<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>task pause</td>
<td>126</td>
</tr>
<tr>
<td>task resume</td>
<td>127</td>
</tr>
<tr>
<td>task show active</td>
<td>127</td>
</tr>
<tr>
<td>task show detailed</td>
<td>127</td>
</tr>
<tr>
<td>task show detailed-active</td>
<td>127</td>
</tr>
<tr>
<td>task show detailed-history</td>
<td>128</td>
</tr>
<tr>
<td>task show history</td>
<td>128</td>
</tr>
<tr>
<td>Command-only Functionality</td>
<td>129</td>
</tr>
</tbody>
</table>
Preface

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

Note
This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to make sure that you are using the latest version of this document.

Purpose
This guide describes how to use EMC Data Domain Management Center (DD Management Center) features and tools.

This guide should be used after completing the instructions in the EMC Data Domain Management Center Initial Configuration Guide.

Audience
This guide is intended for use by both system administrators and general users of DD Management Center.

Related documentation
The following EMC publications provide additional information:

- EMC Data Domain Management Center Initial Configuration Guide
- EMC Data Domain Management Center Version Support Matrix
- EMC Data Domain Management Center Release Notes
- For additional information about EMC Data Domain systems, see:
  - The EMC Data Domain Operating System software documentation set.
  - The EMC Data Domain system installation and setup guides for each of your Data Domain platforms.

Special notice conventions used in this document
EMC uses the following conventions for special notices:

NOTICE
A notice identifies content that warns of potential business or data loss.

Note
A note contains information that is incidental, but not essential, to the topic.

Typographical conventions
EMC uses the following type style conventions in this document:
Table 1 Typographical Conventions

**Bold**
Indicates interface elements, such as names of windows, dialogs, buttons, fields, tab names, key names, and menu paths

**Italic**
Highlights publication titles referenced in text

**Monospace**
Indicates system information, such as:
- System code
- System output, such as an error message or script
- Pathnames, filenames, prompts, and syntax
- Commands and options

**Monospace italic**
Highlights a variable name that must be replaced with a variable value

**Monospace bold**
Indicates text for user input

[]
Indicates optional values

|
Indicates alternate selections - the bar means “or”

{}
Indicates content that the user must specify, such as x or y or z

...
Indicates nonessential information omitted from the example

Where to get help
Information about EMC software documentation, product updates, support, licensing, and more can be found at EMC Online Support (https://support.emc.com).

EMC Data Domain product documentation
To view documentation for EMC Data Domain products, go to EMC Online Support (https://support.emc.com), and select Support by Product below the Search box. Type Data Domain in the Find a Product box, wait for those words to appear in the list of matches below the box, and select the words. Then select ». In the list of categories under the Search box, select Documentation.

- The Product choices let you filter results by Data Domain system model number, such as DD990, or by DD OS software release.
- The Content Type choices let you filter results by category. Select More under Content Type to see all of the categories. The categories that contain end-user and compatibility documentation are:
  - Manuals and Guides, for the software and hardware manuals for your system, and for integration guides that explain how to use EMC Data Domain systems with backup software and other products
  - Release Notes, for specific versions of the EMC Data Domain Operating System and EMC Data Domain products
  - Compatibility Document, for guides that show which EMC and third-party components are compatible

Technical support
From EMC Online Support (https://support.emc.com), select Service Center. You will see several options for contacting EMC Technical Support. To open a service request, you must have a valid support agreement. Contact your EMC sales representative to get a valid support agreement or for questions about your account.
Your comments
Your suggestions help us continue to improve the accuracy, organization, and overall quality of user publications. Send your opinions of this document to DPAD.Doc.Feedback@emc.com.

Revision History of this Guide

The following table shows the revision history of the *EMC Data Domain Management Center User Guide*.

**Table 2** Revision History of this Guide

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>November 2014</td>
<td>Initial publication for release 1.2</td>
</tr>
</tbody>
</table>
Preface
CHAPTER 1

Overview of DD Management Center

This chapter includes:

- **Introducing DD Management Center** .......................................................... 12
- **DD Management Center Capabilities** ........................................................... 12
- **Differences between DD Management Center and DD System Manager** .......... 13
- **Backing up and Restoring in a VMware Environment** ..................................... 13
Introducing DD Management Center

Data Domain Management Center (DD Management Center) is a scalable, virtual appliance-based solution for centralized management of multiple Data Domain systems (DD systems).

DD Management Center provides current and historical data for these managed systems, with subject presentation ranging from site-wide summaries to drill-down detail for a selected object.

Comprised of a set of browser-based pages, DD Management Center, a rich Internet application (or RIA), is installed and runs on a VMware system, as described in the EMC Data Domain Management Center Initial Configuration Guide.

DD Management Center can also configure and monitor secure multitenant DD Boost backup and replication storage on multiple DD systems.

For a complete list of new features, see the EMC Data Domain Management Center Release Notes.

DD Management Center Capabilities

Using the robust features of DD Management Center, you can:

- Monitor the health and operation of managed objects on a user-defined dashboard
- Display site-wide storage capacity, showing aggregated usage totals
- Graph current and historical data about space usage, data consumption, and daily written data trends
- Manage the DD Secure Multitenancy (SMT) feature, especially to configure and monitor DD Boost access
- Monitor operational status of configured replications and set thresholds that generate alerts when replications lag
- Estimate projected capacity needs based on historical trends, and pinpoint specific dates (both past and future) for usage comparison
- Generate usage and performance reports, on demand, or set up a schedule and email list to facilitate proactive management
- Manage user access through configurable RBAC (role-based access control) settings

With DD Management Center, you can create custom groupings of DD systems, organized efficiently and intentionally. Applying groups and properties to managed objects lets you customize how content will be displayed, to best represent your infrastructure.

DD Management Center also allows feature configuration for its managed systems, such as managing user access and upgrading the operating system of a DD system or groups of systems.

From DD Management Center, you can also open a DD System Manager session for each managed system to provide full single-system management capabilities. In this way, DD Management Center provides both advanced multiple-system management capabilities and full single-system management capabilities.

DD Management Center can process alerts, which are viewed from a single list, for all of its managed DD systems.
Differences between DD Management Center and DD System Manager

The primary differences between DD Management Center and DD System Manager are the number of DD systems that each can manage, how these systems are managed (in an aggregated or non-aggregated manner), and whether storage is directly managed.

DD System Manager is primarily a single-system management tool that provides centralized monitoring and management for up to 20 systems. DD System Manager does not aggregate storage and/or performance data from multiple systems, nor can you compare operational information among systems. DD System Manager does directly manage storage (using VTL, CIFS, NFS, DD Boost, etc.).

DD Management Center provides centralized management for up to 100 DD systems, and you can perform the same task on all of these systems at the same time. Storage and performance data is aggregated for all systems, as well. Operational information can also be compared across systems.

You can launch DD System Manager from DD Management Center to get more information about, or to perform configuration for, a managed DD system.

Backing up and Restoring in a VMware Environment

Any process that creates and restores a snapshot of your entire virtual machine can successfully protect your DD Management Center installation.

It is highly recommended that you perform a snapshot before doing an upgrading procedure.

DD Management Center does not depend on having any integration with the backup software.

After the snapshot is restored, DD Management Center automatically performs any necessary application recovery.

Suitable backup software choices would include VMware Data Recovery (VDR), EMC Avamar, etc.

As with any data protection software, make sure to test your setup after you have installed your chosen backup software.

Note

The use of cloning has not been validated.
Overview of DD Management Center
CHAPTER 2

Getting Started

This chapter includes:

- Logging In and Out of DD Management Center .......................................................... 16
- Continuing DD Management Center Configuration ...................................................... 17
- DD Management Center Page Elements .................................................................... 17
- Organizing the Dashboard ............................................................................................ 18
- Organizing Managed DD Systems ............................................................................... 20
- Assigning Properties ................................................................................................. 24
- Displaying Property Information ................................................................................. 26
- Managing Groups ........................................................................................................ 27
- Managing Replication Lag Threshold Policies ............................................................ 27
- Working with Filters .................................................................................................... 28
Logging In and Out of DD Management Center

DD Management Center is accessed by using a supported browser on a workstation that has network access to the VMware server hosting DD Management Center. DD Management Center supports multiple simultaneous users.

The following browsers are supported for use with DD Management Center:

- On Microsoft Windows – Microsoft Internet Explorer 9, Mozilla Firefox 30 or later, Google Chrome
- On Apple OS X – Mozilla Firefox 30 or later, Google Chrome

Other browser versions may also work. These are the versions that had been validated at the time of DD MC v1.2 product release. See the EMC Data Domain Management Center Release Notes for the most-recent supported browser and Adobe Flash versions.

To enable file downloads to show a prompt dialog in Internet Explorer, it is recommended that the Security Zone in which the DD Management Center’s hostname or IP address belongs has the Automatic prompting for file downloads option set to Enabled for that Security Zone.

To change this setting for a specific Security Zone:

1. Select Tools > Internet Options.
2. In the Internet Options dialog, select the Security tab, select the Security Zone that applies to the DD system, and select Custom level.
3. In the Security Settings dialog, scroll to the Downloads section.
   - For the Automatic prompting for file downloads option, select Enable, and select OK. If a prompt appears asking if you are sure you want to change the settings for the Security Zone, select Yes.
4. Select OK to exit the Internet Options dialog.

Note

If DD Management Center is not already installed on the VMware server, refer to the EMC Data Domain Management Center Initial Configuration Guide for instructions.

Logging In to DD Management Center

Initial login requires using the “sysadmin” user ID and the “changeme” password (the default password). You are then prompted to change the sysadmin password. After that, other users with different roles (that have been added to DD Management Center) may login.

To log into DD Management Center:

Procedure

1. Open a browser, and enter the hostname or IP address of DD Management Center.
   - A Secure Login link is provided for establishing a secure connection over the network using HTTPS instead of HTTP. This option uses a self-signed certificate by default, which the user must accept, despite browser warnings.
2. In the login window, enter a user ID and password, and press Enter, or select Login.
Results
After you log into DD Management Center, the Dashboard is displayed, showing the default set of monitoring widgets.

Logging Out of DD Management Center
To log out of DD Management Center, select the Logout button (right-pointing arrow on the right side of the banner), or use the standard Close button on the browser window. Use the mouse to hover over any button or other graphical element to learn the names of controls, or to see more detail.

Continuing DD Management Center Configuration
After the installation procedure is complete, as described in the *EMC Data Domain Management Center Initial Configuration Guide*, the DD Management Center is running a basic configuration, but needs additional settings configured to be fully functional. The sysadmin may need to configure network settings and routing tables, set time zone configuration, and provide access for users.

DD Management Center Page Elements
The DD Management Center page is composed of:
1. Navigation Panel
2. Banner
3. Widget (this is the Current Health Status widget)
4. Logout Control
5. Online Help Control
6. Module (this is the Replication module)
7. Work Area
8. Status Bar and Notification Area

*Figure 1*  DD Management Center Page Elements

Unless the dashboard is maximized, the banner is visible at all times and provides controls to filter the scope of the work area’s active page (the filter control appears only on monitoring pages), open the online help, and log out.
The navigation panel is organized by module – Dashboard, Health, Capacity, Replication, Reports, Administration, and Inventory. Within each module, you can select the name of a subject page to be displayed in the work area.

The status bar shows the active user name and role, date, and alerts notifications (which you can select to see an informational pop-up with a link to the Alerts page).

Standard global controls (add, edit, delete) allow interaction with the application and manage how information is displayed on pages with tables (sorting column content by ascending/descending controls, hiding/displaying columns).

Navigating the DD Management Center Page

To navigate a DD Management Center page in order to change the focus and scope for the content displayed in the work area, you can use this procedure. In the illustration, the numbers correspond to the following steps:

Procedure

1. Select a module topic in the navigation panel.
   The default view for the page opens in the work area.
2. If included, select a tab on the top right to change the content on the page (for example, in the screenshot, display capacity by Systems, not MTrees).
3. If included, select a toggle button at the top right of the page to change the page view between a standard tabular list and a “grouped” tabular list.

For a page displaying groups, only the groups created by the user are shown.

Organizing the Dashboard

The Dashboard holds widgets that you create from a set of monitoring functions. The Dashboard lets you quickly check important conditions, such as unreachable systems, active alerts, diminishing capacity, etc.

You can set up separate tabs on the dashboard and include specific widgets for each of those tabs. Suggested uses for tabs are to organize a set of systems based on group membership, location, OS version, data type, etc. Another suggestion is to organize by widget type, for instance, a tab containing Current Health Status widgets for all systems.

By default, each user is assigned a Dashboard with one tab, populated by one each of the supplied widgets, configured to cover all of the systems that a user is monitoring. You can modify, add to, or even delete this default Dashboard tab.
A tab with all of its widgets can be copied to a new tab and then edited. Up to seven tabs are allowed.

## Adding Tabs

**Before you begin**

Navigate to the Dashboard > Monitoring page.

**Procedure**

1. Select the Add Tab control in the banner, at the top right.
2. In the Add and Configure Dashboard Tabs dialog, select Add.
3. In the highlighted text field, enter the name for the tab.
4. Choose the number of columns for the tab (more columns produce smaller widgets).
5. Order the placement of the tab across the dashboard using the Move Up or Move Down controls.
6. Select Save.

**Results**

The new tab is displayed on the dashboard.

## Adding Widgets

**Before you begin**

Navigate to the Dashboard > Monitoring page.

**Procedure**

1. On the dashboard, navigate to a tab, or create a new tab.
2. Select the Add widget control in the banner, at the top right.
3. In the Add Dashboard Widget dialog, enter a Name will reflect the widget’s use. For example, using a Top Replication Lags template, you may want to name the widget “New Jersey Replication Lag” if you set filters to show only those systems that replicate to New Jersey. The name must be unique on this tab.
4. Select a Template for the desired output. When you select a template, an icon appears under Example, showing a typical widget of that type.
5. If applicable, in the Settings area, select any of the available options (such as filtering to narrow the scope of the widget monitoring). Widgets can be filtered using standard filter primitives such as systems, groups, and properties. Also, depending on the template, you may have other settings that you can configure.
6. Select Add.

**Results**

The new widget is displayed on the dashboard.

## Copying Tabs

**Before you begin**

Navigate to the Dashboard > Monitoring page.

To create a new tab that contains the same widgets as an existing tab:
Procedure
1. Select the **Add Tab** control in the banner, at the top right.
2. In the Add and Configure Dashboard Tabs dialog, select the name of the tab to copy and then **Copy**.
3. In the text field, enter the new name for the tab (typing over “Copy of ...”).
4. If you want to change the number of columns, select the current number, and change it using the drop-down list.
5. If you want to change the placement of the new tab, use the **Move Up** or **Move Down** arrows.
6. Select **Save**.

Results
The new tab is displayed on the dashboard. You can open the widgets on the new tab to modify their properties.

Modifying Widgets
You might want to modify widgets that were copied from a tab as a starting point for a new set. For example, you could change the filter properties to monitor a different group, set of systems, or rule.

To modify a widget, use the Edit widget icon on the title bar to change the name, settings (if available), and filtering.

**Note**
The widget type (as determined by the widget template) cannot be changed with the Edit function.

Organizing Managed DD Systems
When you add a DD system to DD Management Center, the “Add systems” wizard includes options to assign it to a group, or groups, and to set properties for it.

As you organize and categorize each system, be aware that:
- Groups can be applied only to DD systems.
- Properties can be applied to DD systems, MTrees, and replication contexts.
- A set of system properties (DD system model, DD OS version, domain name, and data center) is automatically assigned when a system is added, so you will need to set only *custom* properties.

After you create groups and properties, they can be assigned when you add a DD system, although you can also assign them at any time.

Creating Groups
Groups are ways to organize Data Domain systems (DD systems) under a specific name, in a hierarchical structure created by the DD Management Center administrator. Groups are helpful for performing searches. When used by filters, groups reduce the number of systems returned. Groups can contain other groups and/or DD systems, after they have been added. A group can belong to only one group, but a DD system can belong to many groups.

You start by creating one or more super-groups at the Groups level, and then add sub-groups and DD systems.
Note
DD systems cannot be added at the root Groups node.

Procedure
1. From the Administration › Groups page, select Add.
2. Enter the name for the group.

Note
Group hierarchy structures cannot be changed. They must be deleted and re-created to change the structure.

3. To add a group at the root level, select Add. In the Add Group window, make sure only the “/” is in the Path text box. Enter a name for the new group, and select Save.
   The /newgroup is listed in the Groups panel.

4. To add a sub-group to a group, select a group (which will be the parent group) from the Groups panel, select Add, enter a name for the sub-group, and select Save.
   The sub-group is nested under the parent group in the Groups panel.

5. After a DD system has been added to DD Management Center, it can be added to a group. Select the target group from the Groups panel, and select Add. In the Add Group window, select a DD system from the Available Systems panel, select > to move the system into the Systems in the group panel, and select Save.
   The DD system displays in the Group groupname details panel when the group is selected in the Groups panel. When a DD system resides in more than one group, hover the cursor on the Information control to display the group assignments.

Adding Properties

To help with searching, filtering, and organizing, you can add properties for DD systems, for MTrees, and for Replication pairs.

For example, you could assign properties to help filter the list of DD systems in the Inventory › Systems page and narrow the scope of output produced by a dashboard widget or generated report.

When a DD system is added to DD Management Center, a set of default administration properties (DD system model, DD OS version, domain name, and data center) is automatically added.

You can add and assign other properties as needed.

The following procedure describes how to add a property; there are other procedures for actually assigning the value to the property.

Procedure
1. Select Administration › Properties. At the top right, select one of the three tabs (System, MTree, or Replication), and select Add.
2. In the Add Property dialog, enter a name for the property, and select its operation type:
   - String – Allows a string of up to 256 characters to be set when assigning the property, for example, you could name the property “Comments”, and then someone could enter “Waiting for Tom’s response”, “Not ready yet”, etc.
• **Boolean** – Creates a condition where you can assign one of two values, for example, you could name this property “Restored?”, and then the a value could be “True” or “False”, or “Yes” or “No”.

• **Fixed-value String** – Lets you provide a name and specific values for the property, for example, “Department” could be the name, and then “Finance”, “Human Resources”, “Marketing”, etc., could be the values. Selecting the option **Allow multiple types** lets you assign more than one value for a property to a DD system, or MTree, or Replication pair.

3. Select **Add**.

After you finish

After properties are created, you can assign them to an object.

**Adding (Registering) Data Domain Systems to DDMC**

**Before you begin**

Before you can manage a Data Domain system (DD system) in DD Management Center, you must add (register) it to the inventory with the following procedure.

A maximum of 100 DD systems can be added to a DD Management Center.

Groups of up to 20 systems can be registered at one time.

**Procedure**

1. Navigate to the **Inventory > Systems** page.

2. Select the **Add** (green + sign) control. Enter the following for the first DD system, then select **Add** to continue adding systems (up to 20 systems total). Make sure the box next to the system being added is checked. Select **Register** to continue:

   • **Host name** (required) – Enter the fully-qualified host name (use alphanumeric characters, dashes, periods, and underscores) or IP address. Ensure that the host name and the DNS name for the DD system match; a mismatch may cause problems with backup software.

   • **Sysadmin Password** (required) – Enter the sysadmin password used on the DD system (required).

   • **Firewalls** (optional) – Enter the inbound and outbound IP address (or host name) and port settings used by the firewall. If this option is selected, and you do not change the port setting, the default (3009) is used. If you do change it, the port number must be between 1 and 65535. The default port settings let DD Management Center communicate with the DD system. If the ports have been changed on the firewall or the DD system, they should also be updated here.

   • **Certificate** (optional) – Check certificate information by clicking in the associated cells. The Subject name in the DD Management Center CA certificate should match the DD Management Center host name, or SSL will fail the host verification.

3. The status page reports the success and/or failure of the additions. In the event of an error, select **Back** to return to the first page to display error messages and correct errors, or to delete the system. When you have fixed all of the errors, select **Next** to continue to the Properties page or **Close** to quit. (The **Next** button will be disabled until all of the errors are corrected.)
Note

Any settings made on the Properties page, the Groups page, and the Thresholds page will be applied to all of the systems being added.

4. Optionally, on the Properties page, select check boxes from the available properties list to assign properties to the DD systems, and select Next to continue to the Groups page.

5. Optionally, on the Groups page, select check boxes from the available groups list to make all DD systems members of the selected groups, and select Next to continue to the Thresholds page.

6. Optionally, on the Thresholds page, set warning and critical capacity thresholds for the DD systems (shown on capacity views and in reports).

7. Select Finish.

Results

A progress bar appears on the page showing the progress of the initial data synchronization for the newly added DD system(s). Additionally, the job progress details can be tracked on the Health > Jobs page.

After a DD system is added to DD Management Center, all historical information for that DD system is copied to DD Management Center. Then, anytime operational data changes on a DD system, the DD system notifies DD Management Center, which immediately polls the DD system to get the latest operational data.

Common Causes of Errors While Adding Systems

The following checklist may help you resolve some errors that can occur when trying to add a DD system to DD Management Center:

- Make sure the DD system is online. A DD system must be online in order to be added to DD Management Center.
- If you specified a port number in the firewall settings, make sure it is correct.
- Make sure you have added the DD Management Center to the DD system as a host. Also, if the system is a DDVE, make sure the system has been added as a host on DD Management Center. (Log into the system, and in ddsh, use `net hosts addIP hostname`).
- Make sure there are no networking issues preventing communication between the DD Management Center and the DD system.
- If you specified a host name for the DD system, make sure the host name can be resolved in your name space (DNS).
- Make sure the password entered for the system is correct.
- Make sure the DD OS version of the DD system is supported by your current version of DD Management Center (see the appropriate EMC Data Domain Management Center Release Notes).
- Make sure the DD system is not already managed by another DD Management Center. You can first delete the system from the original DD Management Center, or you can select the Override adding systems check box. The system will be added to the new DD Management Center, but the system’s status will be changed to unmanaged on the original DD Management Center, and data collection will be suspended for that system.
Editing a DD System's Settings

Before you begin

Navigate to the **Inventory > Systems** page.

After a DD system has been added to DD Management Center, you can edit its settings.

Procedure

1. Select one or more DD systems and then **Edit**.

   **Note**

   When more than one system is selected and they have different values for a property, the value is displayed as “mixed values”. The **Details** button shows all of the current values for each system. If you change a value when you have selected multiple systems, all systems will receive the new value, even if they did not previously have the same value.

2. In the **Edit System** dialog, choose any or all of the tabs to make changes (select **Apply**, or change tabs to save the new settings and continue reconfiguration). If you selected more than one DD system, only the Properties and Thresholds tabs are available.

   • **Configuration** – Add or change the inbound and outbound Firewall IP address (or host name) and port settings. The firewall port is optional. If you do not enter this, the default (3009) is used. If you do enter it, the number must be between 1 and 65535.

   • **Properties** – Assign a value to a property. A list of properties (default and user-created properties) are provided. The default system properties of Model, OS, and Domain Name are not editable. Data Center is a “hybrid” fixed-value string-type property. Because it is a default system property, it cannot be deleted, but its values can be edited and set for a DD system.

   • **Groups** – Add or remove group assignments. Select or deselect group assignments for the system. Any number of groups and subgroups can be selected.

   • **Thresholds** – Change configuration settings for warning and critical capacity thresholds for the system (shown on capacity views and in reports). When editing multiple systems with mixed warning thresholds, the initial warning value is zero.

     When editing multiple systems with mixed critical thresholds, the initial critical value is 100.

3. Select **OK** to save and exit system reconfiguration.

Assigning Properties

The procedure to assign a property is determined by where the property is used.

Properties can be assigned to DD systems, replication, and MTrees.

Assigning System Properties

This procedure describes how to assign a value to a system property that was previously added using **Administration > Properties > System**.

To assign a system property:
Procedure
1. Select **Inventory > Systems**.
2. Select one or more systems.
3. Select **Edit**, and in the **Edit System** window, select the **Properties** tab.
4. For each property listed, select the **Edit** control and assign a value. However, if more than one system is selected and different values are configured for the same setting among selected systems, the field will show **Mixed values**. If the value is changed with the **Edit** control, all systems receive the new value. An **Undo** control is provided for undoing the setting and a **More Details** control shows the saved value for the setting. For properties that were created as a:
   - **String** – Enter the text that will be displayed as the value.
   - **Boolean** – Select one of the two values from the drop-down list.
   - **Fixed-value string (and multi-value)** – Select the value from the drop-down list.
5. Select **OK** to set the values.

### Assigning Replication Properties

This procedure describes how to assign a value to a replication property that was previously added using **Administration > Properties > Replication**.

To assign a replication property:

**Procedure**
1. Select **Replication > Overview** or **Replication > Automatic**.
2. Select a replication pair.
3. Click **Assign Properties** and set a value. For properties that were created as a:
   - **String** – Enter the text that will be displayed as the value.
   - **Boolean** – Select one or the other value from the drop-down list.
   - **Fixed-value string (and multi-value)** – Select the value from the drop-down list.
4. Select **Assign** to set the values.
5. To see values assigned to replication contexts, add this property as a column in the replication table on the Automatic replications page. Select the Show Columns icon, and select the check box of the property from the list.

   The name of the property shows as the column title, and any value assigned to a context will appear in the cell.

### Assigning MTree Properties

This procedure describes how to assign a value to an MTree property that was previously added using **Administration > Properties > MTree**.

To assign an MTree property:

**Procedure**
1. Select **Capacity > Utilization**.
2. At the top right, select the **MTree** tab.
3. At the bottom right, in Properties, select **Assign** and set a value. For properties that were created as a:
• String – Enter the text that will be displayed as the value.
• Boolean – Select one of the two values from the drop-down list.
• Fixed value string (and multi-value) – Select the value from the drop-down list.

4. Select Assign to set the value.

**Displaying Property Information**

Assigned property values can be displayed as follows:

• You can select an element, such as a DD system, and display all of the properties assigned to it, or
• You can select a property and display all of the elements to which it is assigned.

