HEAT software

HEAT PatchLink DataCenter for Microsoft® System Center Version 8.3

User Guide

Table of Contents

HEAT software

HEAT software

HEAT software

HEAT software

HEAT software

Notices

Copyright Information

Lumension Security Inc.,
8660 East Hartford Drive, Suite 300
Scottsdale, AZ 85255
Phone: +1 888.725.7828
Fax: +1 480.970.6323
E-mail: info@lumension.com

HEAT®software

Trademark Information

PatchLink®, PatchLink® for System Center, PatchLink® DataCenter, PatchLink® DeskTop, PatchLink® Update™, Lumension®, Lumension® EMSS, their associated logos, and all other Lumension trademarks and trade names used here are the property of Lumension Security, Inc. or its affiliates in the U.S. and other countries.

HEAT®, HEAT® Content Wizard, their associated logos, and all other HEAT trademarks and trade names used here are the property of HEAT Software USA Inc. or its affiliates in the U.S. and other countries.

RSA Secured® is a registered trademark of RSA Security Inc.

In addition, any other companies' names, trade names, trademarks, and products mentioned in this document may be either registered trademarks or trademarks of their respective owners.

Some or all modules, features or components of this intellectual property are protected by one or more of U.S. Patent Nos. 6,990,660, 7,278,158, 7,487,495, and 7,823,147; other patents are pending, and other non-U.S. patents may apply.

Feedback

Your feedback lets us know if we are meeting your documentation needs. E-mail the HEAT Software Technical Publications department at techpubs@heatsoftware.com to tell us what you like best, what you like least, and to report any inaccuracies.

Preface

About This Document

This User Guide is a resource written for all users of HEAT PatchLink DataCenter for Microsoft® System Center . This document defines the concepts and procedures for installing, configuring, implementing, and using HEAT PatchLink DataCenter for Microsoft® System Center .

Tip: HEAT documentation is updated on a regular basis. To acquire the latest version of this or any other published document, please refer to the HEAT Customer Portal (http://portal.lumension.com/).

Typographical Conventions

The following conventions are used throughout this documentation to help you identify various information types.

Table 1: Typographical Conventions

Convention	Usage
bold	Buttons, menu items, window and screen objects.
bold italics	Wizard names, window names, and page names.
italics	New terms, options, and variables.
`MONOSPACE UPPERCASE`	Keyboard keys.
`BOLD UPPERCASE`	SQL Commands.
`monospace`	File names, path names, programs, executables, command syntax, and property names.

HEAT®software

Contacting HEAT Software

Arizona	Ireland	Luxembourg
8660 East Hartford Drive	HEAT Software Ireland Ltd.	Lumension Security SA
Suite 300	Lyrr Building, Second Floor	Atrium Business Park
Scottsdale, AZ 85255	Mervue Business & Technology	Z.A Bourmicht
United States of America	Park	23, rue du Puits Romain
	Mervue, Galway	L-8070 Bertrange
Phone: +1 888 725 7828	Ireland	Luxembourg
Phone: +1 480 970 1025		
Fax: +1 480 970 6323	Phone: +353 91 44 8980	Phone: +352 265 364 11
	Fax: +353 91 76 6722	Fax: +352 265 364 12

HEAT Support

phone:
+1 480 970 1025 (USA)
+1 877 713 8600 (USA - legacy Sanctuary products)
+353 9142 2999 (EMEA)
+44 800 012 1869 (UK)
+61 (02) 8223 9810 (Australia)
+852 3071 4690 (Hong Kong)
+65 6622 1078 (Singapore)

submit a ticket:
Registered users can open a support ticket via the customer portal (http://portal.lumension.com/).

HEAT customers without a support account should contact our support team (support@lumension.com) to have an account created.

Note: For additional contact information, please visit the Contact HEAT page at http://www.lumension.com/contact-us.aspx.

Chapter

1

HEAT PatchLink DataCenter Overview

In this chapter:

• HEAT PatchLink DataCenter at a Glance

HEAT PatchLink DataCenter Server for Microsoft® System Center audits and remediates software and system configuration vulnerabilities within your network. It can also be used for network-wide installation of content non-related to vulnerabilities, such as software or service packs.

To accomplish this task, HEAT PatchLink DataCenter uses two main components: The *HEAT Patch Manager DataCenter Server* and the *HEAT PatchLink DataCenter Agent for Linux/UNIX.*

HEAT PatchLink DataCenter uses the HEAT Patch Manager DataCenter Server to download content and then deploys it throughout your network. Content includes data that identifies vulnerabilities, patches that remediate them, and various other types of software and service packs. Content is deployed with assistance from the HEAT PatchLink DataCenter Agent for Linux/ UNIX.

The agent scans its host endpoint via a Discover Applicable Updates task, which takes a system inventory of endpoint software, hardware, and system configuration settings. The Discover Applicable Updates results are sent back to the server, which compares these results with a list of known vulnerabilities. Based on these results and administrator input, the server deploys content as needed.

/HEAT®software

HEAT PatchLink DataCenter at a Glance

You can use HEAT PatchLink DataCenter Server for Microsoft System Center to install patches and other software on your network endpoints.

Benefits

- Identifies endpoint vulnerabilities and remediates them by installing content (such as software and patches).
- Scans agent-managed endpoints for an inventory of their hardware and software.
- Lets you deploy patches, software, and other types on content to endpoints.
- Lets you establish Mandatory Baselines, which are content standards applied to endpoint groups that monitor endpoints to ensure defined content is always installed.
- Adds new HEAT PatchLink DataCenter-related reports, agent policies, default options, widgets, access rights, and email notifications.

Chapter

2

Getting Started with HEAT PatchLink DataCenter

In this chapter:

• The HEAT PatchLink DataCenter Server for Microsoft System Center Workflow

Use HEAT PatchLink DataCenter Server for Microsoft® System Center to remotely installs patches and other software on your managed network endpoints. To get started with HEAT PatchLink DataCenter, you should install the module and then perform several other tasks essential to its operation.

After performing these tasks, you will be able to deploy patches and other content to endpoints in your network, thus remediating potential exploits.

Following completion of these initial tasks, take some time to grow accustomed to the HEAT PatchLink DataCenter. You will continue to perform these tasks, plus many others. HEAT PatchLink DataCenter contains many features and functions, and by learning the environment, you can secure your network quickly and efficiently.

The HEAT PatchLink DataCenter Server for Microsoft System Center Workflow

To use HEAT PatchLink DataCenter Server for Microsoft System Center (HEAT PatchLink DataCenter), all HEAT PatchLink DataCenter for Microsoft System Center components must be installed, along with the HEAT PatchLink DataCenter module. After installing all necessary components, review this chart to understand the HEAT PatchLink DataCenter work flow.

Refer to the following flow chart to determine tasks when using the HEAT PatchLink DataCenter module within HEAT PatchLink DataCenter.

Create Groups

Create *groups* containing HEAT PatchLink DataCenter endpoints in preparation for *deployment*. A group associates similar endpoints for the purpose of deploying content to multiple endpoints. For additional information, refer to Creating New Groups on page 20.

HEAT® software

Create Agent Policy Sets	Create new agent policy sets (or edit existing policy set for HEAT PatchLink DataCenter functions) and apply them to HEAT PatchLink DataCenter groups. Agent policy sets are a compilation of values that govern agent behavior. New settings for agent policy sets are added after installing HEAT PatchLink DataCenter. For additional information, refer to Apply Agent Policy Sets on page 22.
View Vulnerabilities and Deploy Content	View network vulnerabilities and then deploy content, which are patches and other software, to managed endpoints. First, view network vulnerabilities. Agents detect vulnerabilities by scanning endpoints for signatures that indicate vulnerabilities are present. Then, remediate vulnerabilities using a deployment, which triggers the agent to download selected content from the HPL Server. For additional information, refer to Viewing and Remediating Vulnerabilities on page 23.
Add Content to Mandatory Baseline	After initial vulnerabilities are remediated, you can define a Mandatory Baseline. This baseline is a selection of user-defined content that must always be installed on all group endpoints. If an endpoint falls out of compliance, the Mandatory Baseline ensures the endpoint is patched back into compliance via automatic deployment.
Define Default Module Settings	Define default HEAT PatchLink DataCenter settings. New default settings are added to HEAT PatchLink DataCenter for Microsoft System Center after HEAT PatchLink DataCenter is installed. New settings include new access roles, email notifications, and deployment options. For additional information, refer to the following topics:

- Defining Default Deployment Options on page 25
- Creating Email Notifications on page 25
- Editing Custom Roles on page 26

Logging in to PatchLink DataCenter Server

1. Open the System Center Configuration Manager Console.
2. Select any of the workspaces available.
3. Navigate to any of the HEAT nodes available in the tree.
4. Enter your credentials.

Creating New Groups

After installing the HEAT PatchLink DataCenter components, create a new group for your HEAT PatchLink DataCenter endpoints. By placing your HEAT PatchLink DataCenter endpoints in a group (or multiple groups), you can manage them collectively. For example, you deploy content to all HEAT PatchLink DataCenter with one deployment by using groups.

Figure 1: Group Diagram

Create and configure groups from the *Groups* page.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **Browser** tree, select **Custom Groups**.

   Groups are arranged within a tree structure. You can place your new group anywhere within the custom group hierarchy.

   Note: The group you create is added as a child group to the group selected within the directory tree.

3. Create a group.

   a) From the **View** list, select **Group Membership**.
   b) Click **Create**.
   c) In the **Name** field that displays, type a group name.
   d) In the **Description** field that displays, type a description.
   e) Click the **Save** icon.

4. Add endpoints to the group.

   a) From the **View** list, select **Endpoint Membership**.
   b) Click **Membership**.
   c) Assign endpoints to the group.

      For more detailed information, refer to Adding Endpoints to a Group on page 160.
   d) Click **OK**.

5. Define the group's settings.

   Group settings contain additional group controls.

   a) From the **View** list, select **Settings**.
   b) Define the settings.

      For more detailed information, refer to Editing Group Settings on page 212.
   c) Click **Save**.

Result: The group is created.

After Completing This Task:
Continue to Apply Agent Policy Sets on page 22.

HEAT software

Apply Agent Policy Sets

After you create a group, create and assign an agent policy set to govern the group endpoint behavior. Agent policy sets can control endpoint communications, hours of operations, and so on.

