the grid specification file. If you need to edit the file, use the procedure in Export the Latest Grid Specification File (page 72) instead.

1 In the NMS MI, go to **Grid Management > Grid Configuration > Configuration**.



Configuration: Grid Configuration
Updated: 2009-04-09 11:04:59 PDT

Grid Options

Grid Language	United States - English
Compression	Enabled
Encryption	Disabled
Deduplication	Disabled
HTTP No-Delete Flag	Disabled
Security Partitions	Disabled
DICOM	Enabled
Configurable ILM	Enabled
Metadata Replication	Disabled

Grid Specification File

Click the export button to view the Grid Specification File.

Export Grid Specification File

Figure 22 Exporting the Grid Specification File

2 Click **Export** at the bottom of the page, next to Grid Specification File. A new browser window opens, showing the grid specification file in raw XML.

Export the Latest Grid Specification File

Follow this procedure to retrieve a copy of the current grid specification file in order to modify it.

Prerequisites and required materials

- USB flash drive
- Passwords.txt file

Procedure

1 At the primary Admin Node server, press **<Alt>+<F1>** to access a command shell and log in as `root` using the password listed in the `Passwords.txt` file.

2 Insert a USB flash drive.

3 Copy the provisioned grid specification file to the USB flash drive. Enter: **`copy-grid-spec`**

4 Log out. Enter: **`exit`**

Manually Edit the Grid Specification File for Deployment

Before you can install a grid, you need to customize the grid specification file by entering networking information specific to the particular installation, for example, IP addresses.

This step is not necessary if you are recovering a failed grid node and replacing the server with hardware that is different than the original server.

Prerequisites and required materials

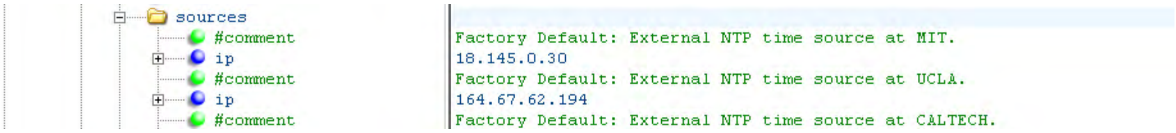
- Default grid specification file
- Microsoft XML Notepad

To edit the grid specification file manually:

1 With XML Notepad 2007, open the default grid specification file.

2 Update the file with installation-specific information, for example, network settings. See Table 5 for a list of the XML tags that are most likely to be updated.

The best way to work through the default grid specification file is to search for all comments Factory Default, update these default settings as needed, and then delete the Factory Default comment. Continue until there are no Factory Default comments remaining.



```
sources
  #comment    Factory Default: External NTP time source at MIT.
  ip          18.145.0.30
  #comment    Factory Default: External NTP time source at UCLA.
  ip          164.67.62.194
  #comment    Factory Default: External NTP time source at CALTECH.
```

Figure 23 Sample Factory Default Comment

3 Save the default grid specification file as revision 1 of the deployment grid specification file. Use the following naming convention:

`GID<`*`grid_ID`*`>_REV<`*`revision_number`*`>_GSPEC.xml`

For the initial installation of the grid, <*revision_number*> must be 1 (REV1). For example: `GID1234_REV1_GSPEC.xml`

NOTE Provisioning will fail if `REV<`*`revision_number`*`>` is incorrect.

Edit IP Addresses in Grid Specification Files

You need to edit the grid specification file if you have to update server IP addresses such as:

- external NTP sources IP address
- customer network IP address
- grid network IP address
- virtual IP address in Gateway Node clusters
- routing

Edit Grid Specification Files Manually

Use this procedure to edit grid specification files.

Prerequisites and required materials

- Latest provisioned grid specification file, see Export the Latest Grid Specification File (page 72)
- Microsoft XML Notepad

Procedure

1. Open the grid specification file in XML Notepad.
2. Locate the server for which you need to change settings. See the list of server tags in Table 4 (page 69).

   NOTE Make sure that you select the correct server. Use the server name to confirm.

3. Edit the required settings. See the list of settings commonly changed in Table 5 (page 70).
4. Save the grid specification file using the following file naming convention, incrementing the revision number by one:
   `GID<`*`grid_ID`*`>_REV<`*`number`*`>_GSPEC.xml`

Provision the Grid

Use this procedure to implement the changes made to the grid specification file. The provisioning script imports the updated grid specification file into the grid and generates any grid tasks required to complete the implementation of the changes.