**Viewing Element Properties**

To see the properties assigned to a particular element:

**Procedure**

• **Systems** – Select Inventory > Systems, and select a DD system.
  All properties assigned to that system are displayed in the Properties panel.

  **Note**

  You can also display properties by selecting the “gear” control in the systems banner. When you select one or more properties from the list of configured properties, a column for that property is added to the table. To hide the property, uncheck the property from the list. Some properties may not be removed from the table, so they will not appear in the list of configured properties under the gear control.

• **Replication** – Select Replication > Overview, select a replication pair, and select Pair Details.
  Any properties assigned to the replication pair are displayed in the Properties panel.

• **MTree** – Select Capacity > Utilization, select the MTree tab, and select an MTree.
  Any properties assigned to the MTree are displayed in the Properties panel.

**Finding Elements by Property Value**

To display a list of elements that are assigned the same property value:

**Procedure**

1. Select Administration > Properties, and select the property type (System, MTree, or Replication).
  The table shows all of the properties that have been created. Selecting a property displays its assigned values in the panel at the right.

2. To display where the property is assigned, select a property, and select the icon on the right side of the Key column.
  In the Property Assignment dialog, you can see the property type, the element where it is assigned, and the property values.
Managing Groups

Although group creation and modification can be performed only by the DD Management Center system administrator, any user can apply group designations to their DD systems, and can see the complete group structure, although RBAC (role-based access control) permissions control the systems that are displayed for each user.

Any permissions that are applied to a group affect all DD systems in that group. A lock image is added to the groups folder icon when permissions are directly applied to that group.

Use the Administration > Groups page to perform group management:

- Use Add to create groups or to add DD systems to existing groups.
- Use Delete to remove DD systems from the group-level organization. (You cannot use delete to remove systems from a group. But you can edit the group, and remove systems by selecting them in the right panel and selecting the left-pointing arrow)
- Use Edit on a selected group to modify the presence of DD systems within that group or the name of the group.

Note

Groups cannot be dragged and dropped into a different location; they must be changed with the Edit function.

Managing Replication Lag Threshold Policies

Replication lag threshold policies warn you when replication pairs do not complete replication within a set amount of time.

By assigning a replication lag threshold policy, you are assured that notifications will be displayed in the Replication > Automatic page and the Top Replication Lags and Replication Lag Status widgets when the replication has not completed within the time periods you have set for Warning and Critical levels.

The default policy level for Warning is 24 hours, and the default for Critical is 48 hours.

Replication lag threshold policies can be created only for MTree, collection, and directory replication. Lag threshold policies for On-Demand replications are not supported.

To create a lag threshold policy:

Procedure

1. Navigate to the Replication > Automatic page.
2. Select one or more replication pairs from the table.
3. To create a policy, select Lag Threshold Policy (or right-click the pair, and select the option).
   a. In the Lag Threshold Policy dialog, from the Threshold policy menu, select Create a new policy.
   b. In the Manage Lag Threshold Policies dialog, select Add.
   c. In the text field, enter the policy name, and use the slider controls to set the threshold points for the Warning and Critical lag levels.
   d. Select Save.
4. Back in the Lag Threshold Policy dialog, select a policy from the Threshold Policy menu, and select **Assign**.

**Results**

The policy is applied to the selected replication(s). The assigned policy name is displayed in the table in the Threshold Policy column.

To modify or destroy a policy, select **Manage Lag Threshold Policies** (or right-click the pair and select the option). In the Manage Lag Threshold Policies dialog, select a policy from the list, and select **Edit** or **Delete**. If a deleted policy was assigned anywhere, it is replaced with the Default policy. Select **Save** to exit.

---

**Note**

The Default policy cannot be renamed or deleted, but it can be modified.

---

**Working with Filters**

Filters are used to selectively define the output of a DD Management Center function. For example, filters can be used to define the scope of elements that display on a page, tailor the output of a Report, or target the DD systems to be monitored for Dashboard Widgets. The **Filter** (funnel-shaped) control appears on pages and dialogs whenever a filter can be used.

The drop-down menu on the **Filter** control allows you to select the groups, properties, DD systems, or rules to be used for filtering. When a filter is active on a page, the **Filter** control is highlighted in yellow. Filtering can be switched on or off using the **Filter** control as a toggle.

The **Filter by rule** option lets you create custom rules that can be saved for reuse or run in the current location. The rule can be built using any of the standard filter criteria (groups, properties, DD systems), along with any existing properties or groups that have been created. Controls for logic (is, is not, contains, does not contain, etc.) are provided, and statements can be inclusive or selective.

To create a custom rule:

**Procedure**

1. From the **Filter** drop-down menu, select **Filter by rule**.
2. In the Filter by Rule dialog, provide a name for the filter.
3. Using the selection menus in the **Match the following** area, create the criteria for your rule. The criteria consists of one or more statements.

   Create the first statement by selecting an object from the first menu (System, Group, Model, OS, Domain Name, etc.) and a logic condition (contains, does not contain, is, is not, etc.), then the target (text you input or a menu selection, based on the previous selections). For example, a statement could be “Model is DD880”.

4. If needed, add more statements with the **Add row (+) control**, or add conditions to the rule using the **Block (...) control**, which adds the choice of **All** or **Any** to the **Match the following** area, and create additional statements.
5. Select the **Save** (disk) control to make this filter available from the **Filter** menu list or select **Filter** to run the filter once and exit.
6. To remove the filter and return to unfiltered content, select **Clear filter** from the **Filter** menu.

   Note that the filter may still be available with the **Recent filters** option on the **Filter** control list.
CHAPTER 3

Monitoring Systems with DD Management Center

Included in this chapter are the topics:

- How DD Management Center Helps You Monitor Systems ........................................ 30
- DD Management Center Data Retention Policy .......................................................... 30
- DD Management Center Space Projection Algorithm .................................................. 31
- Performing Daily Monitoring .................................................................................... 31
- Performing Capacity Monitoring ............................................................................... 35
- Performing Replication Monitoring .......................................................................... 36
- Monitoring Status with Reports .................................................................................. 36
How DD Management Center Helps You Monitor Systems

The monitoring tools of DD Management Center let you examine a wide array of operational information about managed Data Domain systems.

After a Data Domain system (DD system) is added to DD Management Center, all historical information for that system is copied to DD Management Center.

When operational data changes on a DD system, the DD system notifies DD Management Center, which immediately polls the DD system to get the latest operational data.

DD Management Center monitoring tools draw on this data for current and historical reporting and for creating trend projections.

DD Management Center monitoring tools are highly visual – using charts, graphs, and color coding to help you interpret essential data points and easily notice alerts for critical markers.

DD Management Center monitoring tools help you focus on areas of interest. They can show mile-high status checks of all managed DD systems and check a specific group of DD systems, as well as drill-down to check the health or operational history of a single system’s components. For capacity monitoring, you can easily check current operation and historical data and perform capacity predictions based on usage trends.

Using the filtering and grouping options provided on monitoring pages, DD Management Center lets you easily shape your data presentation so you can focus on viewing just the information you need.

In addition to data provided on the interface, you can generate reports to compile operational data that can be exported. Reports can be generated ad hoc or scheduled and emailed to a list of interested parties.

DD Management Center Data Retention Policy

DD Management Center maintains up to ten years of performance and capacity measurements for the DD systems it is monitoring. Data from the DD systems are consolidated into hourly sample points, generally collected at 30 minutes past the hour. The hourly samples are consolidated into daily samples, where a day is considered to run from Noon to Noon. Daily samples are further consolidated into weekly samples, where a week begins on Sunday.

To reduce the amount of space needed to store this historical data, DD Management Center periodically discards older samples. The number of samples retained depends on the nature of the data and whether the sample is hourly, daily, or weekly data. The following table shows the length of time that DD Management Center retains each sample.

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Keep Hourly Samples for</th>
<th>Keep Daily Samples for</th>
<th>Keep Weekly Samples for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection space usage</td>
<td>3 months</td>
<td>1 year</td>
<td>10 years</td>
</tr>
<tr>
<td>MTree space used</td>
<td>1 month</td>
<td>3 months</td>
<td>10 years</td>
</tr>
<tr>
<td>Automatic replication (bytes transferred and lag)</td>
<td>1 month</td>
<td>3 months</td>
<td>10 years</td>
</tr>
</tbody>
</table>
Table 3 Data Retention Policy (continued)

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Keep Hourly Samples for</th>
<th>Keep Daily Samples for</th>
<th>Keep Weekly Samples for</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-demand replication (number of files and bytes transferred)</td>
<td>3 months</td>
<td>1 year</td>
<td>10 years</td>
</tr>
<tr>
<td>Performance (CPU and network)</td>
<td>1 month</td>
<td>1 year</td>
<td>none created or retained</td>
</tr>
</tbody>
</table>

Finally, DD Management Center retains up to 2,000 historical alerts from each DD system being monitored.

**DD Management Center Space Projection Algorithm**

DD Management Center uses a sophisticated algorithm to project growth in space usage and to predict when a DD system will run out of space. This algorithm was developed and verified using years of autosupport reports and should be quite accurate.

The goal of the algorithm is to compute a linear projection of space growth using an optimal set of recent data points. The data history is scanned to find the projection with the best fit (that is to say, the regression with the highest $R^2$ value). After the best fit is determined, the projection must pass these validation tests to ensure that the prediction is accurate:

1. DD Management Center must have at least 15 days of historical data.
2. The regression $R^2$ value must be at least 0.9 or higher.
3. The slope of the regression must be positive (that is, space usage is growing, not shrinking).
4. Time-to-full must be less than 10 years in the future.
5. The DD system must be at least 10% full.
6. The most recent data sample must be within 5% of the projection.

Combining all of these validation criteria accounts for typical DD system usage behavior, such as space becoming free after a cleaning cycle, jumps in usage as new backup loads are stored on the DD system, and space becoming free when backups are deleted.

**Performing Daily Monitoring**

Using DD Management Center to perform daily monitoring of your site lets you check for unusual activity before it becomes a serious problem.

The following sections describe tasks you should perform at least daily to get an overview of the operational status of your DD systems and data replication.

**Checking Dashboard Status Widgets**

The Dashboard > Monitoring widgets (Current Health Status, Active Alerts, etc.) provide an overview of key performance indicators for your monitored DD systems. Widget functions let you check the health and status of DD systems and alert you to storage capacity threshold warnings and replication lags or failures.

The graphs, dials, and color-coded alerts make it easy to spot system operational problems. Many components on the widgets provide a link to the full-featured page for the function so you can drill-down to see complete information.
By default, one tab is provided named **All Systems** that is populated with one of each type of widget, which are configured to monitor all managed DD systems.

If any of its monitored systems are not online, a **Status** button appears at the top right corner of a widget (except for Active Alerts). Selecting this button shows the count of systems with connection issues. Selecting the **Show Health Status** link opens the Health Status page, where a list of these systems is displayed.

**Checking Health Status**

The Dashboard health status and alerts widgets highlight systems that are reporting major reachability or operational problems. And if there are problems, the widgets provide drill-down links to system details.

**Current Health Status**

The Current Health Status widget highlights unreachable systems and systems having problems with file system and replication operation, alerts, and data transmission protocols. The widgets show All Normal or show a count of systems exhibiting problems.

- Selecting the system count for each category navigates to the Health Status page, filtered to display the status of only that widget’s systems.
- Selecting the banner for unreachable systems navigates to the Health Status page to show the status of just the unreachable systems.
- The marker for All Normal status has no navigation or drill-down behavior.

**Active Alerts**

The Active Alerts widget displays a tally of systems with outstanding alerts for Emergency & Alert, Critical & Error, and Warning, using color-coded bar graphs.

- The length of the bar shows the total number of alerts, while color and symbol provide visual clues.
- Selecting the alert bar takes you to the Alerts page, filtered by the widget’s configured filters and the type of alert category.

**Checking System Capacity**

The System Capacity widgets help you to spot shortfalls in overall managed storage capacity and monitor managed system storage usage.

**Capacity**

The Capacity widget displays systems that are nearing warning or critical storage capacity levels.

Also, if configured, you can monitor the projected capacity usage for an upcoming selected interval.

**Space Usage**

The Space Usage widget lets you monitor aggregate totals of storage levels for all of the DD systems it is configured to manage. This widget monitors the total storage capacity of all systems (for space that is used and available) or a selected group if a filter is set. You can also check pre-compressed space usage and compression ratios to verify that deduplication is working as expected.

**Checking Replication Progress**

The Replication widgets provide replication status, problems, and statistics.

**Replication Status**

The Replication Status widget highlights replications with performance problems for the widget’s monitored systems. Also, if configured, it shows the total bytes written and the total bytes replicated in the last 24 hours.
Top Replication Lags
The Top Replication Lags widget shows source DD systems with replication pairs exhibiting critical and warning lag, ranked by severity (Critical, followed by Warning) and by longest delay. The lag time for the worst performing replication pair on the system is shown, along with the lag trend for that pair (increasing, decreasing, or holding steady). Select a system entry to open the Replication > Automatic page, showing all pairs originating from that system.

Replication Lag Status by Pairs
The Replication Lag Status by Pairs widget shows the count of replication pairs exhibiting Critical, Warning, and Normal threshold levels, based on the assigned policies. Selecting a bar navigates to the Replication > Automatic page, showing all pairs with that severity.

Checking Alert Notifications
For new, unacknowledged alerts on systems you are authorized to manage, always check the “Notification Area,” located in the lower left of the Status Bar (the bottommost border of the DD Management Center window).

This Notification Area is not constrained by filter settings that are active, that is, it displays notifications of alerts for all of the systems you are authorized to manage.

The “New Alerts” area shows the current unacknowledged Emergency, Error, and Warning level alerts. Click anywhere on the New Alerts area to display a pop-up reporting the severity, system name, and class of the new alert. After the pop-up has been displayed, the alerts notification is removed from the Alerts Notification area.

To see the alert details, select the “Show me these alerts” link to open the Health > Alerts page, where the table is filtered to show only the new alerts.

Checking Health: Status
For operational problems, check the Health > Status page.

Use the Systems/Groups/Tenants icons at the top right of the page to toggle page content to show all DD systems and DD systems organized by group or tenant assignment.

Note
Secure Multitenancy functionality requires DD systems running DD OS 5.5 or later.

When you select the Tenants icon, note the following:

- When a DD system is offline, the tenant units in that system become offline as well. The tenant unit offline icon is displayed in the tenant unit tree.
- The Tenant Unit Details control (top left) launches the Tenant Unit Details Lightbox.

You can use the Sort Ascending option on the Connection Status column to find connection problems on systems. Check the status LEDs for any red or yellow status conditions.

Here is an explanation for the different colors of the LEDs:

- Grey – disabled components
- Red – errors or problems. Hover the cursor over a red LED for a link to a page with more detail.
  - Hover the cursor over the icon in the Systems column, and select the link Show alerts to open the Alerts page.
If the File System is destroyed or disabled, a red LED is displayed. As a result of this non-activity, Protocols and Replication are affected and show a red LED as well.

- Yellow – warning and errors
- Green – normal operation
- Non-licensed components are shown with an empty socket

If a system is unreachable, the last known state of the LED shows for all other columns. (This does not apply to disabled or non-licensed systems.)

### Checking Health: Alerts

In addition to checking Health Status for operational problems, also check the **Health** > **Alerts** page. Be sure to watch for new or repeating alerts.

Use the Systems/Tenants icons at the top right of the page to toggle page content to show all DD systems or DD systems organized by tenant assignment.

**Note**

Secure Multitenancy functionality requires DD systems running DD OS 5.5 or later.

Select the Active Alerts or All Alerts tab, depending on what you need to view.

Use the Date range filters to narrow or expand the focus of alert scoping or to go back to a specific point in time.

When you select the Tenants icon, note the following:

- The Tenant Unit Details control (top left) launches the Tenant Unit Details Lightbox.
- A special “all” tenant unit alert is applied to all tenant units in the system.

**Note**

For additional information on specific alerts, see the Error Message Catalog on the EMC Online Support Site.

### Checking Health: Jobs

In addition to checking Health Status for operational problems, also check the **Health** > **Jobs** page.

On this page, you can:

- Filter jobs by Failed, In progress, and/or Succeeded.
- View more details in the Details panel at the bottom. Up to ten levels of details are displayed for each job.
- Select a job from the main list and expand the steps to see sub-steps up to ten levels deep.

### Checking the System Details Lightbox

To see detailed highlights of the operation and status of a Data Domain system (DD system), open the **System Details lightbox**.

The lightbox can be opened by navigating to the **Health** > **Status, Capacity** > **Utilization** or **Replication** > **Overview** page; then selecting a DD system from the table; and selecting the **System Details** button.
Using Graphs to Chart Performance

To chart historical activity for the CPU utilization and throughput of the file system, protocol, and replication activity of a Data Domain system (DD system), check the System Details > Charts page.

With this tool, you can graph a system’s resources (CPU utilization and network throughput) to identify:
- whether a system’s resources have been overloaded for significant time periods
- the time frames and systems to consider for a new backup or replication
- whether more systems are required

Checking System Bandwidth

To see if a Data Domain system (DD system) is experiencing bandwidth related bottlenecks, go to the System Details > Charts page, and select the Network throughput chart.

Determine how much network bandwidth is being used by DD systems sharing the same subnet to see if any are using more than expected or allowed by IT departments.

Performing Capacity Monitoring

Use the Capacity pages to view information about storage utilization, by toggling between the Data Domain systems and MTrees being managed by DD Management Center.

You can check the current and historical space consumption, as well as estimate projected near-term future storage needs.

Checking System Capacity Utilization

The Capacity > Utilization page presents storage usage amounts for monitored systems (default), or their MTrees. These selections can be viewed either by system or MTree name or by configured group. Each row in the table shows usage levels for a managed system or MTree, and aggregated totals are presented as the last row of the table. Selecting multiple systems displays their aggregated details.

This information gives you the ability to:
- Monitor the capacity of logically grouped or single systems to track usage and identify the systems that are using capacity too quickly
- Identify systems that have used up all their storage space
- Identify systems that have deviated from their norm for compression ratio, etc.
- Identify systems as targets for new back ups, replication, and migration
- View how much data was written during a timeframe, such as a back-up cycle, and determine how much it has been compressed
- Identify when garbage collection runs and how much space is reclaimed
- For Extended Retention systems, identify how much space is available and used on the Archive and Active tiers, and how well it is compressed

Checking Disk Space Usage Trends

To monitor disk space usage trends, check the Capacity > Utilization page.

The Space Usage and Consumption tabs in the Charts panel provide information about:
- Systems that are consuming space at a rate significantly greater or less than their historical norm
- Total capacity, amount consumed, and compression ratio (aggregate) for a group of systems
- Data ingest rate for a group of systems, for example, the total data ingest rate for the last 24 hours
- Systems that are out of space or critically low on space
- The amount of data that was backed up the previous night (24 hour period), and the compression ratio for a group of systems
- The last time that garbage collection was run and how much space was reclaimed

Check the **Capacity > Projected** page to:
- Predict when systems will run out of storage space or reach a critically low point
- Determine future capacity needs by projecting historical and current trends
- Determine targets for migration by projecting the systems that are filling up versus the same model systems that will have space available

### Performing Replication Monitoring

The Replication pages let you check the status of managed Data Domain system (DD system) replication and file replications by viewing pairs, cascaded replications, and topology charts. You can:

- Find status problems by selecting **Sort Descending** on the Status column to bring replication pairs with errors to the top of the table.

- On the Replication Automatic page, select **Sort Descending** on the Lag and Lag Trend columns to bring replication lag trends and lag time over critical and warning thresholds on DD systems to the top of the table. If replication is not working because of an error, the lag trend value for replication will be empty.

- On the Replication Overview page, select the Topology tab to visually check the operational status of connections, clicking the color-coded status indicators of arrows between systems to view details; and hovering the mouse to view details. Use controls to zoom in and out, and expand and collapse the contents of configured contexts on systems.

- Drill down (double-click a pair) to see status and details for a replication pair on the Cascades view

### Monitoring Status with Reports

Reports compile information for areas of interest on managed systems and are generated based on three default template types (capacity, replication, and status) for DD Systems, and on two default template types (status and usage) for Secure Multitenancy (SMT).

The template configures the report's content, schedule, and email distribution.
Creating a Report with the Wizard

This section describes how to create a report template for use in running reports about key data points, using the Add Report Template wizard.

Procedure

1. From the Reports > Management page, select Add.

2. In the Add Report Template dialog, select the type of report you want (System Reports or Multitenancy Reports), and select Next.

3. Enter a name, and select a Template. For System, the choices are Capacity, Replication, or Status. For Multitenancy, the choices are Status or Usage. Choose one or more Sections to include, and select Next.

4. Depending on whether you selected Multitenancy or System:
   a. Multitenancy: Select a Scope (Tenant Unit or Tenant). The SMT Status report is always configured to show the last 24 hours of historical data, and you can select the Report retention (Forever, 7 days, 30 days, 90 days). The SMT Usage report (which generates as an excel spreadsheet) lets you display data for a full month or a full week, and you can select the day of the week/month for it to start (by selecting Edit). You can also specify Report retention.
   a. System: Select a filter to narrow the scope of reported objects (for example, filter by selected groups). Select the time span for data collection (for example, last 24 hours), and the report retention (for example, 7 days). Select Edit to set a schedule for the frequency and time the report is run. Select Next.

5. Optionally, add recipient email addresses (for when the report completes and/or if an error occurs). Select Next.

6. Review the details, then select whether to run the report immediately and/or save the template for later use. Select Finish.

Results

After it has been created, the report template is added as an entry in the reports table. When selected, the template can be used to immediately run a report, or it can be edited or deleted, or the time it was last run can be displayed.

Generating a Report Immediately

To generate a report immediately, select a report template listed in the Template name table, and select Run Report.

A report (named by concatenating the data stamp to the template title) is created and opened as a PDF file in your browser, except for the Tenant Usage report, which generates an .xlsx file.

The report generation information is listed in the Report History table, where it can be viewed, renamed, or deleted.
CHAPTER 4

Managing Data Domain Systems

Provided in DD Management Center are some tools that can be used to manage Data Domain systems. They include:

- Launching DD System Manager ................................................................. 40
- Upgrading Data Domain System Software ................................................ 41
- Creating Access for Users ...................................................................... 42
Launching DD System Manager

From some DD Management Center pages, you can launch a DD System Manager session for the selected Data Domain system (DD system) to perform configuration or troubleshooting. The launched version of DD System Manager actually runs on DD Management Center and not on the DD system, thereby giving you centralized, secure, and simultaneous administration for multiple DD systems.

**Note**

Launching from DD Management Center, v1.2, will bring up DD System Manager, v5.5.0. Any new features introduced in releases later than 5.5.0 will not be displayed.

To initiate a session, select an entry in a table listing (for example), and select Launch DD System Manager from any of the following DD Management Center pages:

- **Health** > **Alerts**
- **Capacity** > **Utilization**
- **Capacity** > **Projected**
- **Inventory** > **Systems**
- **Replication Pair Details Lightbox**
- **System Details Lightbox**

**Note**

Be sure the pop-up blocker on your browser is configured to allow pop-ups for DD Management Center.

The DD System Manager session that starts (in a new window) requires no login or logout and provides complete management of the DD system. DD System Manager opens showing the corresponding area from where it was launched (for example, if the launch was from the Alerts view, the Alerts page on the DD system is opened).

The launched DD System Manager appears the same as a native DD System Manager session, except the navigation panel and Reports and Task Logs tabs are omitted. The banner shows the DD Management Center name, and the DD System name, OS release, and model type, as well as your management role (admin, etc.).

Note the following about launching DD System Manager from DD Management Center:

- You can launch DD System Manager only for a system for which you have an admin role.
- A permission is comprised of a system or group, a user (local or NIS), and a role.
  - The admin role is required for replication configuration and IPMI configuration.
  - The Security Officer role is not supported.
- The inventory of DD systems on DD Management Center is used.
  - The DD systems shown are based on your effective permissions.
  - Only replication source and destination systems registered with DD Management Center are shown.
- You do not need to open any additional firewall ports for the session (that is, after a DD system is added to DD Management Center, the existing port assignments are used for the DD System Manager connection).
Upgrading Data Domain System Software

The DD OS on one, or a group of, Data Domain systems (DD systems) can be upgraded from DD Management Center. You must have admin rights on the DD system to upgrade and manage upgrade packages, and you must have admin rights on DD Management Center to manage upgrade packages.

To perform a DD OS upgrade, you must

- Obtain a DD OS upgrade package, by downloading an upgrade package from the EMC Online Support site.
- Upload the DD OS upgrade package to DD Management Center using the Inventory/Systems Manage Packages dialog.
- Perform the DD OS upgrade on the DD system.

Managing DD System Upgrade Packages

You can create a collection of upgrade packages to use when upgrading the DD OS on managed Data Domain systems (DD systems).

You first download the upgrade package from the EMC Online Support site to a locally accessible drive and then add the package to the DD Management Center upgrade package collection.

Procedure

1. Navigate to the Inventory > Systems page.
2. Select a DD system or systems.
3. The banner will display Upgrade if the currently selected system(s) allow an upgrade. In this case, to manage packages, use the drop-down for “Upgrade” to select Manage Upgrade Packages. If the currently selected system(s) do not allow an upgrade, the banner will display Packages, and selecting this will present the Manage Upgrade Packages dialog.
4. Select the appropriate option from the Manage Upgrade Packages dialog:
   - Select the EMC Online Support link to obtain an upgrade package to store locally.
   - To upload a package to the DD Management Center inventory, select Add and browse to the local drive to select the package.

Results

After the upgrade package has been uploaded to DD Management Center, it can be used to upgrade one or more DD systems.

Performing DD System Upgrades

The DD OS on one or more Data Domain systems (DD systems) can be upgraded from DD Management Center with one upgrade operation.