Prerequisites:

Complete Creating New Groups on page 20.
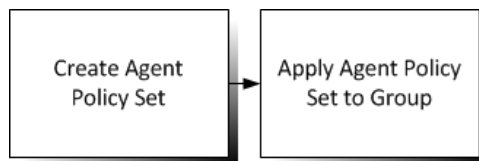
Figure 2: Install Server Module

Create agent policy sets using the *Agent Policy Sets* page, and then assign them to a group using the *Groups page.*

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Agent Policy Sets**.

2. Click **Create** to create an agent policy set.
   For additional information, refer to Creating an Agent Policy Set on page 230.

3. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

4. Select **Manage** > **Groups**.
   Step Result: The *Groups* page opens.

5. From the **View** list, select **Agent Policy Sets**.
   Step Result: The *Agent Policy Sets* view opens.

6. From the **Browser** tree, select the group you created.

7. Click **Assign** to assign the agent policy set to your created group.
   For additional information, refer to Assigning an Agent Policy Set to a Group on page 197.

Result: The agent policy set is created and assigned.

After Completing This Task:

Continue to Viewing and Remediating Vulnerabilities on page 23.

Viewing and Remediating Vulnerabilities

After installing the HEAT PatchLink DataCenter module server and endpoint components, your network endpoints complete their first Discover Applicable Updates task, which detect vulnerabilities. Following this task, you can then view vulnerabilities in your network and then deploy patches and other content to resolve them.

Prerequisites:

Complete Apply Agent Policy Sets on page 22.
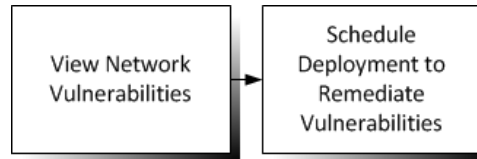
Figure 3: Viewing and Remediating Vulnerabilities

1. View dashboard widgets, vulnerabilities, and reports to identify vulnerabilities in your network.

   Dashboard widgets and reports provide detailed graphs and statistics about the state of your network. Reviewing this information provides insight about the actions required to secure your network. For additional information, refer to the following documentation:

   • To see an overview of how many vulnerabilities are in your network, view *The Dashboard*. View the dashboard from the **Assets and Compliance** workspace and select **Dashboard**.
   • To view the vulnerabilities on a specific endpoint, view *The Endpoint Details Page*. View the *Endpoint Details* page from the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter for Microsoft System Center** > **Endpoints** and click on an endpoint link.
   • To view the specific vulnerabilities in your network, view *The Content Pages List*. View this page from the **Software Library** workspace and select **HEAT PatchLink DataCenter for Microsoft System Center** > **Security Updates** > **All Security Updates**.
   • To view a report of vulnerabilities in your network, view *Generating a Report*. To generate reports, go to the **Monitoring** workspace, select **HEAT PatchLink DataCenter for Microsoft System Center** > **Reporting** > **Standard Reports**, select a report, and click **Generate Report**.

2. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **Security Updates** > **All Security Updates**.

3. From the list, select the vulnerabilities you want to deploy.

   Tip: Use the page filters to find vulnerabilities applicable to your endpoints.

HEAT software

4. Click **Deploy** to remediate vulnerabilities.

   Remediate network vulnerabilities by deploying content that fix identified vulnerabilities. For additional information, refer to Using the Deployment Wizard on page 303.

Result: The deployment is scheduled and will begin at the scheduled time. Completion time of the deployment varies dependent on size.

After Completing This Task:

Continue to Adding Content to a Mandatory Baseline on page 24.

Adding Content to a Mandatory Baseline
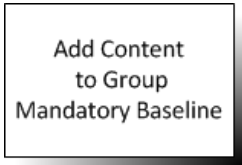
Each group in HEAT PatchLink DataCenter for Microsoft System Center has a Mandatory Baseline, which is a list of content that must be installed on the group's endpoints at all times. By default, this baseline is empty. However, you can add patches, software, and other content to this baseline. After adding content to the baseline, HEAT PatchLink DataCenter for Microsoft System Center continually checks group endpoints for the content's presence. If a group endpoint is found to not have content included in the Mandatory Baseline, HEAT PatchLink DataCenter for Microsoft System Center automatically deploys that content to the endpoint.

Prerequisites:

Complete Viewing and Remediating Vulnerabilities on page 23.

Figure 4: Adding Content to Mandatory Baselines

Add content to a Mandatory Baseline from the *Groups* page.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **Browser** tree, select the group you created earlier.

3. From the **View** list, select **Mandatory Baseline**.

4. Click **Manage** to add content.

   For additional information, refer to Adding Content to Mandatory Baselines on page 170.

5. Click **OK**.

Result: Content is added to the group Mandatory Baseline.

After Completing This Task:

Continue to Defining Default Deployment Options on page 25.

Defining Default Deployment Options
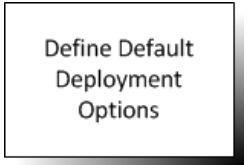
After you install HEAT PatchLink DataCenter, a **Deployments** tab is added to the **Options** page. Configure this tab to define the default values for the **Deployments Wizard**.

Prerequisites:

Complete Adding Content to a Mandatory Baseline on page 24.

Figure 5: Define Default Deployment Options

Define default deployment options from the **Options** page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Options**.

2. Select the **Deployments** tab.

3. Define the default deployment options.

   For additional information, refer to Configuring the Deployments Tab on page 67.

4. Click **Save**.

Result: The default deployment options are defined.

After Completing This Task:

Continue to Creating Email Notifications on page 25.

Creating Email Notifications

After installing HEAT PatchLink DataCenter, two new email notification types are added: New Vulnerabilities and Deployment Failure. To use these new notifications, edit your defined email addresses or create new ones.

Prerequisites:

Complete Defining Default Deployment Options on page 25.

Figure 6: Create Email Notifications

HEAT®software

Create email notifications from the ***Email Notifications*** page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Email Notifications**.

2. For each defined email address, select one of the new notification types available after installation of HEAT PatchLink DataCenter.

   Tip: For more information on how to define a new address and email notifications, refer to Creating Email Notifications on page 80.

3. Click **Save**.

4. Click **OK**.

Result: The email addresses you edited are configured to receive the new email notifications.

After Completing This Task:

Editing Custom Roles

After installing HEAT PatchLink DataCenter, new access rights are added for new features. To update custom roles for these features, edit your roles.

Prerequisites:

Edit custom roles from the ***Users and Roles*** page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Security** > **Users and Roles**.

2. Select the ***Roles*** tab.

3. From the page list, click the edit icon for the custom role to which you want to add access rights.

   Step Result: The ***Edit Role*** dialog opens.

4. Select the ***Access Rights*** tab.

5. Define the HEAT PatchLink DataCenter access rights.

6. Click **OK**.

Chapter

3

Using the HEAT PatchLink DataCenter Console

In this chapter:

• Common Functions
• The Dashboard

Within the HEAT PatchLink DataCenter for Microsoft® System Center console, you can use a number of common functions to navigate and operate the system. After you log in, HEAT PatchLink DataCenter opens to the *Dashboard*.

HEAT PatchLink DataCenter for Microsoft System Center performs the following functions:

• Endpoint Detection
• Agent Installation
• Endpoint Management
• Endpoint Grouping
• Agent Policy Set Creation
• User and Role Creation and Management
• Server Module Management
• Report Generation

HEAT PatchLink DataCenter for Microsoft System Center consists of a browser-based management console, which provides access to system management, configuration, reporting, and deployment options.

Common Functions

HEAT PatchLink DataCenter for Microsoft System Center uses standard Web browser conventions and unique conventions. Familiarize yourself with these conventions to facilitate efficient product use.

From the **Navigation Menu** and system pages, you can access all features and functions you are authorized for.

HEAT®software

Common Conventions

The Web console supports user interface conventions common to most Web applications.

Table 2: Common User Interface Conventions

Screen Feature	Function
Entry Fields	Depending on text, type data into these fields to either: • Retrieve matching criteria • Enter new information
Drop-Down Menus	Display a list of selectable values when clicked.
Command Buttons	Perform specific actions when clicked.
Check Boxes	A check box is selected or cleared to: • Enable or disable a feature • Initiate functions for list items Some lists include a **Select All** check box for selecting all items, including overflow items.
Radio Buttons	Select the button to select an item.
Sort	Data presented in tables can be sorted by clicking column headers. Columns can be sort in the following orders: • Ascending (default) • Descending
Mouseovers	Move your mouse over an item to display a text description.
Auto Refresh	Some pages feature an **Auto Refresh** check box. Select the check box to automatically refresh the page every 15 seconds.
Scrollbars	Drag scrollbars to see additional data.
Tabs	Select different tabs to display hidden information.

Tip: Most pages support right-click.

List Pages

Most pages feature lists of selectable items. These items represent different product features that can be edited using menus and buttons.
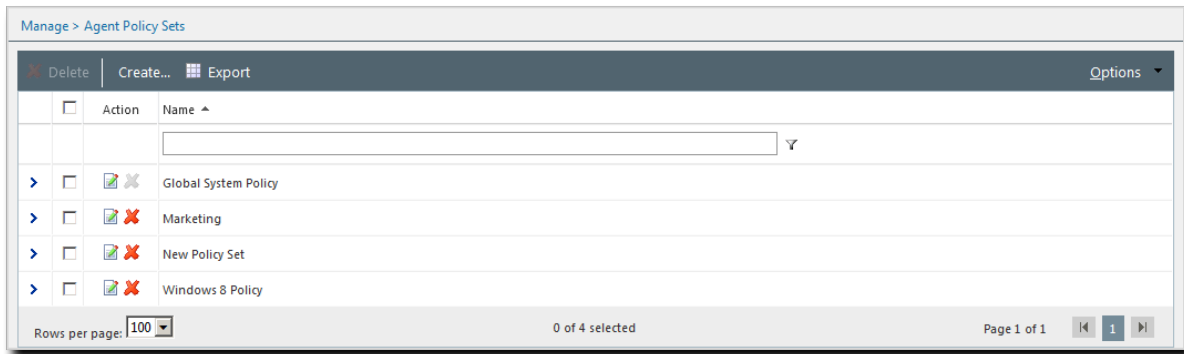
Figure 7: List Page

To select a single list item:

- Select a check box.
- Click a list row.