Prerequisites and required materials

- Deployment grid specification file, see Export the Latest Grid Specification File (page 72)
- Provisioning USB flash drive
- Backup Provisioning USB flash drive
- Passwords.txt file
- Provisioning passphrase

Procedure

1. Copy the edited grid specification file to the root level of the Provisioning USB flash drive.
2. Remove the old grid specification file from the root level of the Provisioning USB flash drive.
3. Verify that the Provisioning USB flash drive contains only one grid specification file at the root level, that is, there is only one file named `GID<grid_ID>_REV<revision_number>_GSPEC.xml`.

△ CAUTION The Provisioning USB flash drive must contain only one grid specification file at the root level. Provisioning will fail otherwise.

4. Run the provisioning script:
   a. At the primary Admin Node server, press **<Alt>+<F1>** to access a command shell and log in as `root` using the password listed in the `Passwords.txt` file.
   b. Run the provisioning script. Enter: **`provision`**
   c. When prompted, insert the Provisioning USB flash drive.
   d. When prompted, enter the provisioning passphrase.
   e. When provisioning is complete, remove the Provisioning USB flash drive.

NOTE If provisioning ends with an error message, see Provisioning Troubleshooting (page 78).

5. Back up the provisioning data:
   a. Insert the Backup Provisioning USB flash drive.

b Enter: **`backup-to-usb-key`**

c When prompted, enter the provisioning passphrase.

6 When backup is complete, remove the Backup Provisioning USB flash drive.

7 Review the current configuration to confirm all settings are correct:

a Copy the file `GID<`*`grid_ID`*`>_REV<`*`number`*`>_SAID.zip` on the USB Provisioning flash drive to the service laptop and extract the contents.

b Inspect the file `Index.html` to make sure that the settings are correct. If there is an error, you need to provision the grid again. For more information, see Errors in Grid Specification File (page 79).

8 Store the Provisioning USB flash drive and the Backup Provisioning USB flash drive separately in safe locations.

⚠ WARNING! Store the Provisioning USB flash drive and the Backup Provisioning USB flash drive separately in safe secure locations such as a locked cabinet or safe.
The Provisioning USB is required to recover from a primary Admin Node failure.
The USB flash drives contain encryption keys and passwords that can be used to obtain data from the grid.

Change the Provisioning Passphrase

Use this procedure to update the provisioning passphrase. The provisioning passphrase is used to encrypt the gpt repository. It is created when the grid is first installed and is required for software upgrades, grid expansions, and many maintenance procedures.

⚠ WARNING! The provisioning passphrase is required for many installation and maintenance procedures. The provisioning passphrase is not listed in the Passwords.txt file. Make sure that it is documented and kept in a safe location.

Prerequisites and required materials

- Provisioning USB flash drive
- Backup Provisioning USB flash drive
- Passwords.txt file
- Current provisioning passphrase
- New provisioning passphrase

Procedure

1. At the primary Admin Node server, press **<Alt>+<F1>** to access a command shell and log in as `root` using the password listed in the Passwords.txt file.
2. Change the passphrase:
   a. Enter: **`change-repository-password`**
   b. When prompted, enter the old passphrase.
   c. When prompted, enter the new passphrase. It must be at least six characters.
   d. When prompted, enter the passphrase again.
3. Remove the Provisioning USB flash drive and store in a safe place.
4. When prompted, insert the Backup Provisioning USB flash drive.
5. When backup is complete, remove the Backup Provisioning USB flash drive and store it in a safe place.
6. Close the command shell. Enter: **`exit`**
7. Write down the provisioning passphrase for future reference.

⚠ WARNING! Store the Provisioning USB flash drive and the Backup Provisioning USB flash drive separately in safe secure locations such as a locked cabinet or safe.
The Provisioning USB is required to recover from a primary Admin Node failure.
The USB flash drives contain encryption keys and passwords that can be used to obtain data from the grid.

Provisioning Troubleshooting

In case of provisioning errors, follow these guidelines:

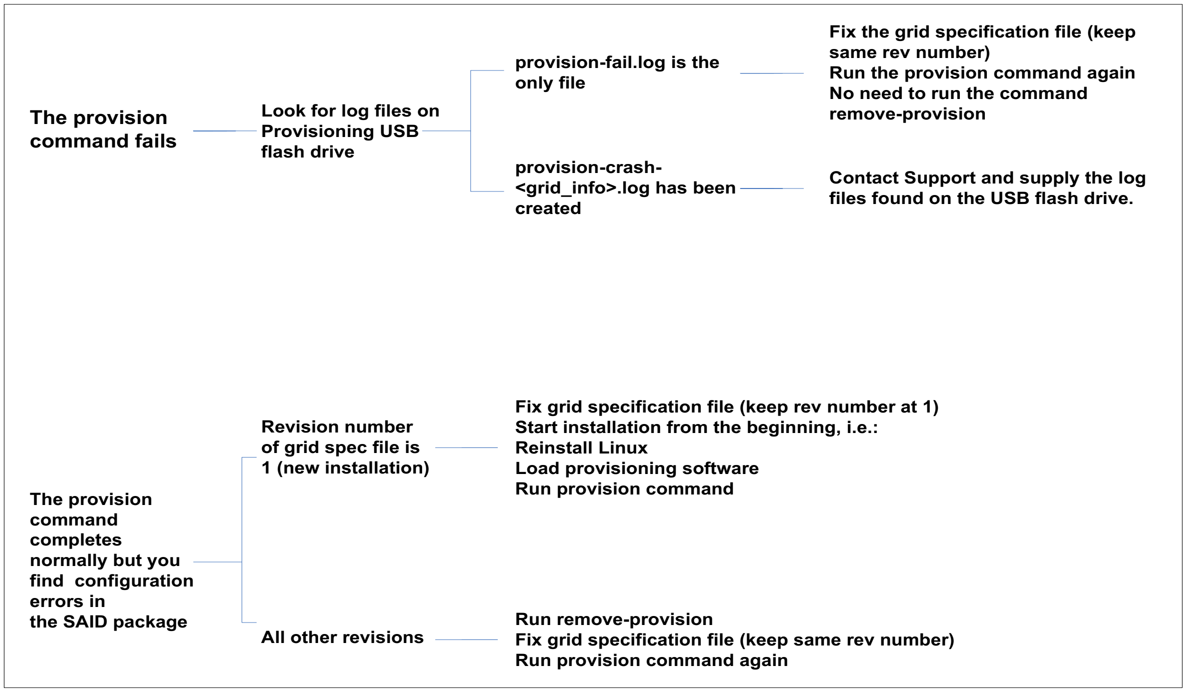

The provision command fails
Look for log files on Provisioning USB flash drive
provision-fail.log is the only file
Fix the grid specification file (keep same rev number)
Run the provision command again
No need to run the command remove-provision
provision-crash-<grid_info>.log has been created
Contact Support and supply the log files found on the USB flash drive.
The provision command completes normally but you find configuration errors in the SAID package
Revision number of grid spec file is 1 (new installation)
Fix grid specification file (keep rev number at 1)
Start installation from the beginning, i.e.:
Reinstall Linux
Load provisioning software
Run provision command
All other revisions
Run remove-provision
Fix grid specification file (keep same rev number)
Run provision command again

Figure 24 Troubleshooting Provisioning Errors

Provision Command Fails

If provisioning fails because the grid specification file is incorrect, the file `provision-fail.log` is created on the Provisioning USB flash drive. This file contains the error message that the provisioning software displayed before terminating.

If the provisioning program terminates abnormally (crash), two identical log files are saved to the Provisioning USB flash drive:

- `provision-fail.log`
- `provision-crash-<`*`grid_info`*`>.log`

Where <*grid_info*> includes the grid ID, the grid revision being created and a timestamp.

If the `provision-fail.log` file is the only file created, fix the grid specification file and run provisioning again. If the `provision-crash-<grid_info>.log` file is created, contact HP support.

If provisioning ends with an error, no information is saved and the `remove-revision` command does not need to be run

Errors in Grid Specification File

If the provision command completes normally but you discover an error in the provisioning data after examining the configuration pages in the SAID package, you need to fix the grid specification file and reprovision the grid.

Initial Installation

NOTE Follow this procedure if the revision number of the grid specification file is 1.

If during the initial installation you discover errors in the SAID package, you must fix the grid specification file and reinstall the primary Admin Node from the beginning, that is, you must reinstall Linux, load provisioning software, and provision the grid.

Upgrades, Expansion, and Maintenance Procedures

NOTE Follow this procedure if the revision number of the grid specification file is greater than 1. This procedure cannot be used for a new installation.

1 Confirm that no scripts or grid tasks generated by provisioning have been started.

⚠ WARNING! Do not use this procedure if you have started any scripts or grid tasks that were generated by provisioning. Contact HP support for assistance.

2 Remove the provisioning data from the grid. Enter: **`remove-revision`**

3 When prompted, enter the provisioning passphrase.

4 Cancel any pending grid tasks created by the provisioning.

5 Fix the deployment grid specification file and save it to the root directory of the Provisioning USB flash drive. Do not change the `REV<revision_number>`.