Procedure

1. Navigate to the Inventory > Systems page.
2. In the Inventory table, select one or more target systems for the DD OS upgrade. Ensure the OS column is visible.
3. From the Upgrade menu, select Upgrade.
4. In the Upgrade Systems dialog, select the DD OS version from the drop-down list. Versions that display in the drop-down list reside on the DD Management Center; they have been either downloaded from the EMC Online Support site or uploaded from a local drive, as described in the previous topic.

The body of the window shows any warnings or errors. All errors must be removed before the upgrade is allowed. Errors can be removed by removing the offending system from the list, or possibly by changing the target upgrade version. You may choose to correct the condition separately, and try again later. Warnings such as those for resulting incompatible versions in a replication pair will not disallow the upgrade.

Also, if there are no packages in the DD Management Center inventory, there will be a link above the table on the right that will take the user to the Manage Upgrade Packages dialog.

5. Select Upgrade to upgrade the selected systems.

If systems are not in an acceptable managed state (for example, unreachable, suspended, upgrading) the upgrade action is unavailable.

Note

Depending on the number of DD systems selected for the upgrade and other factors, the upgrade may take a long time. After the upgrade, each DD system automatically reboots. File access is interrupted during the upgrade. Progress for the upgrade can be tracked on the Health > Jobs page.

Creating Access for Users

To allow a group of users to access DD Management Center:

Procedure

1. Go to the Administration > Settings page, and select the Access > Local Users tabs.

2. Select Create to add users and access groups (NIS and Active Directory) to DD Management Center.

These users can log into DD Management Center, but can't see any other systems. You can add permissions to view (user role), administer (admin role), or take snapshots (backup operator) for groups and Data Domain systems (DD systems).

Users and user groups have either admin or user roles. If a user or a user group has the admin role, they can view all DD systems by default; it is not necessary to set any other permissions for admin users and groups. For users and user groups with the user role, perform the next step to set permissions on DD systems so these users may view the systems.

3. To add permissions, go to the Administration > Permissions page, and select Add.

4. Select where to add the permission:

   • Add permissions to systems – Select this option, and from the list of managed DD systems, select the check boxes of the systems where the permissions are to be assigned.

   • Add permissions to groups – Select this option, and from the list of groups, select the check boxes of the groups where the permissions are to be assigned.

5. In the User area, select + (Add), select one or more users from the Select Users dialog, and select Select.
6. Click in the Role field for the user, and select the access role: Administrator, Backup Operator, or User.

7. Select **Add**.

The users are given the assigned role (Administrator, Backup Operator, or User) for the selected systems or groups.

**After you finish**

To simplify the management of permissions:

- It is recommended that the use of the admin role for the DD Management Center be minimal.
  - The admin role can manage all DD systems in the DD Management Center inventory. In addition, the admin for the DD Management Center configures the DD Management Center properties and groups and assigns its permissions.
  - Configure most logins for DD Management Center with the user role.
- Use NIS user groups for permissions – this simplifies the process for adding, removing, and modifying users without changing the permission assignment.
- Use DD System Groups for permissions rather than assigning permissions to individual systems.
  By assigning permissions at the group level, policy-based permissions can be used with a union model that is applied to the entire group hierarchy.
- Start with lower level permissions at the top of the hierarchy:
  - Assign lower level permissions toward the root of the Group hierarchy.
  - Assign higher level permissions toward the leaf of the Group hierarchy.
  - Use a union model, not an override model. This makes it easy to change permissions at lower levels without affecting the entire hierarchy.

**Verify Changes:**

- After assigning permissions or changing group membership, verify the change by looking at the Effective role for a system.

**Use Central Administration:**

- Use DD Management Center to centrally administer all systems, reducing the use of local accounts on each managed DD system. Turn off direct GUI access to DD systems that are managed by DD Management Center.
CHAPTER 5

Administering SMT using DD Management Center

Included in this chapter are the topics:

- How DD Management Center Helps You Monitor SMT............................................. 46
- Creating and Managing Tenants ............................................................................ 50
- Creating and Managing Tenant Units ..................................................................... 53
- Creating, Editing, and Generating Multitenancy Reports........................................ 62
How DD Management Center Helps You Monitor SMT

DD Management Center can configure and monitor secure multitenant DD Boost backup and replication storage on multiple DD systems.

In a secure multitenant environment, storage administrators (“landlords”) and backup administrators (“tenants”) cooperate to allocate and manage storage, as follows:

1. The storage administrator creates tenants on DD Management Center. For example, the storage administrator in a corporate IT organization might create a tenant for the backup administrator in the finance department.
2. The storage administrator creates one or more Tenant Units on DD systems to serve as virtual containers for each tenant.
3. The storage administrator creates one or more MTrees and/or DD Boost Storage Units.
4. The backup administrator configures backup software to use the MTrees in the Tenant Unit as storage targets.

For additional information, see the “Working with Secure Multitenancy” chapter of the *EMC Data Domain Operating System Administration Guide*.

DD Secure Multitenancy Overview

EMC Data Domain Secure Multitenancy (SMT) provides secure storage consolidation in Protection Storage.

Segregating, isolating, and protecting data of multiple customers – on a single DD system – is the main feature of SMT.

Multiple tenants can simultaneously reside on a single DD system, but the activities of one tenant cannot be detected by another.

Within an enterprise, a tenant may consist of one or more business units or departments on a DD system configured and managed by IT staff.

- For a business unit (BU) use case, the Finance and Human Resources departments of a corporation could share the same DD system, but each department would be unaware of the presence of the other.
- For a service provider (SP) use case, the SP could deploy one or more DD systems to accommodate different Protection Storage services for multiple end-customers.

Both use cases emphasize the segregation of different customer data on the same physical DD system.

SMT Components Defined

This section provides definitions for some of the components in a Secure Multitenancy (SMT) environment.

**MTrees**

*MTrees* are logical partitions of the Data Domain file system and offer the highest degree of management granularity, meaning users can perform operations on a specific MTree without affecting the entire file system. MTrees are assigned to Tenant Units and contain a Tenant Unit’s individualized settings for managing and monitoring SMT.

**Multitenancy**

*Multitenancy* refers to the hosting of an IT infrastructure by an internal IT department, or an external service provider, for more than one consumer/workload (business unit/
department/tenant) at the same time. Data Domain’s Secure Multitenancy (SMT) feature enables data-protection-as-a-service.

Role-based Access Control (RBAC)
Role-based Access Control (RBAC) offers multiple roles with different privilege levels, which combine to provide the administrative isolation on a multitenant DD system. (The next section will define these roles.)

Storage Unit
A Storage Unit is an MTree configured for the DD Boost protocol. Data isolation is achieved by creating a Storage Unit and assigning it to a DD Boost user. The DD Boost protocol permits access only to Storage Units assigned to DD Boost users connected to the DD system.

Tenant
A tenant is a consumer (business unit/department/customer) who maintains a persistent presence in a hosted environment.

Tenant Self-Service
Tenant Self-Service lets a tenant log in to the DD system to access the Tenant Units assigned to him or her and perform their own administration and reporting for their own environments. Tenant Users and Tenant Admins will, of course, have different privileges, as described in the next section.

Tenant Unit
A Tenant Unit is the partition of a Data Domain system that serves as the unit of administrative isolation between tenants. Tenant Units are secured and logically isolated from each other, which ensures security and isolation of the control path when running multiple tenants simultaneously on the shared infrastructure. Tenant Units can contain one or more MTrees, which hold all configuration elements needed in a multitenancy setup. Users, management-groups, notification-groups, and other configuration elements are part of a Tenant Unit.

How Data Domain Uses RBAC in SMT
Within Secure Multitenancy (SMT), the ability to perform a task depends on the role assigned to a user. Each user role has a unique set of permissions enforced at the infrastructure level by the DD system using role-based access control (RBAC).

Note
These roles, including Management Groups, are enforced by the Data Domain system, not DD Management Center.

admin role
A user assigned the admin role has full access to the entire DD OS command set and can perform all administrative operations on a DD system. The admin can also perform all SMT administrative operations on a DD system, including setting up SMT, assigning SMT user roles, enabling tenant self-service mode, and others. SMT commands are included in the DD OS command set. In the context of multitenancy, the admin is typically referred to as the “landlord.” In DD OS, the role is known as the “sysadmin.”

tenant-admin role
A user with a tenant-admin role can perform the designated operations only when the “Self-Service” option is enabled on the specific Tenant Unit. Responsibilities include scheduling and running a backup application for the tenant, and monitoring resources and statistics within the assigned Tenant Unit. Tenant-adms ensure administrative separation when tenant self-service mode is enabled. In the context of multitenancy, the tenant-admin role is typically referred to as the “backup admin.”
tenant-user role
The tenant-user role allows users to monitor the performance and usage of SMT components on their assigned Tenant Unit only, and only when tenant self-service is enabled. Tenant-users may run the `show` and `list` commands.

none role
A user with a role of `none` is not allowed to perform any operations on a DD system other than changing their password and accessing data using DD Boost. However, after SMT is enabled, the admin can select a user with a none role from the DD system and assign them an SMT-specific role of tenant-admin or tenant-user. Then, that user can perform operations on SMT management objects.

management groups
Backup service providers (BSPs) can use `management groups` defined in a single, external Active Directory (AD) or NIS to simplify managing user roles on Tenant Units. Each BSP tenant may be a separate, external company and may use a name-service such as AD or NIS.

With SMT management groups, the AD and NIS servers are set up and configured by the admin in the same way as SMT local users. The admin can ask their AD or NIS administrator to create and populate the group. The admin then assigns an SMT role to the entire group. Any user within the group who logs in to the DD system is logged in with the role assigned to the group.

When users leave or join a tenant company, they can be removed or added to the group by the AD or NIS administrator. There is no need to modify the RBAC configuration on a DD system when users who are part of the group are added or removed.

Use Cases for SMT

The following use case examples summarize how Secure Multitenancy (SMT) can be deployed in protection storage infrastructures.

Local Backup
In the local backup use case, a protection storage infrastructure is shared across clients and deployment is local to the enterprise. The on-premise IT staff uses each Tenant Unit to back up the data of a specific business unit.

Replicated Backup
In the replicated backup use case, the tenant performs local backups at their physical site, but does not want to own or manage a remote site for disaster recovery purposes. For this type of tenant, service providers can host multiple tenants, each replicating to their own Tenant Unit, to provide replicated backup services on a shared Data Domain backup appliance platform.

Remote Backup
In the remote backup use case, a client does not perform local backups at the physical site. Instead, the client performs direct backups over the WAN to a hosted backup IT environment managed by a service provider or a hosted provider. Remote backup is used for traditional client-based backup and application-direct backup.

Multi-User DD Boost and Storage Units in SMT

*Multi-User DD Boost* refers to the use of multiple DD Boost user credentials for DD Boost Access Control, in which each user has a separate user name and password.

A *Storage Unit* is an MTree configured for the DD Boost protocol. A user can be associated with, or “own,” one or more Storage Units. Storage Units that are owned by one user cannot be owned by another user. Therefore, only the user owning the Storage Unit can access the Storage Unit for any type of data access, such as backup/restore. The number
of DD Boost user names cannot exceed the maximum number of MTrees (current maximum is 100).

Each backup application must authenticate using its DD Boost user name and password. After authentication, DD Boost verifies the authenticated credentials to confirm ownership of the Storage Unit. The backup application is granted access to the Storage Unit only if the user credentials presented by the backup application match the user names associated with the Storage Unit. If user credentials and user names do not match, the job fails with a permission error.

Managing Tenant Users and their Privileges

There is no direct way to create a tenant user. The only way for a tenant to have users is by association with its Tenant Units. Tenant users are all users in their Tenant Units.

You can create a user with the DD System Manager (see the EMC Data Domain Operating System Administration Guide) or the Command Line Interface (CLI) (see the EMC Data Domain Operating System Command Reference Guide).

Adding a user with an association to DD Boost data access or tenant self-service using the CLI can be dangerous because of cross-tenancy issues. The CLI will not validate users belonging to other tenants when adding DD Boost data access users or tenant self-service users to the current tenant.

You can also create local users with DD Management Center. If you create a local user with a role of none using the DD System Manager or CLI, the user will appear in the DD Management Center list of available users to be added for DD Boost data access and/or tenant self-service.

Overview of Using SMT with DD Management Center

In DD Management Center, the Secure Multitenancy feature is administered by selecting Administration > Multitenancy.

The Administration Multitenancy page shows a Tenant tree on the left, from which you can create and manage tenants, Tenant Units, and provisioned storage.

Above this tree are controls to Add (green +), Edit (pencil), and Delete (red X) tenants and/or Tenant Units (depending on what is highlighted in the tree), as well as a Tenant (Unit) Details (blue i) icon that displays the Tenant (Unit) Details Lightbox (again depending on what is highlighted). You can also right-click on each node in the tree to perform these functions, as well. All of these actions are controlled by RBAC (role-based access control).

Also in the tree, each node has a control to its left, indicating its Warning or Offline status. This status rolls up to the tenant and all tenant nodes. Additionally controls for creating, editing, or deleting states are displayed while each operation is in progress. Some actions may not be allowed, depending on the different state or status of the nodes. If there are Tenant Units under a tenant with the same name, an information icon is displayed for the tenant node.

The All Tenants node is always displayed and lets you create tenant objects.

The Unmanaged node is displayed only if there are unmanaged Tenant Units available. The only actions allowed on the Unmanaged node and the Unmanaged Tenant Units are Add all to Tenant and Add to Tenant, respectively, and are available only through the right-click context menus.

To the right of the tree is a summary.

When All Tenants is selected, the summary shows the total number of tenants, Tenant Units, and host systems. You can see if any of the tenants or Tenant Units are offline or
have configuration problems in different severity panels. You can also see the number of unassigned Tenant Units.

When you select a tenant or Tenant Unit, the summary includes (depending on the item) the name, status, administrator name and email, host systems, data center location, alerts, and MTree and storage information, DD Boost Users, Tenant Self-Service information, and Report schedule and recipients.

To generate reports about tenants or individual Tenant Units, select Reports > Management.

To see the general health for tenants and Tenant Units, select Health > Status, Health > Alerts, and/or Health > Jobs.

To changed a Data Center Location, select Administration > Properties and edit the Data Center property. Note that each DD system must explicitly be assigned a value for Data Center in Administration > Systems. If a DD system has a Data Center property assigned, it will be grouped under All in the Create Tenant Unit wizard.

Using DD Management Center as a Storage Administrator in a Multitenant Environment

Storage administrators are the “landlords” for backup operators ("tenants"). Storage administrators install and configure DD system hardware and software and use DD Management Center to provision and assign storage to the tenants that they support.

Some of the tasks and goals of the storage administrator in a multitenant environment include:

- Migrate users from multiple small DD systems to one or more larger systems.
- Isolate each tenant’s data from other tenants who share storage on the same physical DD system.
- Monitor and manage the space usage and performance of each system.
- Monitor and manage the space usage by, and performance provided to, each tenant. This ensures that the storage administrator meets the requirements of the service level agreement with each tenant.
- Group together tenants with similar characteristics on the same physical system to gain more cross deduplication.
- Charge tenants based on their space usage.

Using DD Management Center as Backup Administrator in a Multitenant Environment

Backup administrators are the tenants in a secure multitenant environment. They are responsible for scheduling and managing backups and replication for their organization or department using the storage available in their Tenant Units.

Backup administrators can use DD Management Center to monitor the performance and resources of their Tenant Units, monitor replication, and generate reports.

Creating and Managing Tenants

This section describes how to create and manage tenants.

Creating Tenants

You can create tenants from the Multitenancy page.

Before you begin

Navigate to the Administration > Multitenancy page.
To create a new tenant:

Procedure
1. Highlight All Tenants in the tree, and select the Add Tenant [green plus (+) sign] control above the tree.
2. In the Create Tenant dialog, enter the following information:
   - For Tenant name [which is required, as indicated by the asterisk (*)], use the name of the client or organization that will use the storage. For example, if you are a service provider, the name might be XYZ Widget Corp. If you are a storage administrator for an organization, the name might be Finance Department.
   - For Administrator name (which is optional), enter the name of the backup administrator.
   - For Administrator email [which is required, as indicated by the asterisk (*)], enter the email address of the backup administrator. This will be used to create a default Alert Notification list.
3. Select Create.

Results
The new tenant appears in the tree.

Viewing Tenant Information and Status

You can view information about all tenants or individual tenants from the Multitenancy page.

Procedure
1. Navigate to the Administration > Multitenancy page.
2. Highlight All Tenants to see an overview of the configured tenants, important messages, and the status of multitenant reporting.
3. Highlight a specific tenant to see the backup administrator’s name and email address, important messages about the Tenant Units for this tenant, and information about reports for this tenant.
4. For much more detail about the tenant, select the Tenant Details control (the blue i just above the list of tenants) to see all of the available information about the tenant. This Tenant Details Lightbox is described in the next section.

Tenant Details Lightbox

Use the Tenant Details lightbox when you want to gather detailed operating information about a specific tenant.

The Tenant Details lightbox is accessed from the Administration > Multitenancy, using the Tenant Details control.

The Overview page has the following sections:
- **Tenant**, which includes Tenant name, Administrator, Administrator email, Tenant Units, and Systems.
- **Health**, which includes four LEDs for Alerts, File Systems, DD Boost, and Replication. These alerts can be in a Normal, Warning, or Error state. You can hover over an alert to get more information. The Tooltip on the LEDs lists the Tenant Units that have problems, along with a link to launch the related DD system for that Tenant Unit. Health LEDs can also be in a disabled state if the underlying component (that is,
Replication, DD Boost, etc.) is either not licensed or disabled on any of the DD systems of the tenant.

- **Capacity**, which includes a capacity meter that shows the current utilization, aggregate values for quota available, quota used, quota used % (based on all configured MTrees owned by the tenant), and a warning/error banner, if any of the quotas has not been enabled or configured.

- **Replication**, which includes counts for both automatic and on-demand replication pairs: total, with errors, and with unknown status.

- **Network Bytes Used**, which includes the total, backup, and restore replication bytes used.

The **Capacity** page shows Capacity Overview details with a variable meter that shows the quota (available, used, and used percentage). The Logical Space Usage chart shows plots for Pre-comp used for a selected period of time (24 Hours, 7 Days, 30 Days, 90 Days, or Custom – to set your own time period). There is also a list of Tenant Units associated with this tenant with their MTrees or Storage Units, including a severity panel with any warnings for the MTree/Storage Unit selected.

The **Replication** page shows Replication Overview details that include the total number of bytes replicated for Automatic Replication Pairs and On-Demand Replication Pairs. The Replication Trend chart shows plots for Pre-comp replicated, Post-comp replicated, and/or Compression ratio plots for a selected period of time (24 Hours, 7 Days, 30 Days, 90 Days, or Custom – to set your own time period).

The **Network** page shows Network Overview details that include the last 24 hours of backup, restored data, and total inbound and outbound replication. The Trend Analysis charts show plots for Total Network Used, Backup and Restore Bytes Used, and Replication Bytes Used for a selected period of time (24 Hours, 7 Days, 30 Days, 90 Days, or Custom – to set your own time period).

The **System Charts** page shows the system charts for the DD system of a selected Tenant Unit associated with this tenant. Desired charts can be added to the chart area (at the right) by enabling the respective check boxes. You can display Resource charts for CPU utilization and Network throughput; File system charts for Stream counts, Protocol processing, and Protocol throughput; Replication charts for Inbound/Outbound characteristics and Throughput for each type of replication. In the chart area, multiple charts are displayed vertically according to the selection. All of these charts can be displayed for a selected period of time (24 Hours, 7 Days, 30 Days, 90 Days, or Custom – to set your own time period).

### Editing Tenant Information

You can change tenant names, administrator names, and administrator email addresses using the Edit Tenant dialog.

**Before you begin**

Navigate to the **Administration > Multitenancy** page.

**Procedure**

1. In the tree, highlight the tenant that you want to update, and select the yellow pencil control above the tree.

2. In the Edit Tenant dialog, edit what you need to change, and select **Save**.

**Results**

The edited tenant will again be displayed in the tree.
Deleting Tenants

When you no longer need to provide storage for an organization, you can delete the tenant that corresponds to that organization.

Before you begin

Navigate to the Administration › Multitenancy page.

To delete a tenant:

Procedure

1. Highlight the tenant in the tree, and select the Delete Tenant (red X) control at the top of the tree.
2. In the Delete Tenant dialog, you have two options:
   - Remove all Tenant Units, which will preserve the data, so that the Tenant Unit may be assigned to another tenant. The Tenant Units will be moved to the Unmanaged Tenant Unit pool and will retain all MTrees/Storage Units associated with them.
   - Destroy all Tenant Units, which will destroy all of the Tenant Units and any MTrees and Storage Units associated with them.
3. Select Yes.

NOTICE

Deleting a tenant cannot be undone from DD Management Center, so be very careful when performing this task.

Results

The tenant has been deleted from the tree.

What to do if delete Tenant fails

When you try to delete a tenant, the operation may fail for a variety of reasons.

First, go to the Health › Jobs page, select the failed job, and observe the reason for the failure, which may include:

- The file system of one or more of the DD systems under the tenant is turned off.
- Some of the DD systems under the tenant are not reachable or are powered down.
- The DD Boost feature of one or more of the DD systems under the tenant is disabled or is not licensed.

You can manually fix these problems using both the DD System Manager and the DD Management Center command line interfaces (you need to fix them in both places, as they are DD system-related). Then, you can try to delete the tenant again using DD Management Center.

Creating and Managing Tenant Units

This section describes how to create and manage Tenant Units.

Creating a New Tenant Unit with the Wizard

You can create a Tenant Unit with the Create Tenant Unit Wizard.

Before you begin

Storage for a tenant is contained within a virtual partition called a Tenant Unit on a DD system. To assign storage to a tenant, you can use the Create Tenant Unit Wizard to
create the Tenant Unit, provision storage, and assign the Tenant Unit to a tenant. You can also create an empty Tenant Unit for a tenant and provision storage later.

Select Administration > Multitenancy. Then select a tenant, and the Add (green +) control.

You have three choices when creating a Tenant Unit:

- **Create a Tenant Unit with manual provisioning**, where you create/select the MTrees and Storage Units that will be associated with this Tenant Unit. You can also optionally create DD Boost Data Access users to go with the Storage Units.

- **Create a Tenant Unit with automatic provisioning**, where you can add new or existing DD Boost Data Access users to this Tenant Unit. This will allow backup software to create Storage Units that will be assigned to this Tenant Unit.

- **Create an empty Tenant Unit**, where you can provision the Tenant Unit later using the Edit Tenant Unit dialog.

**Procedure**

1. On the first page of the wizard, Identify Host System:
   - For **Tenant Unit name** [which is required, as indicated with the asterisk (*)], enter a unique Tenant Unit name per system.
   - For **Administrator name** (which is optional), enter the name of the backup administrator.
   - For **Administrator email** [which is required, as indicated with the asterisk (*)], enter the email address of the backup administrator. This will be used to create a default Alert Notification list.
   - For **Datacenter location** (which is optional), enter a location. The Tenant Unit will be created only on systems at this location. This is the same Data Center location from Administration > Properties. The administrator should populate the Data Center property with values (for example, Dallas, New York, etc.). When adding a system, this property should be set for the system, depending on its location (example, Dallas). After this value has been set for any system, it will show up in the drop-down list here (Create Tenant Unit). Selecting it will then filter and show all systems based on only that Data Center location property.
   - For **Size now (GiB)** (which is optional), enter a number to filter systems that do not currently have sufficient storage capacity.
   - For **Size to grow (GiB)** (which is optional), enter a number to filter systems that will not have sufficient capacity at a specified time in the future (set in the next field, “Time to grow”), based on capacity projections. The size to grow is actually *the size to grow to by the specified time*. For example, for a specified time of 6 months, if the size now is 1 GiB, and the size to grow is 2 GiB, in six months, the minimum capacity requirement would be 2 GiB.
   - For **Time to grow** (which is optional), enter the time after which the “Size to grow” amount of capacity should be reached.

2. On the second page of the wizard, Select Host System, you will see systems that have enough logical capacity to host the Tenant Unit:
   - **Available now** indicates systems that you can select now.
   - **Available in 6 months** is displayed if you selected 6 months in the “Time to grow” field on the previous page, or did not explicitly select a value. **Available in 12 months, Available in 18 months, or Available in 24 months** is displayed if you selected those values in “Time to grow”. For example, for a specified time of 6 months, if the size now is 1 GiB, and the size to grow is 2 GiB, in six months, the minimum capacity requirement would be 2 GiB. Any system that has a lower projected capacity will be filtered from the list. Also, any system offline at the time, as well as any collection destination system, will be filtered from the list. Also, any
systems running a version prior to DD OS 5.5.x will be filtered from the list, that is, only systems running DD OS 5.5.x or later will be listed.

- **Existing Tenant Units** displays the current number of Tenant Units on this system.
- For systems with an information (blue i) control, you can hover to see a warning message explaining why a projection cannot be made.
- For the selected system, the charts at the bottom shows historical data, including throughput for selected connection port, CPU utilization for each system, and stream count. You can use this information to determine the best system on which to create the Tenant Unit.

3. The third page of the wizard depends on your previous choice. [Note that for “Create an empty Tenant Unit”, you will just go to the final page (step 4).]

a. For manual provisioning, you can create MTrees/Storage Units.
   - MTrees/Storage Units can be added here, when creating a Tenant Unit with Manual Provisioning. You can also add then when editing a Tenant Unit.
   - You can add new MTrees or Storage Units, or select from the Existing MTrees or Storage Units on the host system.
   - You can also edit, unassign, or destroy MTrees or Storage Units from the same area.
   - If an MTree or Storage Unit selection is disallowed, you can hover the mouse over it, to see more information.

b. For automatic provisioning, you can configure users for data access over the DD Boost protocol.
   - You can add an existing local user or create a new local user and promote the local user to DD Boost user.
   - You can delete the selected DD Boost User.
   - The table contains DD Boost Data Access User names and the Storage Units count associated with the user.
   - The information panel shows when one or more users is selected.
   - The configuration is not changed until you select Create on the Summary page.
   - If there are one or more local users in the list, the first local user in the list will be selected by default. If there are no local users in the list, the “New local user” will be selected. All selected users or newly created users will automatically be default Tenant Units.
   - A warning will show if the current selected local user already has another Tenant Unit as their default Tenant Unit.
   - The first entry in the “Local user” drop-down list is “New local user”, which lets you create a new local user and add it as a DD Boost Data Access user.
   - When selecting “New local user”, the Add DD Boost Data Access User dialog will change to a create new local user form.