To select multiple list items:

- Select the **Select All** check box.
- Select multiple, concurrent items by using `SHIFT+Click` and mousing over list rows.

Toolbars

Toolbars appear on most Web console pages. They contain menus and buttons you can use to initiate page features.
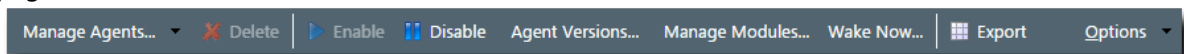
Figure 8: Toolbar

- The menus and buttons displayed vary according to page.
- Click the available menus and buttons to use them.
- User roles determine which buttons are available.

The Options Menu

Toolbars feature an **Options** menu. You can use these options to change how the page displays information.

Table 3: Options Menu Items

Option	Description
Show results on page load	Toggles automatic page results on and off. • When enabled, the page list automatically populates with results. • When disabled, you must define page filters and click **Update View** before results populate. For more information, see Filters on page 30.
Save as default view	Saves the current page settings as the default view.
Clear default view	Resets the saved view to the system default.
Show Filter Row[1]	Toggles the **Filter Row** on and off. For additional information, refer to Using Filter Rows on page 33
Show Group By Row[2]	Toggles the **Show Group By Row** on and off. For additional information, refer to Group By on page 35.
Enable Copy to Clipboard[3]	Toggles the ability to select text for clipboard copy.

1. This option title changes to **Hide Filter Row** when toggled.
2. This option title changes to **Hide Group By Row** when toggled.
3. Selecting this option disables other features, such as right-click context menus and list item dragging.

Filters

Filters appear on most list pages. You can use them to search pages for specific data.

Depending on which page you are viewing, you can filter pages using one of the following features. Only one feature appears per page.

• Filters
• Filter Row

Filters appear above page lists. They feature different fields, lists, and check boxes used for filtering. Filters vary according to page.

Figure 9: Filters

You can save frequently used filter settings as your default view. To save your settings, select **Options** > **Save as default view** from the toolbar. The toolbar **Options** menu contains the following options for filtering.

Table 4: Filter Options

Option	Function
Show results on page load	Automatically retrieves and displays results when selected.

Save as default view	Saves the active filter and sort criteria as the default view for the page.
	• The default view displays each time the page is accessed, including the following events:
	   • Browsing to a different page.
	   • Logging out of the Web console.
	• The default view is saved until you save a new one or you clear it.

Clear default view	Resets a saved default view to the system default view.

Filter Rows

Filter rows appear in the lists themselves. Rows feature a field for each column.

Figure 10: Filter Row

• Filters are not case sensitive.
• Columns can be filtered using a variety of data types. For example, you can use a **Contains** filter or a **StartsWith** filter.
• Date columns filter at the lowest level of granularity. Higher levels of granularity return no filter results.

Supported Wildcards

When searching for or filtering vulnerabilities, you can use wildcards to make search results more specific and efficient.

Wildcards can be used anywhere within the search string. The following table lists the supported operators and wildcards in HEAT PatchLink DataCenter for Microsoft System Center. Type any wildcards that you intend to use in the **Name of CVE-ID** field.

Table 5: Supported Wildcards

Wildcard	Description	Example
%	Any string. The string can be empty or contain any number of characters.	Typing `Microsoft%Server` in the **Name or CVE-ID** field returns any vulnerability with the words *Microsoft* and *Server* in any part of the name, such as: • MS12-043 Security Update for **Microsoft** Office SharePoint **Server** 2007 32-Bit Edition (KB2687497) • The 2007 **Microsoft** Office **Server**s Service Pack 3 (SP3), 32-bit Edition (KB2526299)
_ (underscore)	Wildcard placeholder for any single character.	Typing `_itrix` or `Citri_` in the **Name or CVE-ID** field returns any vulnerabilities with *Citrix* in the name.
[ ]	Any single character within a range ([a-f]) or set ([abcdef]).	Typing `[m]ic` in the **Name or CVE-ID** field returns vulnerabilities with the string *mic* within the name (*Microsoft* and *Dynamic*). Typing `200[78]` in the **Name or CVE-ID** field returns vulnerabilities with 2007 or 2008 within the name.
[^]	Any single character **not** within a range ([^a-f]) or set ([^abcdef]).	Typing `M[^i]cro` in the **Name or CVE-ID** field returns results that: • Replace *i* with all remaining alphanumeric and symbolic charcters (a, $, and so on). • Include all other characters remaining in the string (m, c, r, o). Results would include Macro, Mecro, M$cro, and so on.

Using Filters

When list pages are overpopulated with items, use filters to search for specific list items. Use this feature to filter list pages by criteria specific to the page.

Filters are available on most list pages.

1. Select a list page. For additional information, refer to List Pages on page 29.

2. Ensure filters are displayed.

   If filters are not displayed, click **Show Filters**.

3. Define filter criteria.

   > **Note:** Available filters differ by page.

   - In filter fields, type the desired criteria.
   - From filter lists, select the desired list item.

4. If applicable, select the **Include sub-groups** check box.

   > **Note:** This check box only appears on list pages related to groups.

5. Click **Update View**.

   Step Result: The list is filtered according to the filter criteria.

6. [Optional] Save the filter criteria by selecting **Options** > **Save as default view** from the toolbar.

Using Filter Rows

Some list pages use filter rows rather than filters. Use these rows, which are the first row of applicable lists, to filter column results. Filter column results to search for specific list items.

These rows appear on several list pages.

1. Select a page featuring the filter row.

2. Ensure the filter row is displayed.

   a) If the filter row is not displayed, select **Options** > **Show Filter Row** from the toolbar.

3. Type criteria in a filter row field.

4. Apply a filter type.

   a) Click the **Filter** icon.

      Step Result: A menu opens.

HEAT software

b) Select a filter type.

The following table describes each filter type.

Table 6: Data Filtering Types

Type	Description
NoFilter	Removes previously applied filtering.
Contains	Returns results that contain the value applied to the filter.
DoesNotContain	Returns results that do not contain the value applied to the filter.
StartsWith	Returns results that start with the value applied to the filter.
EndsWith	Returns results that end with the value applied to the filter
EqualTo	Returns results equal to the value applied to the filter.
NotEqualTo	Returns results that are not equal to the value applied to the filter.
Greater Than	Returns results that are greater than the value applied to the filter.
Less Than	Returns results that are less than the value applied to the filter.
GreaterThanOrEqualTo	Returns results that are greater than or equal to the value applied to the filter.
LessThanOrEqualTo	Returns results that are less than or equal to the value applied to the filter.
Between	Returns results that are between two values. Place a space between the two values.
NotBetween	Returns results that are not between two values. Place a space between the values.
IsEmpty	Returns results that are empty.
NotIsEmpty	Returns results that are not empty.
IsNull	Returns results that have no value.

Type	Description
NotIsNull	Returns results that have a value.

> **Note:**
> - Filters are not case sensitive.
> - Date columns filter at the lowest level of granularity. Higher levels of granularity return no filter results.
> - The availability of filtering options depends on the type of data displayed in the column. For example, filtering options that can only apply to numeric data are available in columns that contain text data.

Result: The list column is filtered according to the criteria. If desired, repeat the process to filter additional columns.

Group By

The **Group By** row lets you sort list items into groups based on column headers. Use this feature to see which list items share similarities.

To use the **Group By** row, ensure **Options** > **Show Group By Row** is selected from the toolbar, and then drag a column header into the row. You may drag multiple columns to the row, but you may only drag one column into the row at a time.

To ungroup the list, right-click on the row and select **Cancel All Groupings**. To hide the **Group By** row, select **Options** > **Hide Group By Row**.

Figure 11: Group By Row

Expanding and Collapsing Structures

Certain structures in the Web console are expandable and collapsible. Expand structures to view additional information or options. Collapse them to conserve screen space.

Click available **Plus** icons (+), **Minus** icons (-), and **Rotating Chevron** icons (>) to expand or collapse a structure.
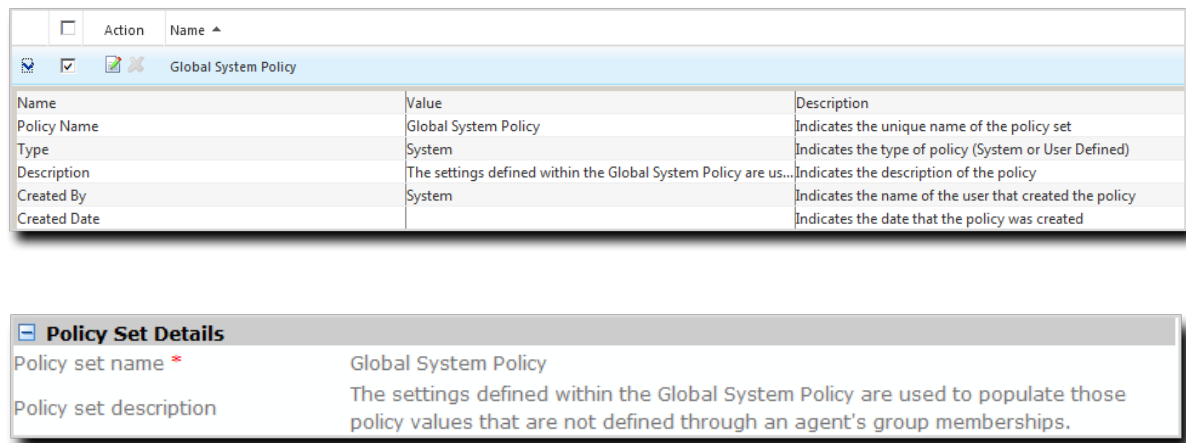
Figure 12: Expandable Structure Examples

Advancing Through Pages

When a list page contains an overflow of items, pagination links are created to manage the overflow. Click these links to advance through list items.

The number of list items and the page you are viewing determines the number of pagination links.

Figure 13: Pagination Feature

Table 7: Pagination Feature Functions

Icon or Link	Title	Function
▶	**Final Page Link**	Advances to the final page of list items.
◀	**First Page Link**	Returns to the first page of list items.
...	**Next Ten/Previous Ten Pages Link**	Displays the next ten or previous ten page links available. Fewer page links will display if the remaining list items cannot populate ten pages.