△ CAUTION The Provisioning USB flash drive must contain only one grid specification file at the root level. Provisioning will fail otherwise.

6 Run provisioning again and generate a new SAID package. For more information, see Provision the Grid (page 75). The old SAID package is overwritten and a new one is generated that uses the same naming convention.

7 Review the contents of the SAID package to confirm that the provisioning information is correct.

D Connectivity

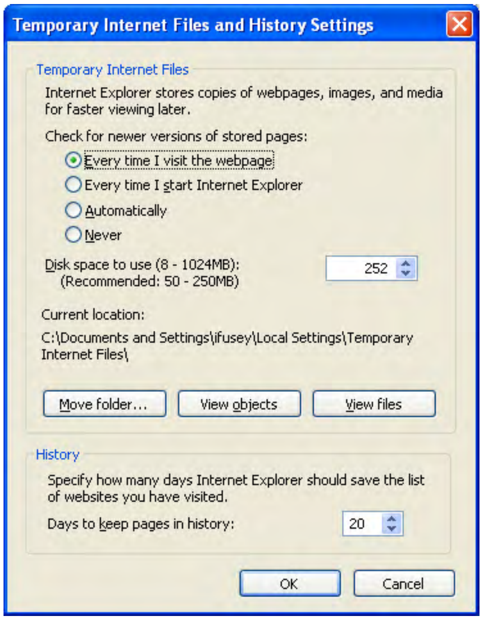
This appendix describes the connection requirements for the NMS management interface and the server command shell.

Browser 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 Browsing history box, click **Settings**.
3. In the Check for newer versions of stored pages section, verify that **Automatically** is selected.



Temporary Internet Files and History Settings

Temporary Internet Files

Internet Explorer stores copies of webpages, images, and media for faster viewing later.

Check for newer versions of stored pages:

● Every time I visit the webpage
○ Every time I start Internet Explorer
○ Automatically
○ Never

Disk space to use (8 - 1024MB): 252
(Recommended: 50 - 250MB)

Current location:
C:\Documents and Settings\jfusey\Local Settings\Temporary Internet Files\

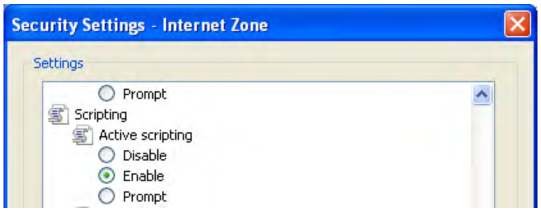
History

Specify how many days Internet Explorer should save the list of websites you have visited.

Days to keep pages in history: 20

Figure 25 Temporary Files Setting

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



Security Settings - Internet Zone

Settings

○ Prompt

Scripting

Active scripting

○ Disable

● Enable

○ Prompt

Figure 26 Active Scripting Setting

5 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 MI at the customer site requires access to the customer's network in close proximity to the HP MAS cabinets.

If the grid is configured with a High Capacity Admin Cluster (HCAC), you can only connect to the reporting Admin Node. You cannot connect to the processing Admin Node. In a grid with two HCACs, you can connect to either HCACs reporting Admin Node. Each HCAC displays a similar view of the grid; however, alarm acknowledgments made at one HCAC are not copied to the other HCAC. It is therefore possible that the grid topology tree will not look the same between two HCACs.

To connect to the NMS MI:

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 (reporting Admin Node in an HCAC) on the customer network. This is needed to access the NMS MI.

4 From the `Passwords.txt` file, note the NMS MI password for the Vendor account or the Admin account.

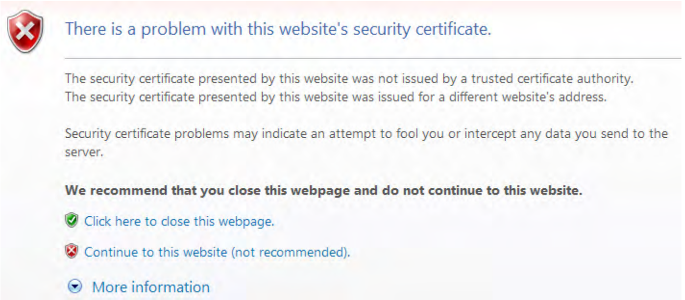
5 Launch the web browser.

6 Open the address **`https://<IP_address>`**

Where ***`<IP_address>`*** is the address of the Admin Node (reporting Admin Node in an HCAC) on the customer network specified in the `Configuration.txt` file.