4. The fourth (final) page (third page for “Create an empty Tenant Unit”) of the wizard is a Summary, showing data from the previous pages.

   - The Tenant Unit is not created until you select Create.
   - You have the option to send an email to the Tenant Unit administrator on the successful creation of the Tenant Unit.
   - Creating a Tenant Unit with any sort of provisioning (not empty) will automatically generate a pair of Report Templates (Status and Usage) and schedule them.
• You may get one of two warnings: (1) You have not provisioned this Tenant Unit correctly. Add MTrees or Storage. (2) You have not provisioned this Tenant Unit correctly. Make this Tenant Unit the Default Tenant Unit for one of the DD Boost Data Access Users.

Results
The newly created Tenant Unit is added to the tree.

What to do if create Tenant Unit fails
Creating a Tenant Unit may fail for a number of reasons.

It may fail for simple reasons such as a duplicate Tenant Unit name, or it may fail if there are network/connectivity issues, sudden system state changes, etc.

Within the create process itself, there may be failures where MTrees or Storage Units may fail to get created for one or more reasons, or DD Boost users may not get created.

Creating a Tenant Unit will succeed even if the configuration of an individual component like MTrees or DD Boost users fails. So, the final components of a newly created Tenant Unit might not match your specifications.

To see the success and/or failed information for each individual task, or if there is an inconsistency in what you expected and what was created, navigate to the Health > Jobs page, which has additional messages.

You must address the reasons for failure before trying to re-create a new Tenant Unit, or you risk seeing the same failure situations again.

Viewing Tenant Unit Information and Status
You can view information about all Tenant Units from the Multitenancy page.

Before you begin
Navigate to the Administration > Multitenancy page.

To view Tenant Unit information and status:

Procedure
1. Select a Tenant Unit in the tree to view a summary page and critical alerts.
2. For more detail about the Tenant Unit, select the Tenant Unit Details (the blue i) control, at the top of the tree, to see all of the available information about the Tenant Unit. This Tenant Unit Details Lightbox is described in the next section.

Tenant Unit Details Lightbox
Use the Tenant Unit Details lightbox when you want to gather detailed operating information about a specific Tenant Unit.

The Tenant Unit Details lightbox can be accessed from the Administration > Multitenancy, Health > Status, or Health > Alerts page (Tenants View), using the Tenant Unit Details control.

The Overview page has the following sections:

• **Tenant Unit**, which includes Tenant Unit name, Administrator, Administrator email, Host System, and Data Center Location.

• **Health**, which includes four LEDs for Alerts, File Systems, DD Boost, and Replication. These alerts can be in a Normal, Warning, or Error state. You can hover over an alert to get more information. Health LEDs can also be in a disabled state if the underlying component (that is, Replication, DD Boost, etc.) is either not licensed or disabled for the DD system of the selected Tenant Unit.
- **Host System Performance Details**, which shows data flow for Throughput, CPU and Stream Count. Different network ports can be selected. Chart durations can be selected among: Last 24 Hours, 7 Days, 30 Days, 90 Days, and Custom.

- **Capacity**, which includes a capacity meter that shows the current utilization, aggregate values for quota available, quota used, quota used % (based on all configured MTrees owned by the Tenant Unit), and a warning/error banner, if any of the quotas has not been enabled or configured.

- **Replication**, which includes counts (inbound and outbound) for both automatic and on-demand replication pairs: total, with errors, and with unknown status.

- **Network Bytes Used**, which includes the total, backup, and restore replication bytes used.

The **Capacity** page shows Capacity Overview details with a variable meter that shows the quota used percentage; a Logical Space Usage chart that can be scaled to view certain periods of usage; and a list of Tenant Units with their MTrees or Storage Units, including a severity panel with any warnings for the MTree/Storage Unit selected.

The **Replication** page shows Replication Overview details that include the total number of bytes replicated for Automatic Replication Pairs and On-Demand Replication Pairs. The Replication Trend chart shows at least one of: Pre-comp replicated, Post-comp replicated, and Compression ratio plots in a customized time plot.

The **Network** page shows Network Overview details that include the last 24 hours of backup, restored data, and total inbound and outbound replication. The Trend Analysis shows charts that can be viewed for a certain period by selecting one of the four options (24 Hours, 7 Days, 30 Days, 90 Days) or by selecting Custom, which lets you select a different time frame.

The **System Charts** page shows the system charts for the DD system of the selected Tenant Unit. Desired charts can be added to the chart area (at the right) by enabling the respective check boxes. You can display Resource charts for CPU utilization and Network throughput; File system charts for Stream counts, Protocol processing, and Protocol throughput; Replication charts for Inbound/Outbound characteristics and Throughput for each type of replication. In the chart area, multiple charts are displayed vertically according to the selection.

### Editing Tenant Unit Information

You can change all types of information for a tenant unit using the Edit Tenant Unit dialog.

**Before you begin**

Navigate to the Administration > Multitenancy page.

To edit tenant unit information:

**Procedure**

1. Highlight the tenant unit in the tree, and select the **Edit Tenant Unit** (pencil) control at the top of the tree.

2. The Edit Tenant Unit dialog has the following tabs: General, Alert Notifications, DDBoost Data Access Users, MTrees, and Tenant Self-Service, which are described in the following sections.
Editing Tenant Units: General Tab

You can change administrative information for a tenant unit using the General tab in the Edit Tenant Unit dialog.

**Before you begin**

Navigate to the Administration > Multitenancy page.

**Procedure**

1. Highlight the tenant unit in the tree, and select the Edit Tenant Unit (pencil) control at the top of the tree.
2. In the General tab, you can change the following:
   - Tenant Unit Name
   - Administrator Name
   - Administrator Email – If the administrator email is modified, report templates sending reports associated with the tenant unit to that administrator need to be re-routed. After editing the administrator email, a popup appears confirming whether a change needs to be made for all report templates associated with the old email. If you select Yes, all old administrator emails will be replaced with the new value.

Editing Tenant Units: Alert Notifications Tab

You can change alert notifications for a Tenant Unit using the Alert Notifications tab in the Edit Tenant Unit dialog.

**Before you begin**

Navigate to the Administration > Multitenancy page.

Each Tenant Unit has a default alert notification list (created by the DD system) containing the administrator email. You can create new alert notification lists, edit existing lists, or delete lists associated with the Tenant Unit.

**Procedure**

1. Highlight the Tenant Unit in the tree, and select the Edit Tenant Unit (pencil) control at the top of the tree.
2. In the Alert Notifications tab, select Add.
3. In the Add Alert Notification Group dialog, enter a name for the notification group.
4. Select Add and enter the first email address.
   Optionally, continue selecting Add to enter more addresses.
5. Select the Add button at the bottom of the dialog when you are finished adding addresses, and then select OK or Apply to save your changes.

Editing Tenant Units: DD Boost Data Access Users Tab

You can create a list of users who will have data access over DD Boost to a particular Tenant Unit, using the DD Boost Data Access Users tab in the Edit Tenant Unit dialog.

**Before you begin**

Navigate to the Administration > Multitenancy page.

Multiple users can be configured for DD Boost access on a DD system. New DD Boost users are assigned the role of none. If a user has already been created with a role other than none, that user will be disabled and can only be deleted from the table.

Backup software uses a DD Boost data access user account to access storage on a DD system. Storage administrators need to configure one or more DD Boost data access
users for each Tenant Unit. Optionally, storage administrators can designate a Tenant Unit as the default Storage Unit for a DD Boost data access user. When backup software creates new Storage Units for a user, the software automatically uses the default Tenant Unit.

**Procedure**

1. Highlight the Tenant Unit in the tree, and select the Edit Tenant Unit (pencil) control at the top of the tree.
2. In the DD Boost Data Access Users tab, add, edit, or delete users, as desired.
3. Select OK or Apply to save your changes.

**Editing Tenant Units: MTrees Tab**

You can create and manage MTrees and Storage Units using the MTrees tab in the Edit Tenant Unit dialog.

**Before you begin**

Navigate to the Administration > Multitenancy page.

Note that, in addition to this method, you can also add MTrees and Storage Units when you are creating a Tenant Unit with Manual Provisioning.

**Procedure**

1. Highlight the Tenant Unit in the tree, and select the Edit Tenant Unit (pencil) control at the top of the tree.
2. In the MTrees tab, add, edit, or delete MTrees and/or Storage Units, as desired.

**Adjusting Soft/Hard Quotas for MTrees and Storage Units**

Quotas can be enabled or disabled on a host system using the command line interface (CLI) or with DD System Manager. You cannot enable or disable quotas using DD Management Center. You can adjust quotas using DD Management Center if the host system quotas have already been enabled.

**Before you begin**

The host system quotas must have already been enabled.

Navigate to the Administration > Multitenancy page.

**Procedure**

1. Highlight the Tenant Unit in the tree, and select the Edit Tenant Unit (pencil) control at the top of the tree.
2. In the MTrees tab, highlight a Storage Unit or MTree in the list, and select Edit.
3. Set the desired quota values in the Edit MTree or Edit Storage Unit dialog, and select Save.
4. Select OK or Apply to save your changes.

**After you finish**

You can also enable or disable quotas on the host system by:

1. Launch the DD System Manager, for the specific DD system, from DD Management Center.
2. Navigate to the Data Management > Quota tab.
3. Enable or disable quotas, as needed.
You can also enable or disable quotas using the CLI. See the *EMC Data Domain Operating System Command Reference Guide*.

**Editing Tenant Units: Tenant Self-Service Tab**

Tenants can perform some basic services on their own, reducing the bottleneck of always having to go through an administrator.

**Before you begin**

Navigate to the Administration > Multitenancy page.

Tenants can add, edit, or delete local users, NIS groups, and/or AD groups.

**Procedure**

1. Tenant Self-Service is disabled by default. To enable it, select the checkbox for Enable Tenant Self-Service. In the table:
   - The Type column displays management-user or management-group.
   - The Role column displays tenant-admin or tenant-user.

2. To add a self-service user, select the Add (+) control. In the Add Self-Service User dialog, select the desired local user, NIS group, or AD group, or create a new local user (there is no default). If you select New local user, the dialog will add fields for Name, Password/Confirm, and Role (tenant-admin or tenant-user).

3. To edit a self-service user, select a User or Group, and select the Edit (the pencil) control. You can change the Role from tenant-admin to tenant-user, or vice-versa.

4. To delete a self-service user, select a User or Group, and select the Delete (X) control. You will get a confirmation dialog to make sure that you definitely want to delete this user or group.

**Deleting Tenant Units and Unassigning Provisioned Storage**

You can delete Tenant Units, and if a Tenant Unit has provisioned storage, you can unassign that storage to be re-assigned later or destroy all of the data.

**Before you begin**

Navigate to the Administration > Multitenancy page.

To delete a Tenant Unit:

**Procedure**

1. Highlight the Tenant Unit in the tree, and select the Delete Tenant Unit (red X) control at the top of the tree.

2. In the Delete Tenant Unit dialog, if the Tenant Unit has provisioned storage, you have two options:
   - Unassign all storage, which retains all MTrees and Storage Units associated with the Tenant Unit and which can be re-assigned to another Tenant Unit later.
   - Destroy all storage, which deletes all MTrees and Storage Units associated with the Tenant Unit.

3. Select Yes to delete the Tenant Unit.

**NOTICE**

Deleting a Tenant Unit cannot be undone from DD Management Center, so be very careful when performing this task.
Results
The Tenant Unit has been deleted from the tree.

What to do if delete Tenant Unit fails
When you try to delete a Tenant Unit, the operation may fail for a variety of reasons.

First, go to the Health > Jobs page, select the failed job, and observe the reason for the failure, which may include:

- The file system of the DD system on which the Tenant Unit resides is turned off.
- The DD system on which the Tenant Unit resides is not reachable or is powered down.
- The DD Boost feature of the DD system on which the Tenant Unit resides is disabled or is not licensed.

You can manually fix these problems using both the DD System Manager and the DD Management Center command line interfaces (you need to fix them in both places, as they are DD system-related). Then, you can try to delete the Tenant Unit again using DD Management Center.

Adding an Unmanaged Tenant Unit to a Tenant

Working from the DD OS Command Line Interface (CLI), administrators can create Tenant Units without adding them to tenants. These Tenant Units are referred to as unmanaged. In DD Management Center, you cannot create an unmanaged Tenant Unit, but you can add an unmanaged Tenant Unit to a tenant.

Before you begin
Navigate to the Administration > Multitenancy page.

To add an unmanaged Tenant Unit (or Units) to a tenant:

Procedure
1. Select the Unmanaged node in the tree. A table is displayed on the right, which contains all unmanaged Tenant Units and the host systems on which they reside.
2. If you want to add all unmanaged Tenant Units to a tenant, right-click the Unmanaged node, and select Add all to Tenant. In the Add All Tenant Units dialog, select the tenant name, and select Add.
3. If you want to add only a specific Tenant Unit or Units to a tenant, go back to the table to select the check box or check boxes next to them. Or to select a single Tenant Unit, and see a summary about it, you can expand the Unmanaged list (if it is not already expanded), and select a single Tenant Unit.
4. At the top right, select the Add to Tenant link.
5. In the Add Tenant Unit(s) dialog, select a tenant name, and select Add. The Tenant Unit will be moved from the Unmanaged node to the selected tenant, in the tree.

After you finish
You may encounter a potential conflict when trying to assign a Tenant Unit.
Suppose you have a DD Boost user, or tenant self-service user, configured under a current unmanaged Tenant Unit. If the same user is configured to the managed Tenant Unit of tenant T2, but you want to assign the Tenant Unit to tenant T1, this is considered a conflict and is not allowed.
Creating, Editing, and Generating Multitenancy Reports

The following sections describe how to create, edit, and generate reports for Multitenancy using DD Management Center.

Creating Multitenancy Report Templates

The multitenancy template configures the daily status and usage report for tenants or Tenant Units. It can also configure schedule and email distribution.

**Before you begin**
Navigate to the Reports > Management page.

**Procedure**
1. Select Add.
2. In the Add Report Template dialog, select Multitenancy Reports and select Next.
3. Enter a name, and select a template. The template choices are Status or Usage. Choose one or more sections to include, and select Next.
4. Select a Scope (Tenant Unit or Tenant). The SMT Status report is always configured to show the last 24 hours of historical data, and you can select the Report retention (Forever, 7 days, 30 days, 90 days). The SMT Usage report (which is generated as an Excel spreadsheet) lets you display data for a full month or a full week, and you can select the day of the week/month for it to start (by selecting Edit). Report generation time will be two hours ahead of Starts On time.
5. For the Tenant Unit report template, the Tenant Unit admin emails will be added by default. For the tenant report template, the tenant admin email will be added by default. You can manually add or remove these emails.
6. Review the details, and then select whether to run the report immediately and/or to save the template for later use. Select Finish.

**Results**
After it has been created, the report multitenancy template is added as an entry in the reports table. When selected, the template can be used to immediately run a report, or it can be edited or deleted, or the time it was last run can be displayed.

Editing Report Templates

A report template can be reconfigured using the Edit control. The report’s content, schedule, and email distribution can be modified in the template.

**Before you begin**
Navigate to the Reports > Management page.

**Procedure**
1. Select a template, and select the Edit (pencil) control. In the Edit Report dialog, you can select from three tabs.
2. In the Content tab, the template name can be renamed and template sections can be re-selected for the report. Note that the template, itself, is not editable.
3. In the Scope tab, the template scope and schedule can be changed. The report template can be changed from a tenant report to a Tenant Unit report or from a Tenant Unit report to a tenant report. For the daily status report template, the schedule can be changed only to daily time. For the usage report template, the time span can be
weekly or monthly. If time span is weekly, only weekly can be scheduled for start on time, and if time span is monthly, only monthly time can be scheduled for start on time. Both daily status and usage report templates can modify the report retention period (Forever, 7 days, 30 days, 90 days).

4. In the Email tab, emails can be manually added or removed from the When report is finished list or/and from the If an error occurs list.

Generating Reports

A report can be generated after the last step of the create report wizard or, as described below, by selecting a report template listed in the Template name table, and selecting Run Report.

Before you begin

Navigate to the Reports > Management page.

Procedure

1. Select a report template from the list.
2. Right-click on the name, and select Run Report.

Results

A report (named by concatenating the data stamp to the template title) is created and opened as a PDF file in your browser, except for the Tenant Usage report, which generates an Excel file.

The report generation information is listed in the Report History table, where it can be viewed, renamed, or deleted.
CHAPTER 6
Performing Advanced Configuration

This chapter describes how to configure settings for DD Management Center that are necessary for it to work in your environment. It includes these sections:

- Managing Network Settings ................................................................. 66
- Managing General Configuration Settings ......................................... 75
- Managing Access to DD Management Center ................................. 82
- Viewing Active Users ......................................................................... 96
- Performing DD Management Center Software Upgrades ............... 97
- Managing System Logs ....................................................................... 98
- Managing Alerts .................................................................................. 98
- Managing Autosupport Reporting ....................................................... 100
Managing Network Settings

The Administration > Settings > Network page presents status and configuration information for network interfaces, settings, and routes, accessible by tabs. By default, the Interfaces tab initially displays. Use this area to configure networking for the DD Management Center.

Configuring Network Interfaces

This section describes how to configure physical network connections and how to create VLANs and IP aliases for DD Management Center.

Viewing Interface Information

The Interfaces page (Administration > Settings > Network tab > Interfaces tab) lets you manage and configure the physical (Ethernet) interface, DHCP, DDNS, and IP addresses, and displays network information and status.

There are two parts to this page: the Interfaces area and the Interface Details area.

Table 4 Interfaces Area

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of each Ethernet interface associated with DD Management Center. Physical interfaces names start with eth.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Lets you view or change status of the interface.</td>
</tr>
<tr>
<td></td>
<td>• Select Yes to enable interface and connect it to the network.</td>
</tr>
<tr>
<td></td>
<td>• Select No to disable interface and disconnect it from the network.</td>
</tr>
<tr>
<td>DHCP</td>
<td>Indicates whether the interface is configured with an IP address from a DHCP (Dynamic Host Configuration Protocol) server.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address associated with the interface, which is used by the network to identify the interface. If the interface is configured through DHCP, an asterisk appears after this value.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Netmask associated with the interface. Uses the standard IP network mask format. If the interface is configured through DHCP, an asterisk appears after this value.</td>
</tr>
<tr>
<td>Link</td>
<td>Indicates whether the interface currently has a live Ethernet connection.</td>
</tr>
<tr>
<td>Additional Info</td>
<td>Provides additional settings for the interface, for example, the bonding mode.</td>
</tr>
</tbody>
</table>

To populate the Interface Details area, select an interface.

Table 5 Interface Details Area

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Name of selected interface.</td>
</tr>
</tbody>
</table>
### Table 5 Interface Details Area (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Address</td>
<td>MAC address of selected interface, for example, 00:02:b3:b0:8a:d2</td>
</tr>
<tr>
<td>Cable</td>
<td>Indicates whether interface is Copper.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transfer Unit value assigned to interface.</td>
</tr>
<tr>
<td>Auto Negotiate</td>
<td>Indicates whether interface is enabled to automatically negotiate Speed and Duplex settings. If it is disabled, then Speed and Duplex values are manually set.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Protocol used with Speed value, which sets data transfer protocol. Values are Unknown, Full, or Half.</td>
</tr>
<tr>
<td>Speed</td>
<td>Protocol used with Duplex value, which sets rate of data transfer. Values are Unknown, 10 Mb/s, 100 Mb/s, 1000 Mb/s, or 10 Gb/s.</td>
</tr>
<tr>
<td>Supported Speeds</td>
<td>Lists all speeds the interface is capable of using.</td>
</tr>
</tbody>
</table>

### Filtering the Interfaces Table

To filter the Interfaces table:

**Procedure**

1. Enter a value in the Interface Name field or select a value from the Interface Type menu. The value All displays physical, VLAN, and IP Alias interfaces.
2. Select Update.
3. To return the interfaces table to the default listing, select Reset.

### Configuring Physical Interfaces

**Procedure**

1. On the Interfaces page, select an interface to configure from the Interface list, and select Configure.
2. In the Configure Interface dialog, decide how the interface IP address is to be set:
   - **Obtain IP Address using DHCP.** Setting a physical interface to DHCP automatically enables the interface.
   - **Manually configure IP Address.** The IP Address and Netmask fields become active.
     - Enter an IP Address.
     - Enter a Netmask address. The format is typically 255.255.255.000. If you do not specify a netmask, DD Management Center uses the netmask format determined by your TCP/IP address class (A,B,C).
   - The combination of speed and duplex settings defines the rate of data transfer through the interface. Select one of these options:
• **Autonegotiate Speed/Duplex**
  The network interface card will autonegotiate the line speed and duplex setting for an interface. Optical interfaces require the autonegotiate option.

• **Manually configure Speed/Duplex** –
  The Speed and Duplex fields become active.
  - Select a speed, which is limited to the capabilities of the hardware device.
  - Select half-duplex or full-duplex or unknown.

4. Specify the MTU (Maximum Transfer Unit) size for the physical (Ethernet) interface.
   Supported values are from 350 to 9014. Ensure that all of your network components support the size set with this option. The default is 1500 (and the Default button will return it to that value).

5. Select **Next**.

6. In the summary, confirm that the values listed reflect the new system and interface state, and if so, select **Finish** and **OK**. If not, select **Back** and redo your settings.

**Configuring a VLAN**

This procedure shows you how to create a new VLAN interface from a physical interface. The recommended total number of VLAN interfaces that can be created is 80. However, it is possible to create up to 100 interfaces (minus the number of aliases and physical interfaces) before the system prevents any more from being created.

**Procedure**

1. On the Interfaces tab (Administration > Settings > Network), from the Create menu, select the **VLAN** option.

2. In the Create VLAN dialog, specify a VLAN Id. The range of a VLAN ID is between 1 and 4094 inclusive.

3. Enter an IP Address.

4. Enter a Netmask address.
   If you do not specify a netmask, the DD system uses the netmask format determined by your TCP/IP address class (A,B,C).

5. Specify MTU Settings, which set the Maximum Transfer Unit size for the physical (Ethernet) interface. Supported values are from 350 to 9014. For 100 Base-T and gigabit networks, 1500 is the standard default. Make sure that all of your network components support the size set with this option. The Default button returns the setting to the default value.

6. Select **Next** to see a summary of your new values.

7. On the summary page, review the new values, and select **Back** if you want to change any of these values.

8. When you are done, select **Finish** and **OK**.

**Modifying a VLAN Interface**

To modify settings on an existing VLAN interface:
Procedure
1. Select the check box of the interface, and disable the VLAN interface by selecting No in the Enabled column. Then, select OK in the warning dialog.
2. Again select the check box of the (now disabled) interface, and select the Configure button.
3. In the Configure VLAN Interface dialog, change any settings.
4. Select Next and Finish.

Creating an IP Alias Interface
You can create a new IP Alias interface from a physical or VLAN interface.
It is recommended that the total number of IP Alias, VLAN, and physical interfaces not exceed 80, although it is possible to have up to 100.

Procedure
1. Select an interface, and choose the IP Alias option from the Create drop-down menu.
2. In the Create IP Alias dialog, enter a number for the IP Alias ID. This number can be from 1 to 4094, inclusive.
3. Enter an IP Address.
4. Enter a Netmask address. The format is typically 255.255.255.000. If you do not specify a netmask, the format is determined by the TCP/IP address class (A,B,C) in use.
5. Specify the Dynamic DNS Registration option. (This option is available only if DDNS has been registered.) Dynamic DNS (DDNS) is the protocol that allows machines on a network to communicate with, and register their IP address on, a Domain Name System (DNS) server.
6. Select Next.
7. Review the summary of your changes, and select Back to adjust anything, or select Finish and OK.

Modifying an IP Alias Interface
To modify settings on an existing IP Alias interface:

Procedure
1. Select the check box of the interface, and disable the IP Alias interface by selecting No in the Enabled column. Then, select OK in the warning dialog.
2. Again select the check box of the (now disabled) interface, and select the Configure button.
3. In the Configure IP Alias dialog, change any setting.
4. Select Next and Finish.

Destroying an Interface
Destroying an interface applies to VLAN and IP Alias interfaces. Destroying a VLAN deletes the VLAN and all IP Alias interfaces that are created under it, if any. Destroy IP Alias deletes only that alias interface.
To destroy an Interface:
Procedure
1. In the Interfaces list, click the box next to the interface to destroy (VLAN or IP Alias).
2. Click Destroy.
3. In the Confirm Destroy dialog box, click OK.

Viewing an Interface Hierarchy
To view an interface hierarchy:
Procedure
1. On the Interfaces tab, select Tree View.
2. In the Tree View dialog, select the plus or minus boxes to expand or contract the tree view, which shows the hierarchy.
3. Select Close to exit the Tree View.

Configuring Network Settings
Use the Settings tab on the Network page to view and configure the network settings.

Viewing Network Settings
Procedure
1. Navigate to Administration > Settings > Network tab > Settings tab.
2. On the Settings page, view the network settings (described in the following table), and add or remove settings using the Edit button.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Settings</td>
<td></td>
</tr>
<tr>
<td>Host Name</td>
<td>Host name of selected DD system</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Fully qualified domain name associated with selected DD system</td>
</tr>
<tr>
<td>Search Domain List</td>
<td>List of search domains used by DD system. The DD system applies the search domain as a suffix to the host name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of host to resolve</td>
</tr>
<tr>
<td>Host Name</td>
<td>Host names associated with IP address</td>
</tr>
<tr>
<td>DNS List</td>
<td></td>
</tr>
<tr>
<td>DNS IP Address</td>
<td>Current DNS IP addresses associated with selected DD system. An asterisk (*) means the IP addresses were assigned through DHCP.</td>
</tr>
</tbody>
</table>

Setting Host Names
Both the host name and domain name are used by other systems when they want to access DD Management Center. The host name can be set manually or automatically generated with DHCP.
Note the following before setting a host or domain name:

- Do not include an underscore in the host name. It is incompatible with some browsers.
- Changing the names of an active host can cause: (1) a break in the current connection – if this happens, log back in and check the saved settings. (2) disruption of communication with managed DD systems.