Icon or Link	Title	Function
1 2 3 4 5	**Pagination Links**	Advances or returns to the selected pagination link.

Each page also features a **Rows Per Page Drop-Down List**. This list modifies the number of list items displayed on a single page (25, 50, 100, 200, 500).

Help

HEAT PatchLink DataCenter for Microsoft System Center contains context-sensitive HTML help that includes feature explanations, step-by-step procedures, and reference materials.

Accessing Help differs according to context.

- From a page, press F1.
- From a dialog, click the **Question Mark** icon (**?**).

Use the following features to navigate through Help:

- From the *Content* tab, expand the bookmarks and click links to display Help topics.
- From the *Search* tab, type criteria in the **Keywords** field and click **Search** to display Help topics related to your search.

Exporting Data

On many system pages, you can export the listed data to a comma-separated value file (`.csv`) available for use outside of the Web console. Use this exported data for management purposes (reporting, noting trends, and so on).

You can export data from a variety of pages.

Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

1. Open a system page or dialog that you can export information from.
2. [Optional] Use the page filters to refine the items listed.
3. Click **Export**.

   Step Result: The *File Download* dialog opens.

4. Use the browser controls to complete the data export.

Result: The data is exported. All data results export, including data on overflow pages.

HEAT®software

The Dashboard

The entry point to HEAT PatchLink DataCenter for Microsoft System Center is the **Dashboard**. From this view, you can see drag-gable widgets that display information about HEAT PatchLink DataCenter for Microsoft System Center and agent-managed endpoints.
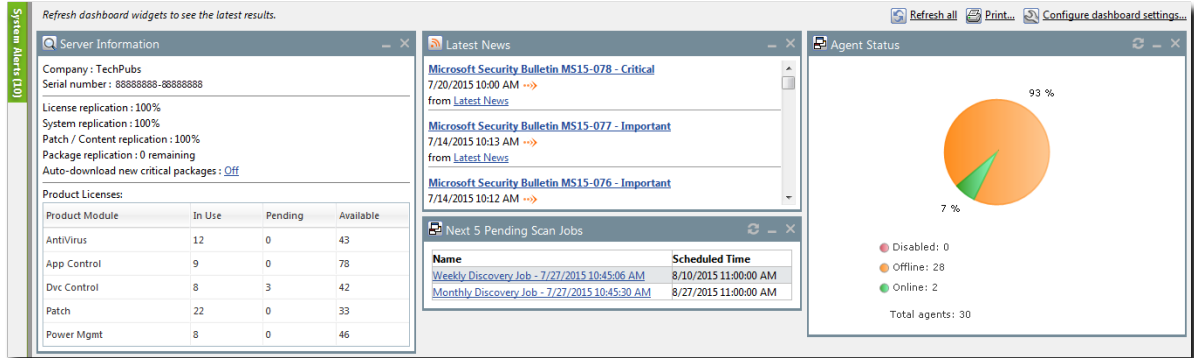
Figure 14: The Dashboard

The Dashboard

The **dashboard** displays widgets depicting the activity on your protected network. Located under the **Assets and Compliance** workspace, this view provides convenient information you can use to ensure your network protection is up to standard. Additionally, you can customize the dashboard to display the widgets most applicable to your network environment.

Widget graphs are generated based on the latest data and statistics available from endpoints, groups, module-specific data, and so on.

The following **Dashboard** widgets are available:

- The Agent Module Installation Status Widget on page 39
- The Agent Status Widget on page 39
- The Applicable Content Updates Widget on page 39
- The Critical Patch Status by Endpoint Widget on page 40
- The Endpoints with Unresolved Updates Widget on page 42
- The Incomplete Deployments Widget on page 43
- The Latest News Widget on page 43
- The Mandatory Baseline Compliance Widget on page 44
- The Offline Patch Endpoints Widget on page 44
- The Patch Agent Module Status Widget on page 45
- The Scheduled Deployments Widget on page 46
- The Server Information Widget on page 46
- The Un-remediated Critical Vulnerabilities Widget on page 47

The Agent Module Installation Status Widget
This widget displays the installation and licensing stats of each agent module.

A graph bar displays for each installed module. The following table describes the widget graph.

Table 8: Graph Bar Color Descriptions

Bar Color	Description
Blue	The number of endpoints with the module pending install or uninstall.
Green	The number of endpoints with the module installed.
Red	The number of endpoints without the module installed.

Tip: Click the graph to open the *Endpoints* page.

Note: Endpoints with an agent version that does not support a module are not counted.

The Agent Status Widget
This widget displays all agents grouped by agent status.

Table 9: Agent Status Widget Fields

Field	Description
Online	The number of agents that are online.
Offline	The number of agents that are offline.
	Tip: Offline status is determined by the amount of time since the agent last communicated as determined on the *Options* page.
Disabled	The number of agents that are disabled.
Total Agents	The total number of agents in your environment.
Tip: Click the graph to open the *Endpoints* page. The page is filtered to display all agents.	

The Applicable Content Updates Widget
This widget displays applicable content updates grouped by content type. View this widget when determining what content is applicable to endpoints in your network.

Table 10: Applicable Content Updates Widget Graph Bars

Bar	Description
Critical	The number of critical content items that are applicable to the your endpoints.

HEAT software

Bar	Description
Recommended	The number of recommended content items that are applicable to your endpoints.
Optional	The number of optional software, informational, and virus removal content items that are applicable to your endpoints.

Tip: Click the widget graph to open the **Content** page, which is filtered to display all applicable non-patched content.

Table 11: Applicable Content Updates Widget Fields

Field	Description
Applicable updates	The total number of content items applicable to your endpoints.
Endpoints	The total number of endpoints with applicable updates.

Note:

- Updates that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Applicable updates** count.
- Updates that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Applicable updates** count.
- If an endpoint is marked as *Do Not Patch* for an applicable update, that update is no longer considered applicable. Therefore, that endpoint is only included in the **Endpoints** count if it has other unresolved updates.

The Critical Patch Status by Endpoint Widget
This widget depicts the patch status of all managed endpoints. Each bar indicates the number of managed endpoints with applicable vulnerabilities within a given release date range.

The following table describes the **Critical Patch Status By Endpoint** widget. Green bars indicate endpoints that are patched for critical vulnerabilities, while red bars indicate endpoints that are not patched for critical vulnerabilities.

Table 12: Critical Patch Status By Endpoint Bars

Graph Bar	Description
<30 days	The number of endpoints with applicable critical vulnerabilities fewer than 30 days old.
30 - 120 days	The number of endpoints with applicable critical vulnerabilities between 30 to 120 days old.

Graph Bar	Description
>120 days	The number of endpoints with applicable critical vulnerabilities greater than 120 days old.

The following table describes the widget fields.

Table 13: Critical Patch Status By Endpoint Fields

Field	Description
Endpoints	The total number of endpoints with applicable critical vulnerabilities.
Critical vulnerabilities	The total number of critical vulnerabilities applicable to your environment.

Tip: Click the graph to view patches that remediate critical vulnerabilities.

Note:

- If an endpoint is marked as *Do Not Patch* for a critical vulnerability, that vulnerability is no longer considered applicable. Therefore, that endpoint is only included in the graph bars and the **Endpoints** count if it has other unresolved critical vulnerabilities.
- Vulnerabilities that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the **Critical vulnerabilities** count.
- Vulnerabilities that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the **Critical vulnerabilities** count.

The Discovery Scan Results: Agents Widget
This widget displays the number of endpoints capable of hosting agents discovered in the latest Discovery Scan Job. The endpoints are classified in to two groups: endpoints with agents and endpoints without agents.

Table 14: Discovery Scan Results: Agents Widget Fields

Field	Description
As of	The name of the Discovery Scan Job used to generate the widget graph and statistics. This job is the job most recently run.
Endpoints with agents	The number of agent-compatible endpoints discovered that have agents installed.
Endpoints without agents	The number of agent-compatible endpoints discovered that have no agents installed.

HEAT®software

Field	Description
Endpoints	The total number of agent-compatible endpoints discovered.

Tip: Click the widget to open the *Results* page for the most recently run Discovery Scan Job.

The Endpoints with Unresolved Updates Widget
This widget displays all endpoints with unapplied applicable content updates, grouped by content type. View this widget when determining if an endpoint requires deployment.

An unresolved update is an occurrence of an endpoint that has not had an applicable content item installed.

Bar	Description
Critical	The number of endpoints that have unresolved critical content updates.
Recommended	The number of endpoints that have unresolved recommended content updates.
Optional	The number of endpoints that have unresolved software, informational, and virus removal content updates.

Tip: Click a widget graph bar to view uninstalled patches that apply to your endpoints.

Field	Description
Endpoints	The number of endpoints with applicable updates within your network.
Applicable updates	The total number of content items applicable to your endpoints.

Note:

- If an endpoint is marked as *Do Not Patch* for an applicable update, that update is no longer considered applicable. Therefore, that endpoint is only included in the graph bars and the **Endpoints** count if it has other unresolved updates.
- Updates that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Applicable updates** count.
- Updates that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Applicable updates** count.

The Incomplete Deployments Widget

This widget displays all deployments with elapsed start dates and a status of *not started* or *in progress*.

Table 15: Incomplete Deployment Widget Fields

Field	Description
<25%	The number of deployments that are less than 25 percent complete. This field includes deployments that have not started.
25% - 49%	The number of deployments that are 25 to 49 percent complete.
50% - 69%	The number of deployments that are 50 to 69 percent complete.
70% - 79%	The number of deployments that are 70 to 79 percent complete.
80% - 89%	The number of deployments that are 80 to 89 percent complete.
>90%	The number of deployments that are more than 90 percent complete.
Total	The total number of deployments that have a status of *in progress* or *not started* with an elapsed start time.
Total affected endpoints	The total number of endpoints receiving pending or in-progress deployments.

The Last 5 Completed Scan Jobs Widget

This widget contains information about the last five completed discovery scan jobs. Each job name is a link to the associated **Result** page.

Table 16: Last 5 Completed Scan Jobs Widget Columns

Column	Description
Name	The job name. Click the name to open the **Results** page for the job.
Completed Date	The date and time the job completed on the server.
Status	The status of the completed job.