Security Certificate

Depending on your version of Windows and web browser, you may be warned of a problem with the security certificate when you access the NMS MI URL.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Figure 27 Security Alert Window

If this appears, you can either:

- Proceed with this session. The alert will appear again the next time you access this URL.
- Install the certificate. Follow the instructions of your browser.

Log In

To log in:

1 Enter the username `Vendor` for full access to the NMS MI. If you are not making grid-wide configuration changes, you can also use the Admin account. For more information on user accounts, contact HP Support.
.

2 Enter the password for the NMS MI specified in the `Passwords.txt` file.

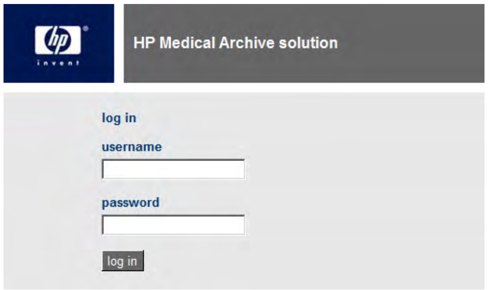


Figure 28 NMS MI Login Window

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.

Log Out

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

To log out:

1. Click **Logout** Logout located at the top right corner of the screen. The logging out message appears.
2. You may safely close the browser or use 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 start a command shell session:

- At the server, press **<Alt>+<F1>** to access a command shell and log in as root using the password listed in the `Passwords.txt` file.

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.

Accessing a Server Remotely

There are three ways to connect to a server remotely using ssh:

- From any server, using the remote server password
- From the primary Admin Node, using the ssh private key password
- From the primary Admin Node, without entering any password except the ssh private key password once

The primary Admin Node acts as an ssh access point for other grid servers. For the procedures to change the ssh private key password and to enable passwordless access from the primary Admin Node to other servers, contact HP Support.

To connect to a server from any 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.
3. When prompted, enter the password for the remote server listed in the `Passwords.txt` file.

To connect to a server from the primary Admin Node using the ssh private key password:

1. Log in to the primary Admin Node.
2. Enter: **`ssh <hostname>`**

   Where `<hostname>` is the name of the remote server.

   —or—

   Enter: **`ssh <IP_address>`**

   Where `<IP_address>` is the IP address of the remote server.
3. When prompted, enter the SSH Access Password listed in the `Passwords.txt` file.

To connect to a server from the primary Admin Node without entering a password:

1. Log in to the primary Admin Node.
2. Add the ssh private key to the ssh agent to allow the primary Admin Node passwordless access to the other servers in the grid. Enter: **`ssh-add`**

   You need to add the ssh private key to the ssh agent each time you start a new shell session on the primary Admin Node.
3. When prompted, enter the SSH Access Password.

   You can now access any grid server from the primary Admin Node through ssh without entering additional passwords.
4. When you no longer require passwordless access to other servers, remove the private key from the ssh agent. Enter: **`ssh-add -D`**
5. Log out of the primary Admin Node command shell. Enter: **`exit`**

Using GNU screen

The GNU screen program, which is installed by default, allows you to manage many shell instances concurrently, to connect to the same session from different locations, to detach from a session without stopping the program running within the session, and to resume a session that was previously detached.

The screen program decouples the terminal emulator from the running program. This means that the program keeps running even if you detach from the session or close the terminal emulator, or lose the connection.

Consider using screen when you execute maintenance procedures remotely and there is a possibility of losing the connection or where it would be useful to 'hang up' and connect back later. For example, you may want to use screen when cloning a CMS database since this procedure can take a few hours to complete.

To use screen:

1. Log in to a server remotely. For more information, see Accessing a Server Remotely (page 85).
2. Start screen. Enter: **`screen`**
3. Enter the command or script you need to execute in the new window.
4. To quit the screen session, enter: **`exit`**

   Screen has a number of command-line options. For example:

`-d`	To detach a session. The running program disappears from the terminal. However, it continues to run behind the scenes.
`-r`	To resume a detached screen session. This brings the program back to your terminal.
`-ls`	To list existing sessions
`-S <name>`	To name a session
`-x <name>`	To attach to a screen session that is already attached by another user (multi display mode). Either user can interact with the screen session or detach from it.

An example of how to use screen:

```
# screen -S CMScloneproc (Create a named session)
# <commands to start cloning process>
# <CTRL+A> <CRTL+D> (Detach screen session)
# screen -ls (List screen sessions)
There is a screen on:
        20849.CMScloneproc      (Detached)
1 Socket in /var/run/uscreens/S-root.
# screen -d -r CMScloneproc (Reattach to screen session)
```

For more information, display the man page for screen, and consult the GNU official web site http://www.gnu.org/software/screen/

Index