**Procedure**

1. Navigate to Administration > Settings > Settings tab, and select Edit in the Host Settings area.
2. In the Configure Host dialog, decide how to set the host and domain names.
   - Obtain Settings using DHCP. (At least one of the network interfaces must be configured using DHCP.)
   - Manually configure host.
     - Enter a host name.
     - Enter a domain name, which is the domain name associated with DD Management Center. Typically, this is your company domain name. For example, yourcompany.com
3. Select OK.

**Managing a Domain Search List**

This section describes how to add and remove a domain from a domain search list.

**Adding a Search Domain**

**Procedure**

1. Select Edit in the Search Domain List area.
2. In the Configure Search Domains dialog, select the add (+) button.
   - In the Add Search Domain dialog, enter a name in the Search Domain text box.
   - Select OK.
3. Select OK.

**Results**

Changes are applied to the system. The system returns you to the Settings view.

**Removing a Search Domain**

**Procedure**

1. Select Edit in the Search Domain List area.
   - In the Configure Search Domains dialog, select the search domain to remove.
   - Select the remove (X) button.
2. Select OK.

**Results**

Changes are applied to the system. The system returns you to the Settings tab.

**Mapping Hosts**

Use the Hosts Mapping area to add a mapping that ties an IP address to a host name.
Adding a Hostname Mapping

Procedure
1. Select Add in the Hosts Mapping area to create a host mapping.
2. If no hosts are listed in the Host Name list, select the add (+) button.
3. In the Add Host dialog, enter a hostname that will be used for the mapping in the Host Name text box.
4. Select OK.
   The new hostname is added to the list of Host Names. Continue to add host names as necessary.
5. In the Add Hosts dialog, enter the IP address that will be mapped to a host, then select check boxes of one or more host names from the list of hosts.
6. Select OK.
   The mapping is created, and you are returned to the Settings tab.

Deleting a Hostname Mapping

Procedure
1. In the Settings view, select the checkbox of the host mapping to delete in the Hosts Mapping area.
2. Select Delete in the Hosts Mapping area.
   The Delete Host dialog appears.
3. Select Delete.
   Confirmation messages are displayed.
4. Select Close when the Completed message appears.
   You are returned to the Settings tab.

Managing DNS IP Addresses

This section describes how to add and remove a DNS IP address.

Adding a DNS IP Address

Procedure
1. Select Edit in the DNS List area.
2. In the Configure DNS dialog, determine the method for obtaining the DNS. Choose to either:
   - Obtain DNS Settings using DHCP. (At least one interface must be configured using DHCP.)
   - Manually configure DNS:
     ▪ Select the plus (+) button.
     ▪ Enter the DNS IP address.
     ▪ Select OK.
Deleting a DNS IP Address

Procedure
1. Select the Manually configure DNS radio button.
2. Select the checkbox of the DNS IP address to delete.
3. Select the delete (X) button.
4. Select OK.

Configuring Routes

Routes determine the path taken to transfer data to and from the localhost (DD Management Center) to another network or host.

DD Management Center does not generate or respond to any of the network routing management protocols (RIP, EGRP/EIGRP, and BGP) in any way. The only routing implemented on DD Management Center is based upon the internal route table, where the administrator may define a specific network or subnet that a physical interface (or interface group) uses.

DD Management Center uses source-based routing, which means that outbound network packets that match the subnet of multiple interfaces will only be routed over the physical interface from which they originated.

Note
The routing for connections initiated from DD Management Center (such as for replication) depend on the source address used for interfaces using the same subnet. To force traffic for a specific interface to a specific destination (even if that interface is on the same subnet as other interfaces), a static routing entry between two systems can be configured and will override source routing.

Viewing Route Information

Procedure
1. Navigate to Administration > Settings > Network tab > Routes tab.
2. On the Routes page, view the configured static and dynamic routes (described in the following table), and create or modify routing information.

Table 7 Route Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Routes</td>
<td>Static routes that are either network or host-based routes.</td>
</tr>
<tr>
<td>Route Spec</td>
<td>Route specification being used to configure routes.</td>
</tr>
<tr>
<td>Dynamic Routes</td>
<td>Dynamically assigned routes that use network or host paths for data transmission.</td>
</tr>
<tr>
<td>Destination</td>
<td>Destination host/network where the network traffic (data) is sent.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Address of the router in the DD Management Center network or 0.0.0.0 if no gateway is set.</td>
</tr>
<tr>
<td>Genmask</td>
<td>Netmask for the destination net. Initially set to 255.255.255.255 for a host destination and 0.0.0.0 for the default route.</td>
</tr>
</tbody>
</table>
Table 7 Route Information (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>Possible values include:</td>
</tr>
<tr>
<td></td>
<td>U – Route is up.</td>
</tr>
<tr>
<td></td>
<td>H – Target is a host.</td>
</tr>
<tr>
<td></td>
<td>G – Use gateway.</td>
</tr>
<tr>
<td></td>
<td>R – Reinstate route for dynamic routing.</td>
</tr>
<tr>
<td></td>
<td>D – Dynamically installed by daemon or redirect.</td>
</tr>
<tr>
<td></td>
<td>M – Modified from routing daemon or redirect.</td>
</tr>
<tr>
<td></td>
<td>A – Installed by addrconf.</td>
</tr>
<tr>
<td></td>
<td>C – Cache entry.</td>
</tr>
<tr>
<td></td>
<td>! – Reject route.</td>
</tr>
<tr>
<td>Metric</td>
<td>Distance to target (usually counted in hops). (It is not used by the DD OS, but might be needed by routing daemons.)</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transfer Unit (MTU) size for physical (Ethernet) interface.</td>
</tr>
<tr>
<td>Window</td>
<td>Default window size for TCP connections over this route.</td>
</tr>
<tr>
<td>IRTT</td>
<td>Initial RTT (Round Trip Time). The kernel uses this to estimate the best TCP protocol parameters without waiting on (possibly slow) answers.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface name associated with routing interface.</td>
</tr>
</tbody>
</table>

Setting the Default Gateway

Procedure
1. Select **Edit** in the Default Gateway area.
2. In the Configure Default Gateway dialog, choose how the gateway address is set. Choose either:
   - **Use DHCP value**
     Dynamic Host Configuration Protocol (DHCP) indicates if the gateway is configured using a value from DHCP server.
   - **Manually Configure**
     The Gateway address box becomes available.
     - Enter the gateway address in the Gateway field.
3. Select **OK**.
   The system processes the information and returns you to the Routes tab.

Creating Static Routes

Procedure
1. Select **Create** in the Static Routes area.
2. In the Create Static Routes dialog, select an interface, and select **Next**.
3. Specify the Destination by selecting either of the following:
   - The Network Address and Netmask – Choose **Network** and enter the destination network address and netmask.
Note
This is not the IP address of a network, nor of an interface. The interface is selected in the initial dialog, and it is used for routing traffic.

- The hostname or IP address of host destination – Choose Host and enter the hostname or IP address of the destination host of the route.
- Optionally, change the gateway for this route – Enter a gateway address in the Gateway field.

4. Review changes, and select Next.
5. Select Finish.
   Progress messages display. When changes are applied, the message indicates Completed.
6. Select OK to close the dialog.
   The new route specification is listed in the Route Spec list.

Deleting Static Routes

Procedure
1. In the Route Spec area, select the checkbox of the route specification to delete.
2. Select Delete.
   The Delete Route dialog appears.
3. Select Delete and Close.
   The selected route specification is removed from the Route Spec list.

Managing General Configuration Settings

The general configuration settings you can work with include those for the identifying the mail server to use, how time and date are obtained, some general system properties, and settings related to SNMP.

Configuring Mail Server Settings

To configure a mail server:

Procedure
1. Navigate to Administration > Settings, and select the General and Mail Server tabs.
2. From the More Tasks menu, select Set Mail Server.
3. In the Set Mail Server dialog, enter the name of the mail server, and select OK.

Configuring Time and Date Settings

The Time and Date Settings tab presents the current DD Management Center date and time, shows whether NTP is enabled or not, and provides the IP addresses or hostnames of configured NTP servers.

To configure time and date settings:

Procedure
1. On the Time and Date Settings page, select Configure Time Settings from the More Tasks menu.
2. In the Configure Time Settings dialog, select the Time Zone drop-down list, and select the timezone where DD Management Center resides.

3. Set how time is synchronized:
   - To manually set the time and date, select the None radio button, and enter the date in the text box, and use the drop-down lists to set the time.
   - To use NTP to synchronize the time, select the NTP radio button. Set how the NTP server is accessed:
     - To use DHCP to automatically select a server, and select the Obtain NTP Servers using DHCP radio button.
     - To configure an NTP server IP address, select the Manually Configure radio button, add the IP address of the server, and select OK.

4. Select OK.

Configuring System Properties

The System Properties tab displays the location of the system, the administrator email address, and the administrator hostname.

To configure system properties:

Procedure

1. On the System Properties page, select Set System Properties from the More Tasks menu.
2. In the Set System Properties dialog, in the Location text field, enter information about where the DD Management Center is located.
3. In the Admin Email text field, enter the email address of the DD Management Center system administrator.
4. In the Admin Host, enter the name of the administration server.
5. Select OK.

Working with SNMP

To monitor DD Management Center using SNMP, you will need to install the Data Domain MIB in your SNMP Management system. The Data Domain MIB will allow SNMP queries for Data Domain-specific information.

DD Management Center also supports the standard MIB-II so you can also query MIB-II statistics for general data such as network statistics. For full coverage of available data you should use both the Data Domain MIB and the standard MIB-II MIB.

DD Management Center supports SNMP V2C and/or SNMP V3. SNMP V3 provides a greater degree of security than V2C by replacing cleartext community strings (as a means of authentication) with user-based authentication using either MD5 or SHA1. Also with SNMP V3, user authentication packets can be encrypted and their integrity verified with either DES or AES.

The default port that is open when SNMP is enabled is port 161. Traps are sent out through port 162.

Checking SNMP Status and Configuration

Navigate to the Administration > Settings > General tab > SNMP tab.

The SNMP page shows SNMP status and properties, and the SNMP V3 and SNMP V2C Configuration.
### Table 8 SNMP Status

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Operational status of the SNMP agent on DD Management Center: Enabled or Disabled.</td>
</tr>
</tbody>
</table>

### Table 9 SNMP Properties

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP System Location</td>
<td>Location of DD Management Center.</td>
</tr>
<tr>
<td>SNMP System Contact</td>
<td>Administrator for DD Management Center.</td>
</tr>
</tbody>
</table>

### Table 10 SNMP V3 Configuration

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Users</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of the user on the SNMP manager with access to the agent for DD Management Center.</td>
</tr>
<tr>
<td>Access</td>
<td>Access permissions for the SNMP user:</td>
</tr>
<tr>
<td></td>
<td>• Read-only</td>
</tr>
<tr>
<td></td>
<td>• Read-write</td>
</tr>
<tr>
<td>Authentication Protocols</td>
<td>Authentication protocol for validating SNMP user:</td>
</tr>
<tr>
<td></td>
<td>• MD5</td>
</tr>
<tr>
<td></td>
<td>• SHA1</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td>Privacy Protocol</td>
<td>Encryption protocol for validating SNMP user:</td>
</tr>
<tr>
<td></td>
<td>• AES</td>
</tr>
<tr>
<td></td>
<td>• DES</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td>Trap Hosts</td>
<td></td>
</tr>
<tr>
<td>Host</td>
<td>IP address or domain name of the SNMP management host.</td>
</tr>
<tr>
<td>Port</td>
<td>Port used for SNMP trap communication with the host. Port 162 is the default.</td>
</tr>
<tr>
<td>User</td>
<td>User on trap host authenticated to access Data Domain SNMP information.</td>
</tr>
</tbody>
</table>
SNMP V3 Configuration

Table 11 SNMP V2C Configuration

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communities</td>
<td></td>
</tr>
<tr>
<td>Community</td>
<td>Name of the community, for example, public, private, or localCommunity.</td>
</tr>
<tr>
<td>Access</td>
<td>Access permission assigned. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Read-only</td>
</tr>
<tr>
<td></td>
<td>• Read-write</td>
</tr>
<tr>
<td>Hosts</td>
<td>The hosts in this community.</td>
</tr>
<tr>
<td>Trap Hosts</td>
<td>Systems designated to receive SNMP traps generated by DD Management Center.</td>
</tr>
<tr>
<td></td>
<td>If this parameter is set, systems receive alert messages, even if the SNMP agent is disabled.</td>
</tr>
<tr>
<td>Port</td>
<td>Port used for SNMP trap communication with the host. Port 162 is the default.</td>
</tr>
<tr>
<td>Community</td>
<td>Name of the community, for example, public, private, or localCommunity.</td>
</tr>
</tbody>
</table>

Enabling or Disabling SNMP

Procedure
1. In the Status area, select **Enable** to use SNMP.
2. In the Status area, select **Disable** to stop using SNMP.

Downloading the SNMP MIB

Procedure
1. In the Status area, select **Download MIB file**.
2. In the Opening DATA_DOMAIN.mib dialog, select **Save**.

Configuring SNMP Properties

Procedure
1. In the SNMP Properties area, select **Configure**.
2. In the SNMP Configuration dialog, in the text fields, add an SNMP system location (a description of where DD Management Center is located) and/or an SNMP system contact (for example, the email address of the system administrator for DD Management Center).
3. Select **OK**.

Managing SNMP V3 Users

Procedures for managing V3 users including creating, modifying, and removing user accounts. Users on the SNMP manager have access to the agent for DD Management Center.
Creating SNMP V3 Users

Procedure
1. In the SNMP Users area, select Create.
   The Create SNMP User dialog appears.
2. In the Name text field, enter the name of the user or the SNMP manager who will have access to the agent for DD Management Center. The name must be a minimum of 8 characters.
3. Select either read-only or read-write access for this user.
4. To authenticate the user, select the checkbox for Authentication.
   a. Select either the MD5 or the SHA1 protocol.
   b. Enter the authentication key in the Key text field.
   c. To provide encryption to the authentication session, click the checkbox next to Privacy.
   d. Select either the AES or the DES protocol.
   e. Enter the encryption key in the Key text field.
5. Select OK.
   The newly added user account appears in the SNMP Users table.

Modifying SNMP V3 Users

Procedure
1. In the SNMP Users area, select a check box for the user, and select Modify.
   The Modify SNMP User dialog appears. Add or change any of the following settings.
2. Select either read-only or read-write access for this user.
3. To authenticate the user, select the check box for Authentication.
   a. Select either the MD5 or the SHA1 protocol.
   b. Enter the authentication key in the Key text field.
   c. To provide encryption to the authentication session, click the checkbox next to Privacy.
   d. Select either the AES or the DES protocol.
   e. Enter the encryption key in the Key text field.
4. Select OK.
   The new settings for this user account appear in the SNMP Users table.

Removing SNMP V3 Users

Procedure
1. In the SNMP Users area, select a check box for the user, and select Delete.
   The Delete SNMP Users dialog box appears.
2. Verify the user name to be deleted, and select OK.
Managing SNMP V3 and V2C Trap Hosts

Managing SNMP V3 and V2C trap hosts includes creating, modifying, and removing hosts that received SNMP traps.

Creating SNMP V3 and V2C Trap Hosts

Procedure
1. In the SNMP V3 Trap Hosts or SNMP V2C Trap Hosts area, select Create.
   The Create SNMP [V3 or V2C] Trap Hosts dialog appears.
2. In the Host text field, enter the IP address or domain name of the SNMP Host where traps will be sent.
3. In the Port text field, enter the port number for sending traps (port 162 is commonly used).
4. Select the user (SNMP V3) or the community (SNMP V2C) from the drop-down menu.
   Alternately, from the drop-down menu select Create New User (SNMP V3) to add an SNMP user, or Create New Community (SNMP V2C) to add an SNMP community.
5. Select OK.

Modifying SNMP V3 and V2C Trap Hosts

Procedure
1. In the Trap Hosts area (either for V3 or V2C), select a Trap Host entry and select Modify.
   The Modify SNMP [V3 or V2C] Trap Hosts dialog appears. Modify any of the following items.
2. In the Port text field, enter the port number for sending traps (port 162 is commonly used).
3. Select the user (SNMP V3) or the community (SNMP V2C) from the drop-down menu.
4. Select OK.

Removing SNMP V3 and V2C Trap Hosts

Procedure
1. In the Trap Hosts area (either for V3 or V2C), select a trap host entry, and select Delete.
   The Delete SNMP [V3 or V2C] Trap Hosts dialog appears.
2. Verify the host name to be deleted, and select OK.
3. In the Delete SNMP [V3 or V2C] Trap Hosts Status dialog, select Close.
   The trap host entry is removed from the Trap Hosts table.
Managing SNMP V2C Communities

**Note**

The Community string is sent in cleartext and is very easy to intercept. If this occurs, the interceptor can retrieve information from devices on your network, modify their configuration, and possibly shut them down. Instead, using the SNMP V3 Users configuration provides authentication and encryption to avoid this.

Creating SNMP V2C Communities

**Procedure**

1. In the Communities area, select **Create**.
   
The Create SNMP V2C Community dialog appears.

2. In the Community text field, enter the Community name of the SNMP manager who will have access to the agent for DD Management Center. The Community name must be a minimum of 8 characters.

3. Select either read-only or read-write access for this community.

4. In the Hosts area, select the check box of a host in the list, or:
   
   a. Select + to add a host.
      
      The Host dialog appears.

   b. In the Host text field, enter the IP address or domain name of the host.

   c. Select OK.

   The Host is added to the host list.

5. Select **OK**.

The new community entry appears in the Communities table.

Modifying SNMP V2C Communities

**Procedure**

1. In the Communities area, select a check box for the community, and select **Modify**.

   The Modify SNMP V2C Community dialog appears. Add or change any of the following settings.

2. Select either read-only or read-write access for this community.

3. In the Hosts area, select the check box of a new host in the list, or:

   a. Select + to add a host.
      
      The Host dialog appears.

   b. In the Host text field, enter the IP address or domain name of the host.

   c. Select OK.

   The Host is added to the host list.

4. Select OK.

The modified community entry appears in the Communities table.
Deleting SNMP V2C Communities

Procedure

1. In the Communities area, select a check box for the community, and select Delete.

   The Delete SNMP V2C Communities dialog appears.

   **Note**

   If the Delete button is disabled, the selected community is being used by one or more trap hosts. Delete the trap hosts, and then delete the community.

2. Verify the community name to be deleted, and select OK.

3. In the Delete SNMP V2C Communities Status dialog, select Close. The community entry is removed from the Communities table.

Managing Access to DD Management Center

Access management includes viewing and configuring the services that provide administrator and user access to DD Management Center.

Roles Required for DD Management Center Tasks

**Note**

Since mutual trust is established between DD Management Center and the DD systems that it manages, if a user is added to DD Management Center with “admin” level access, that user can also access the managed DD systems (through ssh or by launching DD System Manager) to perform admin-level operations. Also, an admin-level user can perform an upgrade operation on a managed DD system. Therefore, you should give each new DD Management Center user the same consideration that you would a new DD System Manager user.

The ability to perform tasks on a DD Management Center page is role-based, and the roles available in DD Management Center are the same as those in DD System Manager:

- “admin”, that is, the **DD Management Center Administrator**. The admin can access all functions on a DD Management Center page.
- “user”, that is, a **DD Management Center User**. A user, which can be a stand-alone user or part of a group, has access to only certain functions on a DD Management Center page, based on the role assigned to that user or group.

The following table shows the actions available for each feature of DD Management Center. [This table is mainly provided to show when only the “user” role is required. The “admin” role can perform all tasks, as previously mentioned.]

<table>
<thead>
<tr>
<th>Action</th>
<th>Minimum Permission</th>
<th>Description of Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage permissions</td>
<td>DD Management Center Administrator</td>
<td>Assign, edit, remove permissions for users</td>
</tr>
<tr>
<td>Manage DD systems</td>
<td>DD Management Center Administrator</td>
<td>Add, edit, delete systems from the inventory</td>
</tr>
<tr>
<td>Manage users / user groups</td>
<td>DD Management Center Administrator</td>
<td>Add, edit, delete local users and AD/NIS user groups</td>
</tr>
</tbody>
</table>
Table 12 Roles Required for DD Management Center Tasks (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Minimum Permission</th>
<th>Description of Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure DD Management Center</td>
<td>DD Management Center Administrator</td>
<td>Work with DD Management Center Administration &gt; Settings pages</td>
</tr>
<tr>
<td>Upgrade DD systems</td>
<td>DD Management Center User/Administrator on the system to upgrade</td>
<td>Run the DD System Upgrade function</td>
</tr>
<tr>
<td>Upgrade DD Management Center</td>
<td>DD Management Center Administrator</td>
<td>Run the DD Management Center Upgrade function</td>
</tr>
<tr>
<td>Manage groups</td>
<td>DD Management Center Administrator</td>
<td>Create, edit, delete groups</td>
</tr>
<tr>
<td>Manage properties</td>
<td>DD Management Center Administrator</td>
<td>Create, edit, delete properties</td>
</tr>
<tr>
<td>Assign properties</td>
<td>DD Management Center Administrator</td>
<td>Assign properties to DD systems</td>
</tr>
<tr>
<td>Assign to groups</td>
<td>DD Management Center Administrator</td>
<td>Assign DD systems to groups</td>
</tr>
<tr>
<td>Manage reports</td>
<td>DD Management Center Administrator</td>
<td>Create report templates and schedule report creation</td>
</tr>
<tr>
<td>Manage dashboard widgets</td>
<td>DD Management Center Administrator</td>
<td>Create dashboard widgets</td>
</tr>
<tr>
<td>Configure dashboard</td>
<td>DD Management Center Administrator</td>
<td>Configure widgets and dashboard layouts</td>
</tr>
<tr>
<td>Manage global filter rules</td>
<td>DD Management Center User</td>
<td>Add, edit, delete filter rules</td>
</tr>
<tr>
<td>Launch DD System Manager</td>
<td>DD Management Center User</td>
<td>Launch the virtual DD System Manager [note that Administrator privilege is required on the managed DD system to change anything]</td>
</tr>
<tr>
<td>Manage user jobs</td>
<td>DD Management Center User</td>
<td>Suspend, resume, cancel jobs owned by user</td>
</tr>
<tr>
<td>Manage all jobs</td>
<td>DD Management Center Administrator</td>
<td>Suspend, resume, cancel any job</td>
</tr>
<tr>
<td>Manage advanced replication</td>
<td>DD Management Center Administrator</td>
<td>View replication status, export to CVS file, assign properties</td>
</tr>
<tr>
<td>Manage basic replication</td>
<td>DD Management Center User</td>
<td>View replication status, export to CVS file</td>
</tr>
</tbody>
</table>

Managing Administrator Access

Administrator Access provides settings to configure how users can connect to DD Management Center.

Each protocol is configured separately, using the procedures in this section.

Viewing Administrator Access

Procedure

1. Navigate to Administration > Settings > Access tab > Administrator Access tab.
2. On the Administrator Access page, you can view the Passphrase, if it is set, or you can set it, if not. The Passphrase is a human-readable (understandable) key – like a smart card – which is used to generate a machine-usable AES 256 encryption key. (For more information, see the EMC Data Domain Operating System Administration Guide.) You can also view the available services, and for a selected service, the service options that are configured for it.
Table 13 Services

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of a service/protocol that can access the system. One of the following protocols can be selected (for viewing or configuring): FTP, FTPS, HTTP/HTTPS, SCP/SSH, or Telnet.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Status of the service: either enabled or disabled.</td>
</tr>
<tr>
<td>Allowed Hosts</td>
<td>Access permissions set for the named host.</td>
</tr>
</tbody>
</table>

Table 14 Service Options

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Option Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>Session Timeout</td>
<td>Configured number of elapsed seconds before the service times out, or Infinite.</td>
</tr>
<tr>
<td>FTPS</td>
<td>Session Timeout</td>
<td>Configured number of elapsed seconds before the service times out, or Infinite.</td>
</tr>
<tr>
<td>HTTP/HTTPS</td>
<td>HTTP/HTTPS port</td>
<td>If applicable, port number opened for the HTTP/HTTPS protocol (HTTP – port 80, by default; HTTPS – port 443, by default).</td>
</tr>
<tr>
<td></td>
<td>Session Timeout</td>
<td>Configured number of elapsed seconds before the service times out, or Infinite.</td>
</tr>
<tr>
<td>SCP/SSH</td>
<td>SCP/SSH port</td>
<td>If applicable, port number opened for the SCP/SSH protocol (port 22, by default).</td>
</tr>
<tr>
<td></td>
<td>Session Timeout</td>
<td>Configured number of elapsed seconds before the service times out, or Infinite.</td>
</tr>
<tr>
<td>Telnet</td>
<td>Session Timeout</td>
<td>Configured number of elapsed seconds before the service times out, or Infinite.</td>
</tr>
</tbody>
</table>

Managing FTP Access

To provide access to DD Management Center through an FTP connection:

**Procedure**

1. In the Services panel, select FTP, and select **Configure**.
   The Configure FTP Access dialog appears.
2. To enable FTP access, select the **Allow FTP Access** checkbox. If FTPS is enabled, it will be disabled before enabling FTP.
3. Determine how hosts connect:
   - To allow complete access, select **Allow all hosts to connect**.
   - To configure specific hosts, select **Limit Access to the following systems**, and select the appropriate icon in the Allowed Hosts panel. Host names can be a fully qualified hostname or an IP address.
     - To add a host, select the plus button (+). Enter the hostname, and select **OK**.
     - To modify a hostname, select the checkbox of the hostname in the Hosts list, and select the edit button (pencil). Change the hostname, and select **OK**.
To remove a hostname, select the checkbox of the hostname in the Hosts list, select the minus button (-), and select OK.