The Latest News Widget

This widget displays important announcements and other information in HEAT PatchLink DataCenter for Microsoft System Center.

Click a link to view additional details about an announcement.

HEAT software

The Mandatory Baseline Compliance Widget
This widget displays the Mandatory Baseline status for all endpoints that have the HEAT PatchLink DataCenter module installed.

Table 17: Mandatory Baseline Compliance Widget Fields

Field	Description
Compliant	The number of endpoints with all Mandatory Baseline content installed.
	Note: Endpoints that don't have Mandatory Baseline content installed that's marked *Do Not Patch* are considered compliant.
In process	The number of endpoints currently downloading Mandatory Baseline content.
No baseline	The number of endpoints with no content assigned to their Mandatory Baselines.
Non compliant	The number of endpoints that do not have all content in their Mandatory Baselines installed.
Total number of endpoints	The number of endpoints with an agent installed.

The Next 5 Pending Scan Jobs Widget
This widget displays information about the next five pending discovery scan jobs.

Table 18: Next 5 Pending Scan Jobs Widget Columns

Column	Description
Name	The job name. Click the link to view the **Discovery Scan Jobs** page **Scheduled** tab.
Scheduled Time	The date and time the job is scheduled for on the server.

Tip: Click a job name link to view the **Discovery Scan Jobs** page **Scheduled** tab.

The Offline Patch Endpoints Widget
This widget displays all offline HEAT PatchLink DataCenter endpoints. These endpoints are grouped by time ranges since they last checked in.

Table 19: Offline Agents Widget Fields

Field	Description
< 48 hours	The number of HEAT PatchLink DataCenter endpoints offline fewer than 48 hours.

Field	Description
48 - 72 hours	The number of HEAT PatchLink DataCenter endpoints offline 48 to 72 hours.
> 72	The number of HEAT PatchLink DataCenter endpoints offline greater than 72 hours.
Total number of offline agents	The number of HEAT PatchLink DataCenter endpoints that are offline (since their last scheduled Discover Applicable Updates task).

Tip: Clicking the **Offline Patch Endpoints** widget pie chart opens the *Endpoints* page *HEAT PatchLink DataCenter* tab, which is filtered to display offline patch endpoints.

The Patch Agent Module Status Widget
This widget displays all endpoints with the HEAT PatchLink DataCenter module installed, which are grouped by HEAT PatchLink DataCenter status.

Table 20: Patch Agent Module Status Widget Fields

Field	Description
Working	The number of HEAT PatchLink DataCenter endpoints that are working on a deployment task.
Idle	The number of HEAT PatchLink DataCenter endpoints that are idle.
Disabled	The number of HEAT PatchLink DataCenter endpoints that are disabled.
Sleeping	The number of HEAT PatchLink DataCenter endpoints that are sleeping.
Offline	The number of HEAT PatchLink DataCenter endpoints that are offline.
Disabled	The number of HEAT PatchLink DataCenter endpoints that are disabled.
Agents with PR module installed.	The number of endpoints with the HEAT PatchLink DataCenter module installed.
Total Agents	The total number of HEAT PatchLink DataCenter endpoints in your network.

Tip: Click the graph to open the *Endpoints* page.

HEAT®software

The Scheduled Deployments Widget
This widget displays endpoints that have not yet installed applicable content. These endpoints are divided in to two categories: endpoints with deployments scheduled and endpoints with deployments not scheduled. These categories are further divided into three categories: endpoints with not yet applied critical content, endpoints with not yet applied recommended content, and endpoints with not yet applied optional content.

Orange graph bars indicate endpoints that are not scheduled to receive applicable content, while blue graph bars indicate endpoints that are scheduled to receive applicable content.

Table 21: Scheduled Deployments Widget Graph Bars

Graph Bar	Description
Critical	The number of endpoints scheduled or not scheduled to receive deployments for critical content.
Recommended	The number of endpoints scheduled or not scheduled to receive deployments for recommended content.
Optional	The number of endpoints scheduled or not scheduled to receive deployments for optional content.

Tip: Clicking the **Scheduled Deployments** widget opens the ***Deployments and Tasks*** page, which is filtered to display scheduled deployments.

Table 22: Scheduled Deployments Widget Field

Field	Description
Endpoint with unresolved updates	The number of endpoints with unresolved updates.

The Server Information Widget
This widget lists your serial number, number of licenses available, number of licenses in use, and information about current license usage and availability.

Table 23: Server Information Widget Fields

Field Name	Description
Company	The company your server is registered to as defined during installation.
Serial Number	The license number (serial number) assigned to your server.
License Replication	The subscription status between your server and the Global Subscription Service (GSS).
System Replication	The system replication status between your server and the GSS.

Field Name	Description
Patch / Content Replication	The replication status between your server and the GSS.
Package Replication	The number of packages remaining for replication.
Auto-download New Critical Packages	The indication of whether your automatically downloads packages for critical vulnerabilities. Click the link to open the **Subscription Service Configuration** dialog. For additional information refer to Configuring the Service Tab on page 102.

Table 24: Product Licenses Table Columns

Column	Description
Product Module	The module for which you purchased licenses.
In Use	The number of module licenses in use.
Pending	The number of licenses pending use or pending removal. Licenses pending removal become available upon removal completion.
Available	The number of licenses available.

Note: A license expiration notice displays if all available licenses are expired.

The Un-remediated Critical Vulnerabilities Widget
This widget displays the total number of unremediated critical vulnerabilities that are applicable to your environment grouped by age.

Table 25: Un-remediated Critical Vulnerabilities Widget Graph

Graph Bar	Description
<30 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network fewer than 30 days old.
30 - 120 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network that are 30 to 120 days old.

HEAT software

Graph Bar	Description
>120 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network greater than 120 days old.

Tip: Click the graph to open the **Vulnerabilities** page, which is filtered to display critical but not superseded applicable vulnerabilities.

Table 26: Un-remediated Critical Vulnerabilities Widget Fields

Field	Description
Critical Vulnerabilities	The number of critical but not superseded vulnerabilities applicable in your network.
Endpoints	The number of endpoints with critical but not superseded applicable vulnerabilities.

Note:

- Vulnerabilities that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Critical vulnerabilities** count.
- Vulnerabilities that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Critical vulnerabilities** count.
- If an endpoint is marked as *Do Not Patch* for an applicable vulnerability, that vulnerability is no longer considered applicable. Therefore, that endpoint is only included in the **Endpoints** count if it has other unresolved updates.

Dashboard Setting and Behavior Icons

Setting and behavior icons are UI controls used to manage the dashboard. Click these icons to maximize, minimize, hide, and refresh the dashboard and widgets.

The following table describes each icon action.

Table 27: Widget Setting and Behavior Icons

Icon	Action
	Opens the **Dashboard Settings** dialog.
	Opens the dashboard in print preview mode.
	Collapses the associated widget.
	Expands the associated collapsed widget.
	Hides the associated widget.

Icon	Action
🔄	Refreshes the associated widget (or the entire dashboard).

Note: Not all widgets contain **Refresh** icons.

Previewing and Printing the Dashboard

When viewing the dashboard, you can reformat it for printing. This reformat omits the Web site header and footer, reorganizing the dashboard to display only the selected widgets, making it ideal for printing.

1. From the **Assets and Compliance** workspace, select **Dashboard**.

2. Click 🖨.

   Step Result: The dashboard print preview opens in a new Web browser window.

3. [Optional] Use your Web browser controls to print the dashboard.

Editing the Dashboard

You can customize how widgets are arranged and prioritized. Edit the dashboard to display only the widgets useful in your environment.

Edit the dashboard from the ***Dashboard Settings*** dialog.

1. From the **Assets and Compliance** workspace, select **Dashboard**.

2. Click 🔍.

   Step Result: The ***Dashboard Settings*** dialog opens.

3. Choose which widgets you want to display on the dashboard.

   • Select widget check boxes to display them.
   • Clear widget check boxes to hide them.

4. Prioritize the widgets in the desired order.

   • Click ⬆ to increase a widget priority.
   • Click ⬇ to decrease a widget priority.

   Highly prioritized widgets are more prominently placed.

5. Display or hide widget descriptions.

   • Click 🖼 to display descriptions.
   • Click 🖼 to hide descriptions.

HEAT software

6. Choose a widget layout.

- Click ▦ to display widgets in two columns.
- Click ▦ to display widgets in three columns.

7. Click **OK**.

Result: Your dashboard settings are saved. The dashboard displays the selected widgets in the priority you defined.

License Expiration

When licensing for a module expires, the module behavior changes. All functionality is restored when the licensing is renewed.

Note: When a subscription expires, the module history and configuration is retained. No work is lost when the module is renewed.

Table 28: License Expiration Scenario and Events

Scenario	Event(s)
Server Module Expiration	- Endpoint module functionality is partially disabled. - The module cannot be installed on additional endpoints. - The **Endpoints** page lists the module status as Expired. - The **Server Information** widget lists the **Available** license count as Expired.
Endpoint Module Expiration	- Endpoint module functionality is partially disabled. - The module cannot be installed on additional endpoints. - The **Endpoints** page lists the module status as Expired. - The **Server Information** widget lists the **Available** license count as Expired. - The HEAT PatchLink DataCenter endpoint module component continues to inventory its host, but no longer enforces HEAT PatchLink DataCenter policies or downloads deployments.

Tip:

- You can view subscription service history from
- You can also view license information from

To reactivate your licenses following renewal, open the ***Subscription Updates*** page and click **Update Now**. Your server replicates updated subscription information. The page refreshes when the update completes, and all previous module functionality is restored.

Note: For more information about renewing or adding licenses, contact HEAT Sales Support (sales@lumension.com) .

HEAT software

Chapter

4

Configuring Options

In this chapter:

- The Options Page
- Working with Options
- Defining Access Rights

You can customize your system to use options and settings that you select.

HEAT PatchLink DataCenter for Microsoft® System Center contains general options and agent options. More options are added when you install new modules.

The Options Page

You can control a number of default settings from the **Options** page: user interface options, agent options, and so on. Use these options to customize default settings and values.