4. To configure a session timeout value, select the Advanced tab.

In the Session Timeout text box, enter the interval in seconds that must elapse before the connection closes.

The default setting is Infinite.

Note
Select Default to return a setting back to the default value.

5. Select OK.

Managing FTPS Access

To provide access to DD Management Center through an FTPS connection:

Procedure
1. In the Services panel, select FTPS, and select Configure.

The Configure FTPS Access dialog appears.

2. To enable FTPS access, select the Allow FTPS Access checkbox. If FTP is enabled, it will be disabled before FTPS is enabled.

3. Determine how hosts connect:
   - To allow complete access, select the Allow all hosts to connect radio button.
   - To configure specific hosts, select the Limit Access to the following systems radio button, and select the appropriate icon in the Allowed Hosts panel. Host names can be a fully qualified hostname or an IP address.
     - To add a host, select the plus button (+). Enter the hostname, and select OK.
     - To modify a hostname, select the checkbox of the hostname in the Hosts list, and select the edit button (pencil). Change the hostname, and select OK.
     - To remove a hostname, select the checkbox of the hostname in the Hosts list, select the minus button (-), and select OK.

4. To configure a session timeout value, select the Advanced tab.

In the Session Timeout text box, enter the interval in seconds that must elapse before the connection closes.

The default setting is Infinite.

Note
Select Default to return a setting back to the default value.

5. Select OK.

Managing HTTP/HTTPS Access

To provide access to DD Management Center through an HTTP and/or HTTPS connection:

Procedure
1. In the Services panel, select the checkbox for HTTP or HTTPS, and select Configure.

2. In the Configure HTTP/HTTPS Access dialog, select the checkbox for Allow HTTP Access and/or Allow HTTPS Access.
3. Determine how hosts connect:
   - To allow complete access, select the **Allow all hosts to connect** radio button.
   - To configure specific hosts, select the **Limit access to the following systems** radio button, and select the appropriate icon in the Allowed Hosts panel. Hostnames can be a fully qualified hostname or an IP address.
     - To add a host, select the plus button (+). Enter the hostname, and select **OK**.
     - To modify a hostname, select the checkbox next to the hostname in the Hosts list, and select the edit button (pencil). Change the hostname, and select **OK**.
     - To remove a hostname, select the checkbox of the hostname in the Hosts list, select the minus button (-), and select **OK**.

4. To configure system ports and session timeout values, select the **Advanced** tab.
   - In the HTTP Port text box, enter the port for connection. Port 80 is assigned by default.
   - In the HTTPS Port text box, enter the port for connection. Port 443 is assigned by default.
   - In the Session Timeout text box, enter the interval in seconds that must elapse before connection closes. 10800 seconds (3 hours) is assigned by default.

   **Note**
   Select **Default** to return a setting back to the default value.

5. Select **OK**.

**Managing SSH/SCP Access**

To provide access to DD Management Center through an SSH and/or SCP connection:

**Procedure**

1. In the Services panel, select **SSH** or **SCP**, and select **Configure**.
2. In the Configure SSH/SCP Access dialog, select options to allow SSH or SCP (or both) access. SCP cannot be enabled unless SSH is enabled as well.
3. Determine how hosts connect:
   - To allow complete access, select the **Allow all hosts to connect** radio button.
   - To configure specific hosts, select the **Limit access to the following systems** radio button, and select the appropriate icon in the Allowed Hosts panel. Hostnames can be a fully qualified hostname or an IP address.
     - To add a host, select the plus button (+). Enter the hostname, and select **OK**.
     - To modify a hostname, select the checkbox of the hostname in the Hosts list, and select the edit button (pencil). Change the hostname, and select **OK**.
     - To remove a hostname, select the checkbox of the hostname in the Hosts list, select the minus button (-), and select **OK**.

4. To configure a session timeout value, select the **Advanced** tab.
   In the Session Timeout text box, enter the interval in seconds that must elapse before the connection closes.
   The default setting is **Infinite**.
Managing Telnet Access

To provide access to DD Management Center through a Telnet connection:

**Procedure**

1. In the Services panel, select **Telnet**, and select **Configure**.
2. In the Configure Telnet Access dialog, select the **Allow Telnet Access** checkbox.
3. Determine how hosts connect:
   - To allow complete access, select the **Allow all hosts to connect** radio button.
   - To configure specific hosts, select the **Limit Access to the following systems** radio button, and select the appropriate icon in the Allowed Hosts panel. Hostnames can be a fully qualified hostname or an IP address.
     - To add a host, select the plus button (+). Enter the hostname, and select **OK**.
     - To modify a hostname, select the checkbox of the hostname in the Hosts list, and select the edit button (pencil). Change the hostname, and select **OK**.
     - To remove a hostname, select the checkbox of the hostname in the Hosts list, select the minus button (-), and select **OK**.
4. To configure a session timeout value, select the **Advanced** tab.
   In the Session Timeout text box, enter the interval in seconds that must elapse before connection closes.
   The default setting is **Infinite**.

**Note**

Select **Default** to return a setting back to the default value.

5. Select **OK**.

Managing Local User Access to DD Management Center

This section describes how to manage user access to DD Management Center.

- If you are an administrator on DD Management Center, you become a global administrator, and you can configure and monitor all managed DD systems.
- If you are a user on DD Management Center, you can view only the managed DD systems to which you have been assigned a user role by a DD Management Center administrator.

Viewing Local User Information

The datestamps in the user-authentication module use Greenwich Mean Time (GMT). Therefore, when configuring expiration dates for disabling a user’s account and password, the expiration date should reflect GMT instead of local time.

**Procedure**

1. Navigate to **AdministrationSettingsAccess tab Local Users tab**.
2. On the Local Users page, view information for the configured users, as described in the following table.
Table 15 Local Users

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>User ID, as added to the system.</td>
</tr>
<tr>
<td>Management Role</td>
<td>Possible roles of users based on a set of privileges:</td>
</tr>
<tr>
<td></td>
<td>• admin role: Can configure and monitor the entire DD system.</td>
</tr>
<tr>
<td></td>
<td>• user role: Can monitor DD systems and perform the fastcopy operation.</td>
</tr>
<tr>
<td></td>
<td>Users with admin roles can view all users. Users with user roles can</td>
</tr>
<tr>
<td></td>
<td>view only their own user account.</td>
</tr>
<tr>
<td>Status</td>
<td>• enabled – User access to the account is permitted.</td>
</tr>
<tr>
<td></td>
<td>• disabled – User access to the account is denied because the</td>
</tr>
<tr>
<td></td>
<td>expiration date for the account has been reached or a locked account's</td>
</tr>
<tr>
<td></td>
<td>password has not been renewed. Admin users can disable/enable users with</td>
</tr>
<tr>
<td></td>
<td>admin or user roles, except SysAdmin User. No users can disable SysAdmin.</td>
</tr>
<tr>
<td></td>
<td>Security officers can disable/enable only other security officers.</td>
</tr>
<tr>
<td></td>
<td>• locked – User access to the account is denied because the password has</td>
</tr>
<tr>
<td></td>
<td>expired.</td>
</tr>
<tr>
<td>Disable Date</td>
<td>Date the account is set to be disabled.</td>
</tr>
<tr>
<td>Last Login From</td>
<td>Location where the user last logged in.</td>
</tr>
<tr>
<td>Last Login Time</td>
<td>Time the user last logged in.</td>
</tr>
</tbody>
</table>

3. Select a specific user to see Detailed Information.

Table 16 Detailed Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Last Changed</td>
<td>Date the password was last changed.</td>
</tr>
<tr>
<td>Minimum Days Between Change</td>
<td>Minimum number of days between password changes that you allow a user.</td>
</tr>
<tr>
<td></td>
<td>Default is 0.</td>
</tr>
<tr>
<td>Maximum Days Between Change</td>
<td>Maximum number of days between password changes that you allow a user.</td>
</tr>
<tr>
<td></td>
<td>Default is 99999.</td>
</tr>
<tr>
<td>Warn Days Before Expire</td>
<td>Number of days to warn the users before their password expires.</td>
</tr>
<tr>
<td></td>
<td>Default is 7.</td>
</tr>
<tr>
<td>Disable Days After Expire</td>
<td>Number of days after a password expires to disable the user account.</td>
</tr>
<tr>
<td></td>
<td>Default is never.</td>
</tr>
</tbody>
</table>

Note

The default password policy can be changed by an admin by selecting More Tasks › Modify Password Policy. Default values are the initial default password policy values.
User Roles

Roles provide a way to restrict user access to system functions by using a set of privileges. Permissions allow an admin access to specific groups and systems, reducing the need to configure every user as a global admin. DD Management Center supports the following roles:

- **Admin role**: Allows one to configure and monitor the entire DD Management Center system.

  **Note**

  It is recommended that the Admin role be used judiciously and awarded to very few users, as these users will be able to configure DD Management Center as well as have access to all registered Data Domain systems.

- **User role**: Allows one to monitor DD Management Center and Data Domain systems for which they have permission.

Creating Local Users

You can create new users with either the admin or the user role.

**Procedure**

1. Navigate to **Administration > Settings > Access tab > Local Users tab**.
2. Select **Create**.
3. In the Create User dialog, enter the following in the General tab:

   **Table 17 General Tab**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User ID or name.</td>
</tr>
</tbody>
</table>
   | Password        | User password. Set a default password, and the user can change it later. The default value for the minimum length of a password or minimum number of character classes required for a user password is 1. Allowable character classes include:  
   |                 | Allowable character classes include:                                        |
   |                 | • lowercase letters (a-z)                                                  |
   |                 | • uppercase letters (A-Z)                                                  |
   |                 | • numbers (0-9)                                                            |
   |                 | • special characters ($, %, #, +, and so on)                               |
   | Verify Password | User password, again.                                                      |
   | Management Role | Management role assigned to the user:                                      |
   |                 | • **admin role**: Can configure and monitor the entire DD Management Center and all DD systems. |
   |                 | • **user role**: Can monitor DD Management Center and DD systems for which they have permission. |

4. Enter the following in the Advanced tab:
### Table 18 Advanced Tab

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Days Between Change</td>
<td>Minimum number of days between password changes that you allow a user. Default is 0.</td>
</tr>
<tr>
<td>Maximum Days Between Change</td>
<td>Maximum number of days between password changes that you allow a user. Default is 99999.</td>
</tr>
<tr>
<td>Warn Days Before Expire</td>
<td>Number of days to warn the users before their password expires. Default is 7.</td>
</tr>
<tr>
<td>Disable Days After Expire</td>
<td>Number of days after a password expires to disable the user account. Default is Never.</td>
</tr>
<tr>
<td>Disable account on the following date</td>
<td>Check this box and enter a date (mm/dd/yyyy) when you want to disable this account. Also, you can click the calendar to select a date. This date uses GMT.</td>
</tr>
</tbody>
</table>

5. Select **OK**.

**Note**
The default password policy can be changed by the admin with the More Tasks > Modify Password Policy option. The default values are the initial default password policy values.

---

### Modifying a Local User Profile

**Procedure**

1. Navigate to **Administration > Settings > Access tab > Local Users tab**.
2. Select a user name, and select **Modify**.
3. In the Modify User dialog, change the assigned role.
4. Enter the following information in the Advanced tab:

#### Table 19 Advanced Tab

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Days Between Change</td>
<td>Minimum number of days between password changes that you allow a user. Default is 0.</td>
</tr>
<tr>
<td>Maximum Days Between Change</td>
<td>Maximum number of days between password changes that you allow a user. Default is 99999.</td>
</tr>
<tr>
<td>Warn Days Before Expire</td>
<td>Number of days to warn the users before their password expires. Default is 7.</td>
</tr>
<tr>
<td>Disable Days After Expire</td>
<td>Number of days after a password expires to disable the user account. Default is Never.</td>
</tr>
</tbody>
</table>

5. Optionally, configure a disable date (which uses GMT) for the user account.
6. Select **OK**.
Deleting a Local User

You can delete certain users, based on your user role. If one of the selected users cannot be deleted, the Delete button will be disabled. For example, sysadmin cannot be deleted.

Procedure
1. From the Local Users tab, select one or more user names from the list.
2. Select Delete to delete the user accounts.
3. In the Delete User dialog, select OK and Close.

Enabling or Disabling Local Users

Procedure
1. From the Local Users tab, select one or more user names from the list.
2. Select either the Enable or Disable button.
3. In the Enable User or Disable User dialog, select OK and Close.

Changing User Passwords

Procedure
1. From the Local Users tab, select a user name from the list.
2. Select Change Password.
3. In the Change Password dialog, enter the new password into the New Password box. [If prompted, enter the old password, as well.]
4. Enter the new password again in the Verify New Password box.
5. Select OK.

Modifying the Password Policy

You can modify the password policy settings that are assigned to a user by default.

Procedure
1. Navigate to Administration > Settings > Access tab > Local Users tab
2. Select More Tasks > Modify Password Policy.
3. In the Modify Password Policy dialog, enter the password policy information. To select the default value, select the Default button next to each value.

Table 20 Modify Password Policy Dialog

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Days Between Change</td>
<td>Minimum number of days between password changes that you allow a user. Default is 0.</td>
</tr>
<tr>
<td>Maximum Days Between Change</td>
<td>Maximum number of days between password changes that you allow a user. Default is 99999.</td>
</tr>
<tr>
<td>Warn Days Before Expire</td>
<td>Number of days to warn a user before a password expires. Default is 7.</td>
</tr>
<tr>
<td>Disable Days After Expire</td>
<td>Number of days after a password expires to disable a user account. Default is Never.</td>
</tr>
</tbody>
</table>
Table 20 Modify Password Policy Dialog (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length of Password</td>
<td>Minimum password length required. Default is 1.</td>
</tr>
<tr>
<td>Minimum Number of Character Classes</td>
<td>Minimum number of character classes required for a user password.</td>
</tr>
<tr>
<td></td>
<td>Default is 1. Character classes include:</td>
</tr>
<tr>
<td></td>
<td>• lowercase letters (a-z)</td>
</tr>
<tr>
<td></td>
<td>• uppercase letters (A-Z)</td>
</tr>
<tr>
<td></td>
<td>• numbers (0-9)</td>
</tr>
<tr>
<td></td>
<td>• special characters ($, %, #, +, etc.)</td>
</tr>
</tbody>
</table>

4. Select OK.

Managing NIS Servers and Workgroups

NIS workgroup management includes configuring NIS authentication, domain names, and NIS groups.

Viewing NIS Information

Procedure

1. Navigate to the Administration > Settings > Access tab > NIS tab.
2. On the NIS page, view information about NIS Authentication Servers and Configured NIS Groups, as described in the following table.

Table 21 NIS Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Status of the service: enabled or disabled.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Name of the domain for this service.</td>
</tr>
<tr>
<td>Authentication Servers</td>
<td>Name of the server performing authentication.</td>
</tr>
<tr>
<td>Group</td>
<td>Name of the NIS group.</td>
</tr>
<tr>
<td>Management Role</td>
<td>Management role assigned to the group (admin or user).</td>
</tr>
</tbody>
</table>

3. Edit any of this information by selecting the appropriate Edit button.

Enabling NIS Authentication

To enable NIS Authentication:

Procedure

1. In the Status panel, select Enable.

   The Enable NIS dialog box appears.
2. Click OK.

Disabling NIS Authentication

To disable NIS Authentication:

Procedure
1. In the Status area, click Disable.
   The Disable NIS dialog box appears.
2. Click OK.

Editing the Domain Name

Procedure
1. In the Status area, click Edit to add or modify the NIS domain name.
   The Configure NIS Domain Name dialog box appears.
2. Enter the domain name in the Domain Name box, and click OK.

Configuring Authentication Servers

Procedure
1. In the Authentication Servers panel, click Edit to add or modify an authentication server.
2. In the Configure NIS Authentication Servers dialog box, select one of the following:
   - Obtain NIS Servers from DHCP
   - Manually Configure
     - To add an authentication server, click the plus button (+). Enter the server name, and click OK.
     - To modify an authentication server, select the check box of the authentication server in the server list and click the edit icon (pencil). Change the server name, and click OK.
     - To remove an authentication server, select the check box of the hostname in the server list, click the X icon, and click OK.
3. Click OK.

Configuring NIS Groups

Procedure
1. In the Configured NIS Groups panel, click Edit.
2. In the Configure Allowed NIS Groups dialog box, select an NIS group.
   - To add an NIS group, click the plus button (+). Enter the NIS group name, select the role (admin or user), and click Validate. Click OK to exit the Add NIS Group dialog box. Click OK again to exit the Configure Allowed NIS Groups dialog box.
   - To modify an NIS group name, select the check box of the NIS group name in the NIS group list and click the edit button (pencil). Change the NIS group name, and click OK.
   - To remove an NIS group, select the check box of the NIS group in the list and click the X button, then click OK.
Managing Windows Servers and Workgroups

Windows workgroup management includes configuring Windows authentication and Active Directory, and assigning group roles.

Viewing Windows Information

Procedure

1. Navigate to Administration > Settings > Access tab > Windows tab.
2. View information about your windows setup, as described in the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Type of authentication mode: Workgroup or Active Directory</td>
</tr>
<tr>
<td>Workgroup/Active Directory Names</td>
<td>Name of the Workgroup or Active Directory</td>
</tr>
<tr>
<td>CIFS Server Name</td>
<td>Name of the CIFS Server in use</td>
</tr>
<tr>
<td>WINS Server</td>
<td>Name of the WINS Server in use</td>
</tr>
<tr>
<td>Allowed Groups</td>
<td></td>
</tr>
<tr>
<td>Windows Group</td>
<td>Name of the Windows group</td>
</tr>
<tr>
<td>Management Role</td>
<td>Management role of the group: admin or user</td>
</tr>
</tbody>
</table>

3. Add to, edit, or configure these settings, using the appropriate button.

Configuring Authentication

You can configure two different authentication types: for a workgroup or for an active directory.

Configuring Authentication for Workgroups

You can configure workgroup authentication parameters as follows.

Before you begin

Navigate to Administration > Settings > Access tab > Windows tab > Authentication.

Procedure

1. Select Configure.
2. In the Configure Authentication dialog, from the Mode drop-down list, select Workgroup.
   The Workgroup mode joins DD Management Center to a workgroup domain.
3. Optionally, deselect the Use Default box, and enter a Workgroup Name in the text box.
4. Select the Advanced tab to set additional information.
5. Optionally, deselect the Use Default box, and enter a CIFS Server Name in the text box.
6. Select OK.
Configuring Authentication for an Active Directory

DD Management Center must meet all Active Directory requirements, such as a clock time that differs no more than five minutes from that of the domain controller.

Before you begin

Navigate to Administration > Settings > Access tab > Windows tab > Authentication.

Procedure

1. Select Configure.

The appears.

2. In the Configure Authentication dialog, from the Mode drop-down list, select Active Directory.

The Active Directory mode joins DD Management Center to an Active Directory domain.

3. In the Realm Name text box, enter the full realm name for DD Management Center, such as domain1.local.

4. In the Domain Joining Credential area, enter a user name and password. Enter either a user in a domain to be joined, or a user in a domain that is a trusted domain of your company. The user name and password must be compatible with Microsoft requirements for the Active Directory domain being joined. This user must have permission to create accounts in this domain.

5. Select the Advanced tab to set additional information.

6. Optionally, to set a CIFS server name, in the CIFS Server Name area:
   - Select the check box to use the default CIFS server name.
   - Deselect the check box, and enter the CIFS server name in the text box.

7. In the Domain Controllers area, determine how domain controllers are assigned:
   - For automatic assignment, select the radio button for Automatically assign Domain Controllers. This is the default and recommended method.
   - To add specific domain controllers, select the radio button for Manually assign Domain Controllers, and enter controller name(s) in the text box(es). Up to three controller names can be added. You can enter fully qualified domain names, host names, or IP addresses.

8. Optionally, to set Organizational Units, in the Organizational Unit area:
   - Select the check box to use the default Organizational Unit.
   - Deselect the check box, and enter the Organizational Unit name in the text box.

   Note

   The account is moved to the new Organizational Unit.

9. Select OK.

After you finish

After configuring Windows authentication, you must enable CIFS authentication from the DD Management Center command line:

adminaccess authentication add cifs
Configuring Allowed Groups

Configuring allowed Windows workgroups include creating and modifying access to DD Management Center for a group of users.

Creating Allowed Groups

Before you begin
Navigate to Administration › Settings › Access tab › Windows tab › Allowed Groups.

Procedure
1. Select Create.
2. In the Create Windows Group dialog, enter the Group name in the text box. The domain for the group must be specified. For example, domain\group name.
3. Choose either admin or user from the Management Role drop-down list.
4. Select OK.

Modifying Allowed Groups

Before you begin
Navigate to Administration › Settings › Access tab › Windows tab › Allowed Groups.

Procedure
1. Choose a Windows Group from the list, and select Modify.
2. In the Edit Windows Group dialog, edit the Group name in the text box. The domain for the group must be specified. For example, domain\group name.
3. Choose a role from the Management Role drop-down list.
4. Select OK.

Deleting Groups

You cannot delete default Windows groups, such as Domain Admins. If a default Windows group is selected, the Delete button will be grayed out.

Procedure
1. From the Allowed Groups area of the Windows tab, select a Windows Group from the list, and select Delete.
2. In the Delete Windows Group dialog, select OK.

Viewing Active Users

The Administration › Settings › Active Users page lists information about users who are currently logged in to DD Management Center.

Table 23 Active Users

<table>
<thead>
<tr>
<th>Name</th>
<th>Name of user with an active session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>Amount of time since last activity for user</td>
</tr>
<tr>
<td>Last Login From</td>
<td>System where user is logged in</td>
</tr>
</tbody>
</table>
### Table 23 Active Users (continued)

<table>
<thead>
<tr>
<th>Last Login Time</th>
<th>Datestamp when user logged in</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTY</td>
<td>Terminal notation for CLI login or GUI if user is logged in using the GUI</td>
</tr>
</tbody>
</table>

### Performing DD Management Center Software Upgrades

Upgrading DD Management Center operating system software is done in two stages:

- Obtaining an image from the Data Domain Support Web Site or selecting a previously obtained upgrade image that has been saved.
- Performing the upgrade on the DD Management Center.

**Note**

Only DD Management Center admins have rights to upgrade and manage packages for DD Management Center.

### Managing Upgrade Packages

You can download an upgrade image from the EMC Data Domain Support site to a locally accessible drive, and then add it to the upgrade package collection managed by DD Management Center.

**Procedure**

1. Navigate to Administration > Settings > Upgrade tab.
2. In the Upgrade Packages Available area, view the available upgrade packages, their sizes, and their modification dates. Then, select one of the following options:
   - To get a new upgrade package to store locally, select the EMC Online Support link.
   - To upload a package that has been stored locally to the inventory, select Upload Upgrade Package and browse to the local drive and select the package.
   - To delete a package, select the package from the inventory list, and select Remove Upgrade Package.
3. To perform the upgrade, see the procedure in the following section.

### Performing a DD Management Center Upgrade

To upgrade the DD Management Center operating system software:

**Procedure**

1. Check the DD Management Center Release Notes for information about the release, and verify available system space.
2. Navigate to Administration > Settings > Upgrade tab.
3. Select the upgrade image from the list, and select Perform System Upgrade. This action assumes you have already gotten the package.
4. Monitor the upgrade progress from the DD Management Center console page in the vSphere application.
5. Notice that the upgrade process automatically reboots DD Management Center.
Managing System Logs

A messages file and audit log file are saved on DD Management Center and listed in the Logs area. Files can be opened and saved to a local location and then forwarded to Support if required.

To review the log file list on the system:

Procedure

1. Navigate to Administration > Settings page and click the Logs tab.
   
   The Log Files page shows the log file name and file size, and the date the log was generated. Log files are automatically named.

2. Click a log file name to view its contents. You may be prompted to select an application, such as Notepad.exe, to open the file.

3. Save the log file locally, if needed.

Managing Alerts

The DD Management Center and the Data Domain system use the same alert system. Detailed information about the alert system is described in the *EMC Data Domain Operating System Administration Guide*.

This section describes how to configure settings for who receives DD Management Center alert notifications and the DD Management Center daily alert summaries.

Managing Alert Notifications

The groups that are configured to receive DD Management Center alert notifications are listed in the Administration > Settings > Alerts page with the Notification tab. Clicking a group in the table populates the Details panels for alert class attributes and subscribers who receive notification when alerts reach the severity that is configured for the alert class.

Filtering the Notifications List

To filter (or search for an item) in the notifications group list, type a group name and/or subscriber email in the appropriate text box in Filter By area, then click Update. The result displays at the top of the notification list.

Note

Click Reset to return the group list to the default order.

Creating a Notification Group

By default, all alerts are sent to the autosupport-alert@autosupport.datadomain.com email group, but additional groups can be created to receive specific classes of alert notifications.

To create a notification group:

Procedure

1. Click Add, and in the Add Group dialog window type a name for the group in the Group Name text box.
2. Select the alert classes, set the severity level at which notifications are sent and click OK.
   For example, create a CriticalWarnings group, select all classes and set the severity level to Critical.

3. Select the check box of the group, now in the Notifications group list, and click Modify.

4. In the Modify Group dialog window, click Subscribers and in the Subscribers panel, click the + icon and add the email address of a subscriber, then click OK.

5. Repeat this step for each subscriber that needs to be added to the group and click Finish.

Verifying Subscriber Emails in a Notification Group

Send a test email to subscribers in a notification group to verify the email addresses are operational:

Procedure
1. In the More Tasks menu, select Send Test Alert.
2. In the Notification Groups panel, select the check boxes of the groups to receive the test email, then click Next.
3. In the Additional Email Addresses panel, add or modify email addresses, if necessary.
4. Click Send Now.

Modifying a Notification Group

Procedure
1. Select the check box of the group in the Notifications group table, and select Modify.
2. In the Modify Group dialog, select Group Properties, and in the Class Attributes area, add or remove classes, change any severity levels, and select Next.
3. The Subscribers area displays. Add or remove any subscriber email addresses, as needed, and select Finish.

Deleting a Notification Group

The Default notification group cannot be deleted.

Procedure
1. Select one or more check boxes of groups in the Notifications group table, and select Delete.
2. In the Delete Group dialog, verify the deletion, and select OK.
3. Select OK to exit the confirmation dialog window.

Resetting a Notification Group

You can remove all notification groups that were added and remove any changes to the Default group.

Procedure
1. From the More Tasks menu, select Reset Notification Groups.
2. In the Reset Notification Groups dialog, select Yes, and in the verification dialog window, and select OK.
Managing a Subscriber List

You can add, modify, or delete email addresses from a notification group subscriber list.

Procedure
1. Navigate to Administration › Settings › Alerts tab › Notification tab
2. Select the check box of the group in the Notifications group table, and select Configure in the Subscribers panel of the Detailed Information area.
3. In the Edit Subscribers dialog, select one of the following options:
   • To add a subscriber, select the + control. Enter the email address in the Email Address dialog, and select OK.
   • To modify an email address, select the check box of the email address in the Subscriber Email list, and select the pencil control. Edit the email address in the Email Address dialog, and select OK.
   • To delete an email address, select the check box of the email address in the Subscriber Email list, and select the X control.
4. Select OK.

Managing Daily Alert Summaries

Every morning at 8:00 a.m. local time for the DD Management Center, a Daily Alert Summary email is sent to the configured subscribers. The Daily Alert Summary email contains summaries of alerts and log messages.

To configure the Daily Alerts Summary settings:

Procedure
1. Navigate to the page Administration › Settings › Alerts › Daily Alert Summary.
2. If the 8 AM default delivery time is not acceptable, click Schedule in the Delivery Time area.
3. In the Schedule Alert Summary window, select the hour, minute, and AM/PM, and click OK.
4. Click Configure/Edit in the Subscribers panel.
   The Daily Alert Summary Mailing List dialog window appears.
5. Manage a subscriber email:
   • To add a subscriber, click the + icon and enter the email address in the Email Address dialog window, then click OK.
   • To modify an email address, select the check box of the email address in the Subscriber Email list and click the pencil icon. Edit the email address in the Email Address dialog window, then click OK.
   • To delete an email address, select the check box of the email address in the Subscriber Email list and click the X icon.
6. Click Finish.

Managing Autosupport Reporting

The Autosupport feature emails an automatically generated daily report to EMC Data Domain Support that shows DD Management Center system identification, status information, and entries from various log files. Extensive and detailed internal statistics
and information are included at the end of the report to aid support personnel if the need arises to debug problems.

To disable autosupport reporting, navigate to Administration > Settings > Support > Autosupport, click Disable in the Vendor Support panel.

At any time, you can generate an autosupport bundle.

---

**Note**

No information about managed DD systems are included in this report.

### Adding to the Autosupport Report Email List

By default, autosupport reports are enabled and sent daily to EMC Data Domain Customer Support. You may want to add additional email addresses as recipients of autosupport reports.

To set the list of email addresses that receive the autosupport notifications:

**Procedure**

1. Navigate to Administration > Settings > Support > Autosupport, and in the Autosupport Mailing List panel, click Configure.
2. In the Configure Autosupport Subscribers window, click the plus icon (+) to open the Email dialog box.
3. Enter a recipient's email address in the Autosupport Email text box and click OK.
4. Click OK to exit the Configure Autosupport Subscribers dialog box.

### Reviewing Generated Autosupport Reports

The Autosupport Reports panel contains a list of links to current autosupport report files. Select a file name link to view the report using a text editor. If required by your browser, download the file first.

### Manually Generating a Support Bundle

When troubleshooting problems, EMC Data Domain Support may ask you to immediately generate a support bundle, which is a tar-g-zipped selection of log files and a README file that includes identifying autosupport headers.

To create a support bundle, navigate to Administration > Settings > Support > Support Bundles, select Generate Support Bundle, and email the result to EMC Data Domain Support.

---

**Note**

If the bundle is too large to be emailed, go to the EMC Data Domain Support site, and upload the bundle.

### Checking a DD Management Center Serial Number

Each DD Management Center virtual machine has a unique serial number, which is used to identify the system in autosupport messages. To view your serial number, navigate to the Administration > Settings page, and select the Serial Number tab. To change the serial number, select Edit.
Performing Advanced Configuration

Note

DD Management Center does not require a license, but the Data Domain systems that you manage must have licenses for their core and optional features.
This appendix provides a reference for all of the graphical elements (icons, controls, widgets, LEDs, etc.) of the DD Management Center.

- Global Controls and Icons ................................................................. 104
- Dashboard ...................................................................................... 106
- Health .............................................................................................. 109
- Capacity ......................................................................................... 111
- Replication ..................................................................................... 113
- Reports ............................................................................................ 116
- Administration .............................................................................. 117
- Inventory .......................................................................................... 119
Global Controls and Icons

Here are descriptions of the controls and icons that are used throughout the DD Management Center interface.

### Table 24 Controls that Perform a Function

<table>
<thead>
<tr>
<th>Control</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Help Icon]</td>
<td>Help</td>
<td>Located in the DD Management Center banner, this opens the top-level help page. The help is derived from the <em>EMC Data Domain Management Center User Guide</em>.</td>
</tr>
<tr>
<td>![About Icon]</td>
<td>About DD Management Center</td>
<td>This displays an information page, showing the details of this version of DD Management Center.</td>
</tr>
<tr>
<td>![Log Out Icon]</td>
<td>Log Out</td>
<td>Located in the DD Management Center banner, this logs you out of DD Management Center.</td>
</tr>
<tr>
<td>![Filter Icon]</td>
<td>Filter controls</td>
<td>The filter control is comprised of two parts, the funnel icon and a drop-down menu. When the funnel icon is selected, it toggles filtering on or off.</td>
</tr>
<tr>
<td>![View Icon]</td>
<td>System or Group view toggle</td>
<td>Filter selection is performed with the small down arrow, which opens a drop-down list of the types of filtering that can be employed:</td>
</tr>
<tr>
<td>![View Icon]</td>
<td>View by System</td>
<td>(default) displays systems as a flat list, whose entries are sortable using the table column sorting controls.</td>
</tr>
<tr>
<td>![View Icon]</td>
<td>View by Group</td>
<td>displays systems by their group hierarchy. In this view, sorting of the table is only performed within groups. Group listings can be expanded to a systems list.</td>
</tr>
</tbody>
</table>

Filtering is used in the work area panel for monitoring views, and for Reports and Dashboard widgets.

- **Filter by group** – Enables the selection of one or more groups. Systems belonging to the selected groups display in the work area panel.
- **Filter by property** – Enables the selection of one or more property values. Systems having those property values display in the work area panel.
- **Filter by system** – Enables the selection of one or more systems to be displayed in the work area panel.
- **Filter by rule** – Enables the creation of a filter rule (or selection of a previously created rule) that controls which systems display in the work area panel. Filter by rule is used to combine systems, groups and properties to achieve finer granularity.
- Filtering is used in the work area panel for monitoring views, and for Reports and Dashboard widgets.
### Table 24 Controls that Perform a Function (continued)

<table>
<thead>
<tr>
<th>Control</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Icon](image) ![Icon](image) | System, Group, Tenant view toggle | Same as the previous icon, but you can also select:  
- **View by Tenant** – (default) displays tenants as a flat list, whose entries are sortable using the table column sorting controls. |
| ![Icon](image) | Launch DD System Manager | Starts the DD System Manager application in a new browser window for the selected system, where you can directly manage or investigate the corresponding area from where it was launched. |
| ![Icon](image) | Show columns | Found on many of the views that are table-based, enables the choice of columns that display in the table. |
| ![Icon](image) | Column sorter | On table views, sorts the columns in ascending or descending view (by date, alphabetically, priority, etc), based on the column data type. |
| ![Icon](image) | Add | Opens a dialog to add one or more items. The type of item being added depends on the page being displayed. For example, on the **Inventory > Systems** page, this lets you add systems to DD Management Center. On the **Administration > Properties** page, this lets you to create custom properties for managed objects. |
| ![Icon](image) | Edit | For a selected table element, opens a dialog that allows changing information about the element. |
| ![Icon](image) | Delete | Deletes a selected table element. |
| ![Icon](image) | Continue | Continues an operation, such as adding another statement when creating a custom rule. |

You can select the icon to display a status banner with more information about the connection problem.

### Table 25 Icons Showing Connection Status

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Normal – Communication between the DD Management Center and the DD system is operating normally.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Unreachable – The DD system is not responding or is not transmitting. Data was last retrieved as of the date shown in the status banner.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Unmanaged – The DD system is suspended or unmanaged. When suspended, all data collection ceases. A system is suspended when management taken over by another DD Management Center or when the system is suspended via the CLI.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Adding – The DD system is being added into the inventory.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Upgrading – The DD system is being upgraded and is unavailable during this state.</td>
</tr>
</tbody>
</table>
Table 25 Icons Showing Connection Status (continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Monitor Icon]</td>
<td>Synchronizing – Data for the DD system is being synchronized. The system is unavailable during this state.</td>
</tr>
</tbody>
</table>

Dashboard

The Dashboard > Monitoring page consists of one to seven tabs that you create to hold any number of widgets that provide high-level, quick monitoring views of various aspects of your Data Domain environment.

By default, one tab is provided named All Systems that is populated with one of each type of widget, configured to monitor all managed DD systems.

Widget templates for commonly used monitoring functions can be used to create widgets for all managed systems or filtered by a set of criteria such as groups, properties, systems, or rules.

After they have been created, you can drag widgets around the dashboard to improve their organization. A widget or a tab with several widgets can be copied and modified to create additional widgets.

Tabs can be used to organize groups of widgets on separate pages.

The size of the dashboard can be toggled between full screen and normal view.

Table 26 Dashboard Controls

<table>
<thead>
<tr>
<th>Controls</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Add Widget Icon]</td>
<td>Add Widget</td>
<td>Opens the Add Dashboard Widget dialog where you can select a widget template and optional filters to create a widget.</td>
</tr>
<tr>
<td>![Add/Configure Tabs Icon]</td>
<td>Add/Configure Tabs</td>
<td>Opens the Add and Configure Dashboard Tabs dialog where you can add tabs, modify tab names, or delete tabs. You can also set the number of columns and change the ordering of the tabs across the dashboard.</td>
</tr>
<tr>
<td>![Maximize/Restore Dashboard Icon]</td>
<td>Maximize/Restore dashboard</td>
<td>Toggles the size of the dashboard. Maximize hides the navigation panel and Restore returns to default view, exposing the navigation panel.</td>
</tr>
</tbody>
</table>

Widgets

Widgets are created by means of a dialog that enables you to choose a monitoring function, configure the view, and filter which systems are to be included.

Widget Templates

You can add, edit, or delete widgets from the dashboard, by selecting the Add widget control in the banner at the top right, by using the Edit widget control in the banner of each widget, or by using the Remove widget control in the banner of each widget, respectively.
The following widget templates are available.

**Current Health Status Widget**

The **Current Health Status** widget shows a summary of important health factors for monitored DD systems, such as any unmanaged systems, the status of the file system, replication status, alerts, and protocol status.

Selecting the Show detail control (>>) navigates to the **Health > Status** page.

**Active Alerts Widget**

The **Active Alerts** widget shows the distribution of active alerts across all managed systems by type – Emergency & Alert, Critical & Error, and Warning.

Color-coded bar graphs for severity levels show alert totals and the number of systems affected.

Selecting the Show detail control (>>) navigates to the **Health > Alerts** page, where a complete list of Health Alerts is displayed.

**Capacity Overview Widget**

The **Capacity Overview** widget shows the distribution of capacity usage across all managed systems.

Color-coded bars show critical, warning, and normal capacity levels.

A configuration option lets you show projected capacity usage for a selected period of time (from 1 to 18 months).

Selecting the Show detail control (>>) navigates to the **Capacity > Utilization** page.

**Space Usage Widget**

The **Space Usage** widget shows summaries of capacity factors – total space, space used, space available, pre-comp(ression) space used, and compression ratio.

It also displays alerts for systems at capacity and warnings for those nearing capacity.

Selecting the Show detail control (>>) navigates to the **Capacity > Utilization** page.

**Replication Status Widget**

The **Replication Status** widget shows a summary of important status factors for replication pairs.

This widget shows the number of replications being monitored, the number of source and destination systems or groups, and data transfer totals. If any pairs have critical or warning status, a warning icon displays, which when selected, opens the appropriate Replication page.

Configuration options include setting the widget to monitor only Automatic or only On-Demand replications. Additional options allow selecting specific replication status factors (such as pre-comp bytes written in last 24 hours) for Automatic replications or file transfer status for the last 24 hours when configuring On-Demand replications.

Selecting the Show detail control (>>) navigates to the **Replication > Automatic** page.

---

**Note**

For DD Boost (on-demand replication) monitoring, the DD system must be running DD OS 5.3.1 or later. Any DD system running older software will not display DD Boost replication pair associations between the source and destination systems on any of the file replication reporting pages, widgets, or reports.
Top Replication Lags Widget

The Top Replication Lags widget shows a list of systems exhibiting the longest lag time. Selecting the Show detail control (>>) navigates to the Replication ▶ Automatic page, where the complete list of filtered DD systems with lagging replications is shown, and you can view or change the Lag Threshold Policy.

Selecting a row in the widget navigates to the Replication ▶ Automatic page, filtered to show only those pairs whose source is the selected system.

**Note**

For DD Boost (on-demand replication) monitoring, the DD system must be running DD OS 5.3.1 or later. Any DD system running older software will not display DD Boost replication pair associations between the source and destination systems on any of the file replication reporting pages, widgets, or reports.

Replication Lag Status By Pairs Widget

The Replication Lag Status by Pairs widget shows the count of replications with critical, warning, and normal levels, based on the Lag Threshold Policy.

Selecting the Show detail control (>>) navigates to the Replication ▶ Automatic page, where the list of all filtered replications is shown, and you can view or change the Lag Threshold Policy.

**Note**

For DD Boost (on-demand replication) monitoring, the DD system must be running DD OS 5.3.1 or later. Any DD system running older software will not display DD Boost replication pair associations between the source and destination systems on any of the file replication reporting pages, widgets, or reports.

## Widget Controls

Each widget includes the following standard controls.

**Table 27 Widget Controls**

<table>
<thead>
<tr>
<th>Controls</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Edit Widget" /></td>
<td>Edit Widget</td>
<td>Opens the Edit Dashboard Widget where you can change the widget name and filter criteria, and in some cases, widget details.</td>
</tr>
<tr>
<td><img src="image" alt="Details" /></td>
<td>Details</td>
<td>The global drill-down button on a widget that navigates to the parent page associated with the widget. For example, for Alerts widgets, the Health ▶ Alerts page is opened.</td>
</tr>
<tr>
<td><img src="image" alt="Help" /></td>
<td>Help</td>
<td>Provides information about what the widget monitors and active controls on the widget, such as the control to navigate to the parent monitoring page.</td>
</tr>
<tr>
<td><img src="image" alt="Remove Widget" /></td>
<td>Remove Widget</td>
<td>Deletes the widget from the tab.</td>
</tr>
<tr>
<td><img src="image" alt="Connection Status" /></td>
<td>Connection Status</td>
<td>Click Status to open a popup that lists the counts of DD systems with connection problems in any of these categories: (not responding, not transmitting, suspended, and un-managed). Includes a link at the bottom of the popup to navigate to the Health ▶ Status page that provides more details about just these systems.</td>
</tr>
</tbody>
</table>
Table 27 Widget Controls (continued)

<table>
<thead>
<tr>
<th>Controls</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Note</td>
<td>The Status control displays on a widget when any of the monitored systems (filtered or unfiltered) has one or more connection problems.</td>
</tr>
<tr>
<td></td>
<td>Filter</td>
<td>Indicates a filter is active for the widget.</td>
</tr>
<tr>
<td></td>
<td>Emergency and Alert</td>
<td>When an emergency or alert state is present, click this icon to open the Status &gt; Alerts page to show the emergency/alert messages.</td>
</tr>
<tr>
<td></td>
<td>Critical and Error</td>
<td>When critical or error states are present, click this icon to open the Status &gt; Alerts page to show the critical/error messages.</td>
</tr>
<tr>
<td></td>
<td>Warning</td>
<td>When a warning exists, click this icon to open the Status &gt; Alerts page to show the warning.</td>
</tr>
</tbody>
</table>

**Health**

The Health module includes pages that provide information on the status and alerts of managed Data Domain systems, as well as the status of jobs running within the DD Management Center.

**Status**

The Health > Status page displays status information for DD systems being managed by DD Management Center. The table can be toggled (top right) to list by Systems, Groups, or Tenants. Filtering is supported for narrowing the scope of the display.

DD systems that are unreachable by DD Management Center (not responding, not transmitting, suspended, or unmanaged) are displayed in red text, and Connection Status tells you what is wrong. For more detail, you can hover over the system name; there is also a link to the Alerts page (Show alerts).

The other columns on the page contain color-coded LEDs showing the highest severity level of current alerts, File System status, Replication (the number of pairs with errors), and the status of the protocols: CIFS, NFS, VTL, and DD Boost. The LEDs show the last known state.

**Note**

If the File System is destroyed or disabled, it will have a red LED. As a result of this non-activity, Protocols and Replication are affected and will have a red LED, as well.

Table 28 LED colors

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Normal; no errors or alerts.</td>
</tr>
<tr>
<td>Yellow</td>
<td>Warning level. Hovering on Alerts provides details and a link to a filtered view on the Health &gt; Alerts page.</td>
</tr>
</tbody>
</table>
Table 28 LED colors (continued)

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>Problem exists; file systems destroyed or disabled, and critical and error alerts – alert totals are shown when you hover, which also provides a helpful link to a relevant page for more information.</td>
</tr>
<tr>
<td>Grey</td>
<td>Disabled status; disabled is a user-initiated state.</td>
</tr>
<tr>
<td>Grey LED</td>
<td>Item not licensed.</td>
</tr>
</tbody>
</table>

Use the **System Details** control to view additional information about a highlighted system.

Use the **Tenant Unit Details** control to view additional information about a highlighted tenant unit.

Use the **Launch DD System Manager** control to see the highlighted system in DD System Manager.

**Alerts**

The **Health > Alerts** page lists alerts that have been generated for the DD Management Center and those Data Domain systems being managed.

The table can be toggled (top right) to list alerts by Systems or Tenants.

The page has filter controls to display All Alerts that have occurred or just the Active Alerts. Many, but not all alerts remain active until manually cleared.

The page banner provides summaries of the total number of alerts, those that are errors and above, and those that are warnings.

Use the column controls to sort the alert list by severity, system name, post time, class, message text, and object ID. The System Name column includes a filter for entering system name text.

Alerts in the table can also be filtered by date controls (Last 12 hours, last 24 hours, last 7 days, last 30 days, all active alerts, and custom filtering).

Selecting an alert in the table shows descriptive information about the alert in the Details and the History panels.

To see a summary of the alert's history, select the More Details link to see a list of every occurrence of the alert at the site.

To investigate or resolve an alert on a DD system, open the DD System Manager by double-clicking the alert in the table, or use the Launch DD System Manager control, which is enabled when a Data Domain system alert is selected.

**Jobs**

The **Health > Jobs** page displays information about jobs (also called tasks) that have been initiated from the DD Management Center, including jobs still in progress and jobs that have completed, whether successfully or not. Details of a task, including its subtask status are shown for a selected task in the Details panel.

When upgrading one or more DD systems, the progress of a selected In-progress task can be paused and resumed with the Status control.

Tasks can run on the DD Management Center alone or can run on the DD Management Center and a DD system. For example, the Report Generation task runs solely on DD
Management Center; other tasks, like Upgrade, run mostly on the DD system, but a skeleton process on DD Management Center keeps track of the task's progress. And still other tasks run mostly on DD Management Center (such as Adding Systems), but have subtasks that run on the DD system.

**Note**
Tasks that run on DD System Manager (native to the DD system) are not shown in the Jobs list – only those tasks initiated from DD Management Center are shown.

Additional job-status filtering controls for the table are located at the top left of the page, enabling the inclusion of jobs that have succeeded, have failed, or are still in progress. If no selection is active, no jobs are shown.

The displayed list of tasks is dependent on the role:
- A person with a User role on a DD system or DD Management Center sees only the tasks they initiated on that DD system or DD Management Center.
- An Admin on a DD system or DD Management Center sees all jobs on that DD system and DD Management Center.

**Capacity**

The Capacity module provides storage usage information for the Data Domain systems and MTrees being managed by DD Management Center. This includes an overview of both current and historical space consumption, as well as an estimate of projected future (12 month) storage needs.

**Utilization**

The **Capacity > Utilization** page shows storage usage amounts, organized by System (DD system) or MTree (tabs at top right). This page has controls for opening the System Details Lightbox for examining in-depth information about a system, charting storage data history, launching a DD System Manager session, and exporting data to a CSV spreadsheet program for viewing or saving.

The System page can be filtered by viewing the tabular listing by Systems or Groups (toggle at top right). Selecting an entry in the systems table displays detailed connection status information immediately below the table.

When the Systems filter is selected, space usage amounts are shown for the current time and last 24 hours, Pre-comp used, and configurable columns showing Compression Factor, Cleanable, and Capacity Thresholds for Warning and/or Critical states (by default, thresholds are set to 80% for warning and 90% for critical; they can also be set from the **Inventory > Systems** page **Edit** control). The Warning and Critical Capacity Thresholds columns can be sorted by ascending/descending controls and can also filtered by an entered value (greater, lesser, or equal to entered value).

The MTree page displays the type of MTree (which can be sorted by ascending/descending and filtered by MTree or Storage Unit), space usage amounts for Current Pre-Comp Usage, Quota, Quota Available, Quota Used % are shown. The Space Usage area in the Details Panel shows Pre-Comp, Post-Comp, Comp Factor: Last 24 hours, Last Week, Last 5 week Avg. Properties viewing and setting is supported as well as charting historical storage data. Note that Post-Comp data for an MTree can be determined only over a time interval (last 24 hours, last 7 days, etc.), not for a point in time.
The Space Usage amounts may not exactly match capacity totals reported by DD System Manager. Because of the polling delay of up to an hour, DD Management Center reporting will always lag. This is especially true if there is a lot of churn on the monitored system; the discrepancy will be more visible, and there is a possibility that DD Management Center may never catch up with DD System Manager capacity totals.

Aggregated totals of selected objects (Individual or aggregated systems or MTrees) in the master table (top) are shown below in the Space Usage details panel and graphed in the Charts and Trends panel. Detailed charting is shown for Space Usage, Consumed (Systems only), and Daily Written. Charting controls allow selectable time intervals by manipulating the slider to magnify an interval or clicking a fixed time range (1 day, 7 days, etc).

This guide assumes you are familiar with capacity terms, as introduced in the *EMC Data Domain Operating System Administration Guide*. See that guide, or the DD System Manager online help, for explanations of the terms.

**System Details Lightbox**

Use the System Details lightbox when you want to gather detailed operating information about specific components of a DD system.

The System Details lightbox is accessed from the Inventory > Systems, Replication > Overview, and the Capacity > Utilization and Capacity > Projected pages using the System details control. Open the System Details lightbox when in-depth information about the selected DD system is needed.

The Details page shows the operational status of various system components (such as the file system and protocols) using LED status indicators. Also provided are summaries of file system usage and capacity, and replication status and statistics for inbound and outbound replications. Charts for tracking space usage, consumption, and daily written data allow you to see historical usage trends.

The Charts page allows you to create charts to plot operational data about the system resources (CPU utilization or network throughput), file system and protocols activity, and replication data (viewable by automatic or on-demand type) for throughput, inbound, and outbound replications.

- The Stream Count chart shows the number of reopened read file streams in the past 30 seconds (r+), the number of active read streams (rd), the number of reopened write file streams in the past 30 seconds (w+), and the number of active write streams (wr).
- The Protocol Processing chart shows the number of operations per second.
- The Protocol Throughput chart shows the protocol throughput (amount of data that the file system can read from and write to the kernel socket buffer) and the wait time (time taken to send and receive 1 MB of data from the file system to the kernel socket buffer).

Charting controls allow selectable time intervals by manipulating the slider or clicking a fixed interval (hours, 1 day, 7 days, etc).

**Projected**

The Capacity > Projected page can help you plan future capacity needs, by:
Predicting when systems will run out of storage space
Determining future capacity needs by projecting historical and current trends
Estimating when a system will reach its system-specific warning/critical space usage thresholds

This page also provides tabular information for monitored systems. Each entry shows the system name, model, OS version, and a connection status icon with a pop-up containing a link to the Health > Alerts page. The space usage amounts (size, used, and free) for current, selected past and projected months are provided. A storage graphic depicts the system's capacity by percentage used, with color coding to show normal, warning and critical threshold levels.

Select the timeline to choose a specific month (past or future). This creates a date column for comparison analysis. Projections are based on historical data and require at least 15 daily data points to work. Informational messages are displayed if insufficient data prevents an accurate projection.

Table 29 Insufficient Data Messages

<table>
<thead>
<tr>
<th>Forecast Engine Output</th>
<th>DD Management Center Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient capacity used</td>
<td>The average space used in the last 7 days was less than 10%.</td>
</tr>
<tr>
<td>Negative slope</td>
<td>There was a large recent drop in the amount of space used.</td>
</tr>
<tr>
<td>No data</td>
<td>There were fewer than 15 daily usage points.</td>
</tr>
<tr>
<td>Forecast outside confidence level</td>
<td>The space used varies too greatly over the last 15 days.</td>
</tr>
<tr>
<td>Past forecast date</td>
<td>The usage trend was not consistent during last 15 days.</td>
</tr>
<tr>
<td>Insufficient R squared</td>
<td>A specific usage pattern could not be determined from recent data.</td>
</tr>
<tr>
<td>Not used</td>
<td>Data is no longer being added to the system.</td>
</tr>
</tbody>
</table>

Date column data (Current, and those selected using the timeline) can be sorted by amount of Used Space, Free Space, % Used, and Size in ascending or descending order.