Figure 15: Options Page

HEAT®software

The **Options** page contains the following tabs, which contain options related to their labels:

- The General Tab on page 55
- The Agents Tab on page 58

Figure 16: Options Page

- HEAT PatchLink DataCenter adds the new **Deployments** tab. It features options for configuring the default values in the **Deployment Wizard**. For additional information, refer to The Deployments Tab on page 62.
- Several new options are also added to the **Agents** tab. For additional information, refer to The Agents Tab on page 58.

Viewing the Options Page

Navigate to the **Options** page to edit default system settings.

You can reach this page from the **Navigation Menu**.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Options**.
2. Select a tab.
3. [Optional] Complete a task listed in Working with Options on page 64.

The Options Page Buttons

The **Options** page contains several buttons that are common to each of its tabs. These buttons share similar functions to buttons commonly seen on page toolbars.

The following table describes the **Option** page button functions.

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Reset	Cancels any edits made to the options since the tab was loaded.
Save	Saves the tab option settings (if any edits were made). You must click this button to implement your edits.

The General Tab

Default settings for user interface options, password options, and report and display options are controlled from the **General** tab. The options available on this page are generalized and are not closely related.

UI Options

With these options, you can control user interface features according to your preferences.

Select from lists and check boxes to configure **UI options**.

Table 29: UI Options

Option	Description
Default number of rows per page	Defines the default number of rows that display in list pages (**25**, **50**, **100**, **200**, **500**).
Cache timeout	Defines the maximum number of minutes data is held in the memory before it needs to be reloaded from the database (**5**, **10**, **15**, **20**, **30**).
Session timeout	Defines the number of minutes before a repeat login is required due to inactivity (**20**, **40**, **60**, **80**, **100**, **120**).
Activate automatic IP grouping in the Groups view	Creates groups organized by IP address in the **Groups** page **Browser** named **IP Collection**.

/HEAT software

Password Options
This option defines the number of days before an upcoming password expiration that a warning appears that notifies you of the upcoming expiration.

Complete the field to configure the options.

The following table describes the available **Password option**.

Table 30: Password Options

Option	Description
Display notification *x* days prior to password expiration.	Defines the number of days prior to a required password change (as controlled by Windows) that a notification displays. A value of 0 disables the notification.

Note: User that do not have password expirations are unaffected by this option.

Discovery and Agent Management Job Logging
During Discovery Scan or Agent Management Jobs, a log of events is saved on your server. The **Discovery and Agent Management Job Logging** options lets you configure the information that is logged during job activity.

Table 31: Discovery and Agent Management Job Logging Options

Option	Description
Logging Level	Defines the information recorded in the job during Discovery Scan Jobs and Agent Management Jobs. Options include: • **Trace** • **Diagnostic** • **Information** • **Warning** • **Error** • **Critical**

Option	Description
Include common troubleshooting information for	Defines whether the log include common troubleshooting information for a given part of a job. Options include: • **Agent Management** • **Discover** • **SOAP**

Note: By default, Discovery Scan and Agent Management Job logs are saved to `<Installation Directory>\Lumension\EMSS\Web\Services\ScanEngine\Engine\engine.log` on the server.

Report and Display Options

These options control date, time, and paper formatting for reports. Modify date and time settings according to your locale. Modify paper settings according the paper types your enterprises uses for printing.

Note: These options apply only to reports in a PDF format.

Table 32: Report and Display Options

Option	Description
Date format	Defines the date format displayed in text-based and graphical reports. Select from the following options: • **Default** (mm/dd/yyyy) • **MM/dd/yyyy** • **dd/MM/yyyy** • **yyyy-MM-dd** • **dd.MM.yyyy** • **dd-MM-yyyy** • **yyyy/MM/dd**
Time separator	Defines the character used to separate hours, minutes, and seconds in reports. Select from the following options: • **Default** (the current character in use) • **Colon** (:) • **Period** (.) This option also defines the time format used in reports. Select from the following options: • **12 Hour** • **24 Hour**

HEAT®software

Option	Description
Time format	Displays the selected **Date Format** punctuated by the selected **Time Separator**. This field refreshes as you select different **Report and display options**.
Paper size for reports	Defines how reports are formatted for printing. Select from the following options: • **Default** (the currently saved formatting style) • **Letter** • **A4**

The Agents Tab

This tab contains default options related to the agent.

Agent Installation

These options define default installation values for Agent Management Jobs. Adjusting these settings can help save on effort using an Agent Management Job.

Use **Agent Installation** options to define the default settings for the *Agent Settings* page in the *Schedule Agent Management Job Wizard*. Complete the field and select from the lists to define the options.

Note: When configuring an Agent Management Job, the following options can be changed.

Table 33: Agent Installation Options

Agent Installation Option	Description
Timeout (drop-down list)	Defines the default number of minutes before an agent installation job terminates due to non-responsive status (0-30).
Number of retries (drop-down list)	Defines the default number of attempts an agent installation will retry if initial and subsequent installations fails (1-10).
Number of simultaneous installs (drop-down list)	Defines the default maximum number of agents that can be installed or un-installed simultaneously during an Agent Management Job (1-25). A setting of 1 indicates that serial install/uninstalls should occur.

Agent Installation Option	Description		
Server identity (field)	Defines the default text entered in the **Server Identity** field during agent installation jobs. **Server Identity** is the name agents list as their HEAT PatchLink DataCenter for Microsoft System Center server.		
Scan method for pre-selected targets (radio buttons)	Defines how endpoints pre-selected from a page list are added to a job's **targets** list (discovery scan or agent management) after launching a job configuration dialog. The options are:		
	IP Address	Adds the selected endpoint to a job's target list using its IP address.	
	Computer Name	Adds the selected endpoint to a job's target list using its endpoint name.	

Communication

This section contains default options for agent communications with the server.

HEAT PatchLink DataCenter adds a new option.

Table 34: Communication Options

Option	Description
Agents should be shown offline when inactive for	Defines the time period (in minutes, hours, or days) before an agent is considered offline because it has not checked. A value of *0* disables this option.
	Tip: Disabled and uninstalled agents are not considered offline.

HEAT®software

Option	Description		
Stand alone Patch agent uniqueness based on	Defines how the server identifies Patch Agents during communication.		
	Endpoint name		Configures the server to identify Patch Agents using the NetBIOS name of the endpoint. Select this option in smaller networks where endpoints are unlike to share a NetBIOS name, as it reduces administrative maintenance in the event that an endpoint needs to be re-imaged. This option is selected by default.
	Instance		Configures the server to identify Patch Agents using a unique number. Select this option in larger network environments where multiple instances of a single NetBIOS name may exist. This option prevents communication errors related to multiple agents sharing a name.

Discover Applicable Updates Options

You can select the default events that schedule a **Discover Applicable Updates** task for HEAT PatchLink DataCenter HEAT PatchLink DataCenter endpoints.

Table 35: Discover Applicable Updates Options

Option	Description
DAU should be run after subscription replication	Determines a DAU task is scheduled for all endpoints following a subscription replication.
DAU should be run after inventory change	Determines a DAU task is scheduled for an endpoint after if detects an inventory change.

Absentee Agent Deletion

Sporadically, an endpoints will cease communication with the server. Configure the **Absentee Agent Deletion** option to determine the amount of time before the agent is removed from your server database.

Table 36: Absentee Agent Deletion Option

Option	Description
Delete absentee agent after *x* days.	Removes an uncommunicative agent after the defined time period (days). A value of *0* disables this function.

Note: Absentee agents records are only deleted from the database, leaving no history of them in the Web console. However, the agent software is not deleted from its host endpoint.

ISAPI Communication

Using these options, you can limit connections between the server and HEAT PatchLink DataCenter endpoints. Limiting server and endpoint communications ensures the server can handle all incoming agent communications. These options are added after HEAT PatchLink DataCenter is installed.

HEAT PatchLink DataCenter for Microsoft System Center supports the Internet server application programming interface (ISAPI) communication settings for Internet Information Services (IIS).

Table 37: ISAPI Communication Options

Option	Description	
Concurrent agent limit	Defines the maximum number of threads used by the server. Select from the following options:	
	SQL default (64 threads)	Enables the default thread count for a SQL Server implementation.
	Custom setting (5 to 256 threads)	Enables a custom thread count.
Connection timeout	Defines the number of seconds before an ISAPI thread times out. Select from the following options:	
	Default (30 seconds)	Sets the connection timeout to the default value.
	Custom setting (5 to 300 seconds)	Sets the connection timeout to a custom value.

◢HEAT®software

Option	Description		
Command timeout	Defines the number of seconds before an ISAPI command times out. Select from the following options:		
	Default (60 seconds)	Sets the command timeout to the default value.	
	Custom setting (5 to 900 seconds)	Sets the command timeout to a custom value.	

Agent Versions

There are multiple versions of the agent. By defining **Agent Version** options, you can limit which versions are available for installation.

Table 38: Agent Version Options

Option	Description
Linux, Unix, & Mac agent version	Defines which agent versions are available for installation on endpoints running Unix-based operating systems when working with the following system dialogs: • The *Manage Agent Versions* Dialog • The *Download Agent Installers* Dialog

Note:

When selecting agent version options, remember the following information:

- **Newest Available** means only the latest agent version is available for installation.
- *Agent Version* **only** list items mean only that agent version is available for installation.
- *Agent Version* **+** list items mean that agent version and all versions that supersede it are available for installation.

The Deployments Tab

This tab, added after installing HEAT PatchLink DataCenter, lets you configure default values related to deployments.

This tab includes options for:

- **Deployment defaults**, which you can use to configure the number of deployment-related tasks that can run at one time.
- **Notifications defaults**, which you can use to set the default text that displays when users are notified of their deployments.
- **User interface**, which controls whether the deployments you schedule are listed in the Web console using agent local time or UTC time.

Deployment Defaults

These options let you define how many endpoints can perform actions simultaneously. Defining higher values lets you perform more deployment-related actions simultaneously. However, multiple agents performing actions simultaneously may strain network resources.

Table 39: Deployment Default Options

Option	Description
Maximum number of deployments that can run simultaneously	The number of endpoints that can simultaneously run deployments.
Maximum number of simultaneous Discover Applicable Updates (DAU) tasks	The number of endpoints that can simultaneously run the DAU task.
Maximum number of reboot tasks that can run simultaneously	The number of endpoints that can simultaneously receive a deployment requiring a reboot.
Maximum number of simultaneous mandatory baseline deployments	The number of endpoints that can simultaneously receive Mandatory Baseline deployments.
Maximum number of times a deployment will be consecutively attempted	The number of failed deployment attempts permitted before the server disables it. This option does not apply to Mandatory Baseline deployments. This option also disables the deployment for endpoints that have not started it.