Use the slider controls on the timeline to increase or decrease the date span.

Highlighting a system in the list activates controls for examining system details and launching the DD System Manager.

Replication

The Replication pages provide status and performance details about the replication pairs on managed DD systems.

- The Replication > Overview > All Pairs page lists each monitored DD system that has configured replication pairs. Expand an entry to see its inbound and outbound replications, and for these, expand to see the replication type: Automatic (DD system to DD system replications) and On-demand (client-initiated and controlled replication of DD Boost files), and expand those to see the pairs of that type. The Inbound and Outbound entries are shown only if there are applicable replications.

Use the column selector to display columns for replication status, number of pairs (totals for systems, inbound, and outbound replications), and a selectable/configurable time-interval for displaying historical replication data. Double-click a status error icon at the system level to open the System Details Lightbox, where
hovering over the Replication LED exposes a pop-up with a link to the Alerts page, filtered for the pairs in error. The Status error icon for a category (inbound, outbound, system) shows if any of its items has an error condition.

**Note**

Use the right triangle System control at the top left of the table to expand the inbound and outbound tiers to see all Automatic and On-Demand replications (if the system entries have not been expanded yet), and likewise to collapse all expanded entries.

When the Topology page is active, the site replication pairs are shown on a topology map.

- The Replication > Automatic page lists all monitored DD system replications for the types directory, collection, and MTree. The page banner displays the total count of monitored Automatic replications, and the table shows for each replication pair selectable columns for the status, source and destination systems, and performance data, such as lag time (the lag cell is red when lag duration is greater than or equal to the Critical threshold and yellow for Warnings; hover over the cell for detailed information about the lag threshold), lag trend (increasing – the data cannot be replicated within the lag threshold), steady, decreasing, or no arrow if the pair is suspended or in error), time over threshold (hover to see policy settings), bytes remaining, and status message text. The page-specific controls include Assign Properties and Lag Threshold Policy/Manage Lag Threshold Policies to set/manage alerting for when an Automatic Replication lag time exceeds the set time limit for critical and warning levels.

- The Replication > On-Demand page lists (DD Boost) file replications, showing for the pair: the last transfer status, source and destination storage units, and performance data for recent and completed replications. The table can organized by Pairs or Groups (toggle at top right).

- Historical data for completed replications can be by viewed for the past 24 hours, 7 days, 30 days, 90 days, or by setting a custom time frame. Details shown are for Pre-comp data replicated, completed and failed replicated files, percentage of failure, and the last error messages. For the group view, data for pairs are rolled up at each group level. Data for all pairs are summarized at the last line of the table.

**Note**

The number of completed and failed files can include file replications that the system retried up to four times due to generally recoverable failures. Consequently, the sum of the completed and failed file replications can be greater than the total number of file replications that were initiated by the DD Boost applications on the replication pair.

**Note**

For DD Boost (on-demand replication) monitoring, the DD system must be running DD OS 5.3.1 or later. Any DD system running older software will not display DD Boost replication pair associations between the source and destination systems on any of the file replication reporting pages, widgets, or reports.
Note

If the source or destination fields show an IP address instead of a host name, the DNS server configuration for the DD system must be modified. When configuring DD systems to monitor DD Boost (on-demand replication), ensure their DNS servers include configuration for both forward and reverse host name lookup. Without proper DNS server configuration, DD systems will not be able to translate from IP addresses to host names, and the source and destination paths will contain IP addresses instead of host names.

- The replication **Pair Details** control is active when a pair is selected and shows a lot of replication detail.
- The **System Details** control is active when a DD system entry is selected on the **Overview** page.
- The **Export CSV file** control sends the overview listing with performance data for the last 7 days to a file with comma-separated entries (for viewing in Excel, for example).

**Pairs**

The **Replication > Automatic Pairs** view (default view) is a tabular listing of all replication pairs, sorted by either the source system or group name. The tabular columns are user selectable and can show the replication source and destination systems, lag time, lag trend (increasing, decreasing, or steady), threshold policy, bytes remaining, last sync time, and status message.

**Cascades**

The **Replication > Automatic Cascades** view is a tabular listing of replication cascades. Expand and collapse a cascade to show or hide their pairs. The tabular columns are user selectable and can show the replication cascade's status, source and destination, lag trend, threshold policy, bytes remaining, last sync time, status message, type (MTree, collection, or Directory), and estimated completion time.

**Topology**

When the **Topology** view is selected on the **Replication > Overview** page, it shows the relationships of the site's configured replication contexts and uses color-coded status indicators and other map controls to allow the user to easily locate and drill-down to investigate error conditions.

Use the **Type** menu to select the replication types that are shown in the map work area (MTree, directory, collection, and On-demand files). If a replication type has not been configured among the site's replications, its check box in the menu is disabled. If a type is enabled but de-selected, those node relationships do not show on the map.

A slider on the map controls the scope of replication contexts that are shown in the work area display.

The inset is a miniature representation of the map and its scope is controlled by the slider manipulation. The inset itself can be selected and moved around to include or exclude systems in the map work area.

Replications status between systems are shown with color-coded directional lines, which will show red if any of the replications are in error. Mousing over the line shows the number of replication pairs and a count for each status levels.

Use the plus and search controls on a system's icon to expand to show an in-depth view of all the replication pairs that are configured. The minus control collapses this view.
The right panel lists the replicated pairs (of highlighted systems in the map work area or all contexts is nothing is highlighted), showing the type of context, source and destination systems, status, with a link to additional details. Selecting a context activates the **Pair Details** control.

**Replication Pair Details Lightbox**

Selecting a replication pair on any of the Replication pages activates the **Pair Details** control. Selecting **Pair Details** opens the Replication Pair Details lightbox, which shows a lot of information about the replication pair – last transfer status, source and destination systems, settings such as encryption, operational status, and color-coded icons showing capacity levels.

At the bottom of the page are charts for viewing historical activity for **Pair Characteristics** (plot performance factors such as pre-compression written, pre-compression replicated, replication compression factor, network bytes) and for all pairs except On-demand replications the **Lag Trend** (plot replication lag, replication lag thresholds, pre-compression written, and pre-compression remaining). Hover over the Thresholds check box to display the lag threshold settings.

**Note**

If a Storage Unit for a DD Boost replication pair shows the message, “SU is unresolved”, here are some possible reasons:

- The remote system is not registered with DD Management Center.
- Both systems are registered, but one is running a DD OS earlier than 5.3.1 and is not able to report the Storage Unit name.
- The remote host name is an IP address and cannot be matched to a registered host name.

Select the **Charts** tab to plot the elements of the selected replication (Pair Charts, System Charts, and Other Replications). Track pair characteristics, CPU utilization, data written, and network and replication throughput over time. Also available are options to track All Pairs Characteristics and Common Pairs Characteristics (which can show either Automatic replications only, On-demand Replications only, or All replication types). The All Pairs charts can show Incoming or Outgoing replication data for a system. The Common Pair Characteristics show a subset of data series that are common across both types of charts. The charts are vertically aligned for source and destination systems by the same time interval, allowing comparisons for both systems at any point in time.

**Reports**

The Reports feature lets you compile specific information about managed systems, based on three default template types (capacity, replication, and status) for either System or Multitenancy.

A wizard helps configure a template for the report’s content, schedule, and email distribution. A report can be generated directly from a template ad hoc and not saved, or it can be saved as a template for generating reports for later use.

If a user who is the owner of report templates is deleted from DD Management Center, the ownership of those templates is changed to the DD Management system administrator.
Note
For DD Boost (on-demand replication) monitoring, the DD system must be running DD OS 5.3.1 or later. Any DD system running older software will not display DD Boost replication pair associations between the source and destination systems on any of the file replication reporting pages, widgets, or reports.

Management

Configuring reports to notify recipients with information about managed objects reduces the need for users to log into DD Management Center to get a status update.

Use the Create Report Template wizard, which is started with the Add control, to create a template to generate reports.

After the report template is created, it is listed in the table where it can be viewed, edited, deleted, renamed, downloaded, and saved. The template can also generate a report, at will.

Selecting a report in the table shows a historical listing of its generated output in the Details panel. These reports can be viewed, searched, edited, and deleted.

Administration

The Administration area is where settings for DD Management Center are managed. The Administration module includes sections for permissions, groups, properties and settings.

Permissions

The Permissions pages (Assigned, Groups, Systems, Users) show the permissions of DD Management Center users by assigned role.

Permissions are a “triangle” of three components:
- The managed object (groups or systems)
- The user (local, NIS, or Active Directory)
- The DD System Manager role (Administrator, Backup Operator, or User)

The Permissions pages are also used to add, modify, and remove permissions from groups and systems.

Each of the views show the users, their assigned role and their effective role.

Groups

On the Administration > Groups page, the DD Management Center system administrator creates groups in a tree-like hierarchy for logically organizing DD systems.

Each tier of the hierarchy can contain one or more systems or subgroups. The Groups page left panel shows the created group hierarchy; selecting a group in this panel shows its contents (which can be subgroups or systems) in the right panel. Groups are shown as a folder icon. An information icon is displayed for systems that reside in more than one group; when you hover over it, the groups are listed.

There is only one root (/), but it can contain multiple groups (in the Add Group dialog, set the Path to /, add the group name in the text field; the group created is directly under root). Groups can contain nested groups and DD systems.
The structure of the hierarchy or the contents of the groups are changed with the Group edit controls (Add, Edit, and Delete).

Group creation and modification can only be performed by the DD Management Center system administrator. Any user can apply group designations and see the complete group structure, although RBAC permissions control which systems are displayed for a user.

### Table 30 Groups Page Icons

<table>
<thead>
<tr>
<th>Controls</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Group</td>
<td>Symbolizes a group containing DD systems or other groups. When subgroups are present, the expander icon is displayed to the left of the folder. Selecting the folder displays the members of the group in the Group Details panel.</td>
</tr>
<tr>
<td></td>
<td>Group with permissions applied</td>
<td>Indicates that this group is controlled by access permissions.</td>
</tr>
<tr>
<td></td>
<td>Membership details</td>
<td>Appears when a DD system belongs to more than one group. Hover to view the names of groups of which this DD system is a member.</td>
</tr>
</tbody>
</table>

### Properties

Properties provide information to help you classify systems and the data contained in MTrees and Replication contexts for searching, filtering, and organizing.

For example, you could assign properties to help filter the list of DD systems in the Inventory > Systems page and narrow the scope of output produced by a dashboard widget or generated report.

Properties are organized and managed by type (System, MTree, and Replication), and selecting a property type displays a catalog of its active properties. The value of a property can be a string, a number, a boolean, or a fixed-value string.

Select Administration > Properties to see a list of all assigned properties for System, MTree, and Replication.

The following table shows the controls for the different types of properties.

### Table 31 Property Controls

<table>
<thead>
<tr>
<th>Controls</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>System property</td>
<td>Denotes a fixed, pre-set property that cannot be edited. Selecting this control shows all of its created values in the Values column. The default properties, which cannot be modified, are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• System – Model, OS, Domain Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MTrees – Replicated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Replication – no default properties</td>
</tr>
<tr>
<td></td>
<td>User property</td>
<td>Denotes a user-defined property. When selected, can be edited or deleted, and all of its created values are shown in the Values column.</td>
</tr>
<tr>
<td></td>
<td>Property details</td>
<td>Opens the Property Assignment dialog, which lists the type of property, the name of the element (for example, system name), and assigned value. When opened in the Values column, shows only entities for that value.</td>
</tr>
</tbody>
</table>
### Settings

The Settings view contains pages where you manage and configure settings for DD Management Center.

### Inventory

This area has a link to the inventory of Data Domain systems that are being managed by the DD Management Center, as described in Systems on page 119.

### Systems

The Inventory > Systems page lists the DD systems being managed by DD Management Center. The columns show the system’s host name, status, model, and OS. You can customize the display of these columns using the Show Columns control, at the right. If properties have been created for a system, you can also add those as columns.

Selecting the system status icon for a system with a connection issue produces a detailed status notification panel at the bottom of the systems list.

Selecting a DD system in the table provides additional details for the system at the bottom of the page. They include:

- **Configuration** – Shows the system’s host name, time zone, inbound and outgoing firewall IP address and port settings, as well as warning and critical threshold level settings for the system’s storage capacity.

- **Properties** – Shows the properties assigned to the system and their values. To assign a property or change an existing property’s value, select Edit, then the Properties tab, and enter the value in the property field.

- **Groups** – Shows the names of groups of which this system is a member. To assign a group to this system or remove the system from a group, select Edit, then the Group tab, and select/deselect the group name.

**Note**

If the table is empty, you need to add systems to the DD Management Center.

For any icon for systems exhibiting abnormal status, select the icon or system entry to see a status banner detailing the problem.

Controls for adding DD systems, editing an existing DD system’s settings, viewing a selected DD systems’ details, upgrading DD systems, and launching the System Manager are also included on this page.

### Communication Between DD Management Center and DD Systems

When adding a DD system to the DD Management Center, the IP address or hostname of the DD system you provide in the Add System wizard is used, along with valid DNS entries to set up communication between the DD Management Center and the DD system.
After contact is established with the DD system, its hostname is used from that point onward, unless proxy settings were provided in the wizard.

If communication cannot be established because the DNS entry does not exist or is incorrect for either the DD Management Center or the DD system:

- Add or correct the DNS entry for the DD Management Center or the DD system, or
- If a proxy is not used between the DD Management Center and the DD system, use the proxy settings as a workaround for a missing or incorrect DNS mapping by providing the DD system IP address as the outgoing proxy address and/or the DD Management Center IP address as the incoming proxy address.

To troubleshoot communication with the DD system:

- Use the command `net ping hostname` from both the DD Management Center and the DD system. This command will report the problems that need to be fixed, but may not work if the firewall is causing the blocking.
- Use the command `managed-system sync`. All DD systems are synced with this command (but it will consume additional network bandwidth). Without this command, a sync is run automatically every hour.
This appendix provides a reference for the CLI (command-line interface) of the DD Management Center.

- **Overview of the CLI** ................................................................. 122
- **DD Management Center managed-system Commands** ....................... 122
- **DD Management Center task Commands** ................................... 126
- **Command-only Functionality** .................................................. 129
Overview of the CLI

DD Management Center has a command-line interface (CLI) that was derived from the Data Domain Operating System (DD OS) and modified to support some management tasks and the virtual machine environment. This section describes the DD Management Center CLI.

The main user interface for DD Management Center is the web-based graphical user interface (GUI). It is recommended that you use the GUI for system management tasks; however, a few system administration tasks for the DD Management Center system itself require that you use the CLI.

The DD Management Center CLI differs from the DD OS CLI in the following ways:

- Additional system management commands (managed-system and task) specific to DD Management Center that perform the basic registration, administration, and job management functions for the DD Management Center.
- Some CLI system administration commands derived from the DD OS are modified to support DD Management Center. The command output for many of these commands omits information that is not applicable to the system’s role as a management virtual appliance instead of a storage appliance.
- Some CLI commands derived from DD OS have limited arguments because a DD Management Center does not directly manage storage.
- Some DD OS commands that perform tasks for managing storage (and are therefore not useful or supported in DD Management Center) were removed.

For detailed information on any CLI command, start a secure shell session (ssh), and type `?` at the CLI prompt to see the online help.

DD Management Center managed-system Commands

The DD Management Center managed-system CLI commands let you add and remove systems from management, change their proxy host settings, and suspend, resume, or synchronize data collection.

Note

You can also use the Web interface to perform these actions.

managed-system add

managed-system add hostname [force] [inbound-proxy proxy-host [inbound-proxy-port proxy-port]] [outbound-proxy proxy-host [outbound-proxy-port proxy-port]]

This command adds a Data Domain system into the set of systems that are managed by the current DD Management Center. The command prompts you to:

1. Verify that the certificate obtained from the host is valid.
2. Enter the sysadmin password for the system being added to management.
Argument Definitions

**force**
If the system is already being managed by another DD Management Center, the current DD Management Center assumes management of the Data Domain system from the other DD Management Center, and the Data Domain system entry in the other DD Management Center is placed in the unmanaged state. If the system is already being managed and you omit this argument, the command fails.

**hostname**
The hostname of the system.

**inbound-proxy proxy-host**
Inbound proxy hostname if the incoming connection from the Data Domain system is through a proxy.

**inbound-proxy-port proxy-port**
Inbound proxy port number if the incoming connection from the Data Domain system is through a proxy.

**outbound-proxy proxy-host**
Outbound proxy hostname if the connection from the DD Management Center to the Data Domain system is through a proxy.

**outbound-proxy-port proxy-port**
Outbound proxy port number if the connection from the DD Management Center to the Data Domain system is through a proxy.

---

**Note**
The proxy options are equivalent to the firewall options in the graphical user interface.

---

**Example**

```
# managed-system add host1234.mycompany.com
Do you want to trust this certificate? Are you sure? (yes|no) [no]: yes
** Once added, all "admin" role users on this management center will operate on
"host1234.mycompany.com" system with "admin" role. To allow
"host1234.mycompany.com" to be managed by this management center, Enter sysadmin password:
ok, proceeding.
```

**managed-system check-connection**

```
managed-system check-connection hostname [inbound-proxy proxy-host [inbound-proxy-port proxy-port]] [outbound-proxy proxy-host [outbound-proxy-port proxy-port]]
```

This command checks whether the specified host is reachable and available to be managed by this DD Management Center. Use `managed-system add` to add the system to the set of systems that this DD Management Center is managing.

**Argument Definitions**

**hostname**
The hostname of the system.
inbound-proxy  \textit{proxy-host}  
   Inbound proxy hostname if the incoming connection from the Data Domain system is through a proxy.

inbound-proxy-port  \textit{proxy-port}  
   Inbound proxy port number if the incoming connection from the Data Domain system is through a proxy.

outbound-proxy  \textit{proxy-host}  
   Outbound proxy hostname if the connection from the DD Management Center to the Data Domain system is through a proxy.

outbound-proxy-port  \textit{proxy-port}  
   Outbound proxy port number if the connection from the DD Management Center to the Data Domain system is through a proxy.

\textbf{managed-system delete}  
managed-system delete  \textit{hostname}  
   This command removes the specified Data Domain system from DD Management Center management.

\textit{hostname}  
   The hostname of the system.

\textbf{managed-system resume}  
managed-system resume  \textit{hostname}  
   This command resumes data collection from the specified Data Domain system if collection was suspended by \textit{managed-system suspend}.

\textit{hostname}  
   The hostname of the system.

\textbf{managed-system set}  
managed-system set  \textit{hostname} \texttt{[inbound-proxy \{proxy-host\|none\}]} \texttt{[inbound-proxy-port \{proxy-port\|default\}] \texttt{[outbound-proxy \{proxy-host\|none\}] \texttt{[outbound-proxy-port \{proxy-port\|default\}]]}}  
   This command sets or changes proxy server information for a managed system.

\textit{hostname}  
   The hostname of the system.

\textit{inbound-proxy \{proxy-host\|none\}}  
   Inbound proxy hostname if the incoming connection from the Data Domain system is through a proxy. Use \texttt{none} to remove the proxy host and clear the proxy port.

\textit{inbound-proxy-port \textit{proxy-port}}  
   Inbound proxy port number if the incoming connection from the Data Domain system is through a proxy.
outbound-proxy \{proxy-host\{none\}
Outbound proxy hostname if the connection from the DD Management Center to the
Data Domain system is through a proxy. Use none to remove the proxy host and
clear the proxy port.

outbound-proxy-port \{proxy-port\{default\}
Outbound proxy port number if the connection from the DD Management Center to
the Data Domain system is through a proxy. Use default to reset the proxy port
number.

managed-system show

managed-system show \[{all | hostname}]\]
This command prints basic information for a list of managed systems or the specified
system.

Argument Definitions

all
  Report about all systems. This is the default.

hostname
  The hostname of the system.

The report lists the systems by hostname and includes their serial number, management
state, online status, DD OS version, and the latest synchronization time.

Management States
This list describes the possible values of the management State column.

adding
  The DD Management Center is in the process of assuming management of the
  system.

suspended
  The DD Management Center is not currently managing and collecting information
  about the system. Systems go into this state if you use managed-system
  suspend to stop collecting data or a licensing problem prevents data collection.

managed
  The DD Management Center is managing the system.

unmanaged
  The DD Management Center previously managed the system but another DD
  Management Center has assumed management.

deleting
  The DD Management Center is in the process of ending management of the system.

Management Status Values of “Managed” Systems
This list describes the possible management Status values when a system is in the
managed state.

online
  Communication with the managed system is normal.

not-responding
  The DD Management Center has not been able to send messages to the managed
  system, or communication has failed in both directions, for more than 30 minutes.
not-transmitting
The managed system has not responded to messages from the DD Management Center for more than 120 minutes.

upgrading
The managed system is in the process of upgrading DD OS.

upgrading, not-responding
The managed system is in the process of upgrading DD OS and is not communicating with the DD Management Center.

managed-system suspend
managed-system suspend hostname
This command suspends data collection from the specified host. If you do not want the Management Center to show a system as unreachable while it is shut down for maintenance, you can use this command to suspend monitoring.

Argument Definitions
hostname
The hostname of the system.

managed-system sync
managed-system sync
This command synchronizes and processes both current and historical data from all managed systems.

DD Management Center task Commands
The Health > Jobs page in the Web interface displays information about jobs that have been initiated from the DD Management Center, including jobs still in progress and jobs that have completed, whether successfully or not. Jobs include actions such as adding and removing systems from management. For more information about jobs, see the Data Domain Management Center User Guide.

In the CLI, jobs are called tasks. The DD Management Center task CLI commands let you cancel, pause, resume, and generate reports about jobs. Regular users may work with tasks that they created. The sysadmin user may work on all tasks.

task cancel
task cancel task-id
This command terminates a task.

Argument Definitions
task-id
The ID number for the task, as reported by one of the task show commands.

task pause
task pause task-id
This command suspends a task. Use task resume to continue the task.
Argument Definitions

**task-id**
The ID number for the task, as reported by one of the `task show` commands.

---

**task resume**

`task resume task-id`

This command continues a task that you suspended with `task pause`.

**Argument Descriptions**

**task-id**
The ID number for the task, as reported by one of the `task show` commands.

---

**task show active**

`task show active [type {inventory | replication | upgrade}] [user user]`

This command reports about top-level running tasks. You can filter the results by using `type` with one of the keywords, or with the `user` keyword.

**Argument Definitions**

**type {inventory | replication | upgrade}**
Filter the results to show only tasks of the specified type.

**user user**
Filter the results to show only tasks owned by the specified user.

---

**task show detailed**

`task show detailed task-id`

This command prints a detailed report about a single task and its subtasks.

**Argument Definitions**

**task-id**
The ID number for the task, as reported by one of the `task show` commands.

---

**task show detailed-active**

`task show detailed-active [type {inventory | replication | upgrade}] [user user]`

This command prints a detailed report about active tasks and their subtasks. You can filter the results by using `type` with one of the keywords, or with the `user` keyword.

**Argument Definitions**

**type {inventory | replication | upgrade}**
Filter the results to show only tasks of the specified type.

**user user**
Filter the results to show only tasks owned by the specified user.
task show detailed-history

task show detailed-history [last n {hours | days | weeks | months}] [start MMDDhhmm[[CC]YY] end MMDDhhmm[[CC]YY] [type {inventory | replication | upgrade}] [user user]

This command prints a detailed report about completed tasks and their subtasks. You can filter the results by using type with one of the keywords, or with the user keyword. You can filter the results by time by using the last, start, and end keywords. The default reporting period is the past 24 hours.

Argument Definitions

last n {hours | days | weeks | months}
   Filter the results to show only tasks that finished during the previous n hours, days, weeks, or months.

start MMDDhhmm[[CC]YY] end MMDDhhmm[[CC]YY]
   Filter the results to show only tasks that finished during the specified interval. MMDD indicates month and day. hhmm indicates hours and minutes in 24-hour format. To specify midnight between Sunday night and Monday morning, use mon 0000. To specify noon on Monday, use mon 1200. CC is the first two digits of the year. YY is the last two digits of the year.

type {inventory | replication | upgrade}
   Filter the results to show only tasks of the specified type.

user user
   Filter the results to show only tasks owned by the specified user.

---

task show history


task show history [last n {hours | days | weeks | months}] [start MMDDhhmm[[CC]YY] end MMDDhhmm[[CC]YY] [type {inventory | replication | upgrade}] [user user]

This command prints a brief report about completed tasks. You can filter the results by using type with one of the keywords, or with the user keyword. You can filter the results by time by using the last, start, and end keywords. The default reporting period is the past 24 hours.

Argument Definitions

last n {hours | days | weeks | months}
   Filter the results to show only tasks that finished during the previous n hours, days, weeks, or months.

start MMDDhhmm[[CC]YY] end MMDDhhmm[[CC]YY]
   Filter the results to show only tasks that finished during the specified interval. MMDD indicates month and day. hhmm indicates hours and minutes in 24-hour format. To specify midnight between Sunday night and Monday morning, use mon 0000. To specify noon on Monday, use mon 1200. CC is the first two digits of the year. YY is the last two digits of the year.

type {inventory | replication | upgrade}
   Filter the results to show only tasks of the specified type.

user user
   Filter the results to show only tasks owned by the specified user.
Command-only Functionality

The following commands provide functionality not supported by the graphical user interface:

- managed-system resume host
- managed-system suspend host
- managed-system sync
- system show performance [duration duration {hr | min}] [interval interval {hr | min}]
- system show serialno detailed
  The GUI shows the current serial number for DDSM, but does not support the detailed version.
- system show space
- system show stats [view {net | iostat | sysstat}] [custom-view view-spec,...] [interval nsecs] [count count]