Notification Defaults

When using the *Deployment Wizard*, you can configure a deployment to notify recipients. By using **Notification defaults**, you can create default notification for the *Deployment Wizard*.

These notifications, which are pop-up dialogs, alert endpoint users that a deployment is about to occur. Default notification settings can be overridden when completing the *Deployment Wizard*.

Table 40: Notification Defaults Options

Option	Description
User notification windows should always be on top	Defines the default selection for the **Deployment Notification Options** and **Reboot Notification Options** when completing the *Deployment Wizard*.
Manual Installation	Defines the default message that displays when the deployment recipient receives a package requiring manual installation.
May Reboot	Defines the default message that displays when the deployment recipient receives a package that may require the recipient to reboot.
Default deployment message	Defines the default message that displays with a deployment notification.

HEAT software

Option	Description
Default reboot message	Defines the default message that displays with a deployment reboot notification .

Note: All notifications may contain a maximum of 1000 characters.

User Interface

When using the **Deployment Wizard**, you can configure deployment times in the Web console to display as endpoint local time or endpoint Coordinated Universal Time (UTC). This option also affects what start time option is selected by default when completing the **Deployment Wizard**.

Table 41: User Interface Option Descriptions

Option	Description
Agent Local Time (Deploy at local time for each individual node)	Defines **Agent Local Time** as the deployment start time in the Web console and the **Deployment Wizard**.
Agent UTC Time (Deploy at UTC time for each individual node)	Defines **Agent UTC Time** as the deployment start time in the Web console and the **Deployment Wizard**.

Working with Options

From each **Options** page tab, you can define default behavior for different HEAT PatchLink DataCenter for Microsoft System Center features.

- Configuring the General Tab on page 64
- Configuring the Agents Tab on page 65
- Configuring the Deployments Tab on page 67
- Exporting Option Data on page 68

Configuring the General Tab

Configure this tab to define how user interface, password, and report display options behave.

Configure the **General** tab from the **Options** page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Options**.
2. Ensure the **General** tab is selected.

3. Define the **UI options**.

These options define general user interface behavior.

a) Select a value from the **Default number of rows page** list (**25**, **50**, **100**, **200**, **500**).

This option defines the default number of rows that display in list pages.

b) Select a value from the **Cache timeout** list (**5**, **10**, **15**, **20**, **30**).

This option defines the maximum number of minutes data is held in the memory before it needs to be reloaded from the database.

c) Select a value from the **Session timout** list (**20**, **40**, **60**, **80**, **100**).

This option defines the number of minutes before a repeat login is required due to inactivity.

d) Select or clear the **Activate automatic IP grouping in the Groups view** check box.

This option creates groups organized by IP address in the **Groups** page **Browser** named **IP Collection**.

4. Define the **Password options**.

This option defines the number of days prior to a required password change (as controlled by Windows) that a notification displays. Type a value in the **Display notification *x* days prior to password expiration** field. A value of 0 disables password expiration.

5. Define the **Report and display options**.

These options control formatting options for PDF reports. Perform the step(s) required to define each option.

> **Tip:** The **Default** item available in each **Report and display options** returns the applicable option to the last saved value.

a) Select a value from the **Date format** list.

This option defines the date format displayed in text-based and graphical reports.

b) Select a value from the two **Time separator** options.

This option defines the character used to separate hours, minutes, and seconds in reports. This option also defines the time notation used in reports.

> **Tip:** The **Time format** field previews your **Time separator** selections.

c) Select a value from the **Paper size for reports** list.

This option defines how reports are formatted for printing.

6. Click **Save**.

Result: The *General* tab configuration is saved.

Configuring the Agents Tab

Configure this tab to define default agent behavior. Settings include agent installation settings, communication settings, and agent version settings.

Configure the *Agents* tab from the *Options* page. After installing HEAT PatchLink DataCenter, configure the new communication, DAU, ISAPI, and agent version options that are added.

◢HEAT software

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Options**.

2. Select the *Agents* tab.

3. Define the **Communication** options.

   To define these options, complete the following substeps.

   a) Type a value in the **Agents should be shown offline when inactive for** field (**0**-**9999**).

      This option defines the time period (in minutes, hours, or days) before an endpoint status changed to offline because it has not checked in with your sever. Disabled and un-installed agents are not considered offline. A value of *0* disables this option.

   b) Select a value from the **Agents should be shown offline when inactive for** list.

      Select from the following values:

      - **Minute(s)**
      - **Hour(s)**
      - **Day(s)**

   c) Select a **Stand alone Patch agent uniqueness based on** option.

      These options define how the server identifies patch agents during communication. Select from the following options:

      - **Endpoint name**
      - **Instance**

4. Define the **Discover Applicable Updates (DAU) Options**.

   These options determine whether endpoints perform a DAU task following system actions. Select or clear the following options:

   - **DAU should be run after subscription replication**
   - **DAU should be run after inventory change**

5. Define the **Absentee agent deletion** option.

   This option defines when an uncommunicative endpoints are removed the Web console and system database. Type a value in the **Delete absentee agent after *x* Days** field (**0**-**999**) Days. A value of 0 disables the option.

6. Define the **ISAPI communication** options.

   a) Select a **Concurrent agent limit** option. If you select **Custom setting**, type the number of threads you want to simultaneously allow to your database (5-256).

   b) Select a **Connection timeout** option. If you select **Custom setting**, type the number of seconds that you want to consider an ISAPI thread considered timed out (5-300).

   c) Select a **Command timeout** option. If you select **Custom setting**, type the number of seconds that you want an ISAPI command considered timed out (5-900).

7. Define the **Agent Versions** options.

   These options define the agent versions that are available for installation when working with the following system dialogs:

   - The *Download Agent Installers* Dialog

   a) Select a value from the **Linux, Unix, & agent version** .

   Because the agent is updated regularly, **Agent Versions** option list values change frequently. Additionally, when selecting agent version options, remember the following information:

   - **Newest Available** means only the latest agent version is available for installation.

     > **Note:** This option only defines which agent version is available when working with the *Manage Agent Versions* dialog, the *Download Agent Installers* dialog, or the *Install Agents Wizard*. It does not automatically install newly released agent versions on network endpoints.

   - *Agent Version* **only** list items mean only that agent version is available for installation.
   - *Agent Version* **+** list items mean that agent version and all version that supersede it are available for installation.

8. Click **Save**.

Result: The *Agents* tab configuration is saved.

Configuring the Deployments Tab

Configuring this tab defines default setting for the *Deployment Wizard*. Selecting frequently used values from this tab leads to faster completion of the *Deployment Wizard* when deploying content.

Configure the *Deployments* tab from the *Options* page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Options**.

2. Select the *Deployments* tab.

3. Define the **Deployments defaults** options.

   Complete the following substeps.

   a) Type a value in the **Maximum number of deployments that can run simultaneously** field.

      This option defines the number of endpoint that can simultaneously download deployments.

   b) Type a value in the **Maximum number of simultaneous Discover Applicable Updates (DAU) task** field.

      This option defines the number of endpoint that can simultaneously run the DAU task.

   c) Type a value in the **Maximum number of reboot tasks that can run simultaneously** field.

      This option defines the number of endpoints that can simultaneously run the reboot task.

/HEAT®software

d) Type a value in the **Maximum number of simultaneously mandatory baseline deployments** field.

This option defines the number of endpoints that can simultaneously download Mandatory Baseline deployments.

e) Type a value in the **Maximum number of times a deployment will be consecutively attempted** field.

This option defines the number of failed deployment attempts allowed before the deployment is disabled. This option does not apply to Mandatory Baseline deployments. This option also disables the deployment for endpoints yet to retrieve.

4. Define the **Notifications defaults** options.

Complete the following substeps.

> **Tip:** You can type a maximum of 1000 characters in each field.

a) Select or clear the **User notification should always be on top** check box.

This option forces all notification dialogs to display on top of other windows.

b) Type the desired message in the **Manual installation** field.

This option defines the default message that displays when an endpoint receives a package requiring manual installation.

c) Type the desired message in the **May reboot** field.

This option defines the default message that displays when an endpoint receives a package that may require the recipient to reboot.

d) Type the desired message in the **Default deployment message** field.

This option defines the default message that displays with a deployment notification.

e) Type the desired message in the **Default reboot message** field.

This option defines the default message that displays with a reboot notification.

5. Define the **User Interface** option.

Select a **How should Deployment Wizard Start Times be displayed?** option.

- Agent Local Time (Deploy at local time for each individual node)
- Agent UTC Time (Deploy at UTC time for each individual node)

6. Click **Save**.

Result: The *Deployments* tab configuration is saved.

Exporting Option Data

To export the options settings that are listed on any *Options* page tab to a comma separated value (.csv) file, click the **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

Defining Access Rights

Access rights are individual privileges that define whether a user can access a system feature. These rights control availability for every HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) page, feature, function, and action. The pages and features available to users are based on the access rights associated with the role assigned to them. The system roles are assigned a default set of access rights. Users inherit the access rights of the role they are assigned.

Access rights begin with read-only access to system pages and permission to export data. At the administrative level, users can be assigned rights to fully manage the various system pages and functions.

Note: New access rights are added when you install new modules.

Access Right	Description	Access
All		
Dashboard		
View Dashboard	Access to view the home page dashboard.	
View Current Status	Access to view the status of the server.	
View HPL Widgets	Access to select and view the HEAT PatchLink DataCenter Dashboard widgets.	
Jobs		
View Discovery Scan Jobs	Access to view discovery scan jobs.	
Create Discovery Scan Jobs	Access to create and copy discovery scan jobs	
View Agent Management Jobs	Access to view agent management jobs.	
Create Agent Management Jobs	Access to create and copy agent management jobs.	
Manage Modules via Jobs	Access to install or uninstall agent modules using agent management jobs.	
Manage Jobs	Cancel, pause, resume, delete or merge all jobs the user has access to.	
Export Jobs	Export the jobs list.	
Vulnerabilities/Patch Content		

HEAT software

Access Right	Description	Access
View Content	Access to vulnerability and other content data.	🖥🖳☁🖴
Manage Content	Enable and disable vulnerabilities and other content.	🖥🖳
Export Content	Export vulnerability and other content data list.	🖥🖳☁
View Content Details	Access the detailed information for vulnerabilities and other content data.	🖥🖳☁
View My Custom Patch Lists	Access to view custom patch lists that this user has created.	🖥🖳☁
View All Custom Patch Lists	Access to view custom patch lists that all users have created.	🖥
Manage Custom Patch Lists	Edit, delete or copy custom patch lists that this user has access to.	🖥🖳☁
Endpoints		
View Endpoints	Access the manage endpoints all tab.	🖥🖳☁🖴
Manage All Tab	Enable and disable agents, delete endpoints, manage agent modules, and wake endpoints.	🖥🖳
Export All Tab	Export the all tab endpoints list.	🖥🖳☁
Manage Remotely	Access the remote management options available.	🖥🖳
View HPL Tab	Access the HEAT PatchLink DataCenter tab.	🖥🖳☁🖴
Manage HPL Tab	Install, uninstall, enable and disable the HEAT PatchLink DataCenter module.	🖥🖳
Export HPL Tab	Export the HEAT PatchLink DataCenter tab endpoints list.	🖥🖳☁
Download Agent Installers	Access to the Download Agent Installers page.	🖥🖳☁
Manage Agent Version	Access to the Manage Agent Version dialog.	🖥🖳
Scan Now Discover Applicable Updates	Scan endpoints using the DAU Scan Now Dropdown/button.	🖥🖳☁
Reboot Endpoints	Reboot endpoints using the Reboot Now button.	🖥
Inventory		

Access Right	Description	Access
View Inventory	View the endpoint inventory.	🖥️🎩☁️💾
Export Inventory	Export the endpoint inventory list.	🖥️🎩☁️
Groups		
View Groups	Access the groups.	🖥️🎩☁️💾
Manage Groups	Add, edit, enable, disable, and delete groups.	🖥️🎩
Export Groups	Export the groups list.	🖥️🎩☁️
Users		
View Users	Access the user groups.	🖥️🎩☁️💾
Manage Users	Add or remove users from individual user policies.	🖥️🎩
Export Users	Export the user groups list.	🖥️🎩☁️
Deployments and Tasks		
Create Deployments	Ability to create new deployments.	🖥️🎩☁️
View My Deployments and Tasks	Access the deployments and tasks that this user has created.	🖥️🎩☁️💾
View All Deployments	Access the deployments that all users have created.	🖥️🎩☁️
Manage Deployments and Tasks	Deploy, enable, disable, abort, and delete deployments and tasks that this user has access to.	🖥️🎩☁️
Export Deployments and Tasks	Export the deployments and tasks in the list that this user has access to.	🖥️🎩☁️
Packages		
View Packages	Access the package data.	🖥️🎩☁️💾
Manage Packages	Create, edit, and delete packages.	🖥️🎩
Export Packages	Export the package data list.	🖥️🎩☁️
Cache Packages	Ability to download packages from the GSS onto the local machine.	🖥️🎩
Agent Policy Sets		

HEAT software

Access Right	Description	Access
View All Agent Policy Sets	Access the agent policy sets.	💻👤☁️🖥️
Manage All Agent Policy Sets	Create, edit and delete agent policy sets.	💻
Export All Agent Policy Sets	Export the agent policy sets list.	💻👤
Security Configuration Management		
View SCM Data	Acess to view SCM data on the endpoint detail and groups views.	💻
Reports		
Reports Administer	Generate reports regardless of access rights for groups and endpoints.	💻
View My Core Reports	Generate core reports only for those items this user has access to.	💻👤☁️🖥️
View My HPL Reports	Generate HEAT PatchLink DataCenter reports only for those items this user has access to.	💻👤☁️🖥️
Export Reports	Export the generated reports.	💻👤☁️
Configure Enterprise Reporting (ER)	Configure settings to manage Configure Enterprise Reporting (ER)	💻
Users/Roles		
View Users	Access the users and roles list view.	💻👤☁️🖥️
Manage Users	Create, delete, enable, and disable users and roles.	💻
Export Users	Export the users and roles list.	💻👤
Change Password	Ability to change the password for users other than themselves.	💻
Manage Server Modules		
Installation Manager	Access the Installation Manager to install, update and uninstall server modules.	💻
Subscriptions		
View Subscription	Access the subscription service information.	💻👤☁️🖥️

Access Right	Description	Access
Manage Subscription	Edit or update subscription service updates.	[icon]
Export Subscription	Export the subscription service information.	[icons]
Directory/Computer Synchronization		
View Directory Sync Schedule	Access to view the active directory sync schedule page.	[icons]
Manage Directory Sync Schedule	Create, edit, delete, enable, disable directory syncs.	[icons]
Export Directory Sync Schedule	Export the directory sync schedule lists.	[icons]
Email notifications		
View Email Notifications	Access the email notifications page.	[icons]
Manage Email Notifications	Create and edit email notifications and settings for core feature. Note: All types of notifications may be deleted with this right.	[icon]
Manage HPL Email Notifications	Create and edit HEAT PatchLink DataCenter email notifications and settings. Note: All types of notifications may be deleted with this right.	[icon]
Export Email Notifications	Export the emails notifications list.	[icons]
Options		
View Options	Access to general, agent and deployment default server options.	[icons]
Manage Options	Set and edit general, agent and deployment default server options.	[icon]
Export Options	Export the options list.	[icons]
Technical Support		
View Technical Support	Access the technical product support information.	[icons]
Export Technical Support	Export the technical product support information.	[icons]
Licenses		
View Licenses	Access the product licenses.	[icons]

HEAT software

Access Right	Description	Access
Manage Licenses	Update product licenses.	
Export Licenses	Export the product license information.	

Chapter

5

Configuring Notifications

In this chapter:

- The Email Notifications Page
- Working with Email Notifications
- GSS Notifications

HEAT PatchLink DataCenter for Microsoft® System Center contains several features to notify users of system events and Global Subscription Service updates.

These features include:

- Email notifications. This feature uses your network mail server to send email that system events have occurred. For additional information, refer to The Email Notifications Page on page 76.
- Global Subscription Service notifications. You can subscribe to a RSS feed that lists updates posted to the Global Subscription Service. For additional information, refer to GSS Notifications on page 82.

HEAT®software

The Email Notifications Page

You can configure your server to send email notifications when certain system events occur. These notifications alert you when the system requires administration.

Figure 17: Email Notifications Page

From this page, you can perform the following actions:

- Define your mail server.
- Define email notification alert settings
- Define email addresses to receive notifications.
- Select email notifications

Email Notification Page Buttons

These buttons let you use functions available on the **Email Notification** page.

Table 42: Email Notification Page Buttons

Button	Function
Create...	Creates a new item to **Email Notifications**. For additional information, refer to Creating Email Notifications on page 80.
Save	Saves any page edits made.
Delete	Deletes selected items from **Email Notifications**. For additional information, refer to Deleting Email Notification Addresses on page 81.

Button	Function
Test	Sends a test email to selected email addresses. For additional information, refer to Testing Email Notifications on page 82.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

The Email Notifications Table

This table lists the email addresses that receive system alerts. You can also use this table to define a limitless number of addresses. The alert types sent to each email address can be customized.

Table 43: E-Mail Notification Table

Column	Description
Notification Address	Lists the email address that receives alert notifications. This address is not validated.
New Vulnerabilities	Alerts when a new content item becomes available for deployment.
New Agent Version	Alerts when a new version of the agent is downloaded.
Agent Registrations	Alerts when an agent successfully registers or attempts and fails to register with the server.
Subscription Failure	Alerts when any subscription replication fails.
Deployment Failure	Alerts when a deployment fails.
Low System Disk Space	Alerts when the available system drive space on the server falls below the defined minimum.
Low Storage Disk Space	Alerts when the available storage space on the drive where content is stored falls below the defined minimum.
Low Available License Count	Alerts when the number of licenses available to the server falls below the defined minimum.
Upcoming License Expiration	Alerts when licenses will expire within the defined time frame.
License Expiration	Alerts when a license expires.

Note: Check boxes only display in **Email Notifications** after you create an email notifications entry.

HEAT software

Alert Settings

Alert settings are values that trigger notification emails. These values are defined from the **Alert Settings** options. Edit these values to suit your network.

The following table describes the **Alert Settings** options.

Table 44: Alert Settings Options

Option	Definition	
Outgoing Mail Server (SMTP)	The mail host used to send emails.	
	Note: The **Outgoing Mail Server (SMTP)** is not an alert value setting. However, completion of this field with your network SMTP server is required to send email notifications.	
Low System Disk Space	Defines the threshold that initiates email notifications due to low system disk space.	
	Alert When Below *x* MB	Defines the level of system disk space that your server must drop below before an alert is sent (1-99999 MBs [97.65 GB]).
	Check Disk Every *x Interval*	Defines the interval between **Low System Disk Space** threshold checks. This interval is defined in minutes, hours, or days (1-999).
Low Storage Disk Space	Defines the threshold that initiates email notifications due to low storage disk space.	
	Alert When Below *x* MB	Defines the level of storage disk space that your server must drop below before an alert is sent (1-99999 MBs [97.65 GB]).
	Check Disk Every *x Interval*	Defines the interval between **Low Storage Disk Space** threshold checks. This interval is defined in minutes, hours, or days (1-999).

Option	Definition	
Low Available License Count	Defines the threshold that initiates email notifications due to low available license count.	
	Alert for any Module That Falls Below *x* Licenses	Defines the number of available licenses that your server must drop below before an alert is sent (1-999).
	While License Count Remains Low, Send a Reminder E-mail Every *x* Days	Defines if an alert is sent and the interval in days (1-99).
Upcoming License Expiration	Defines the threshold that initiates email notifications due to upcoming license expiration.	
	Alert for any License That Will Expire Within *x* Days	Defines the number of days before an alert is generated due to upcoming license expiration (1-99).
	While Licenses Aren't Renewed After This Alert, Send a Reminder E-mail Every *x* Days	Defines if an alert is sent and the interval in days (1-99).

Thresholds define the value that trigger email notifications, but not email notifications themselves. Email notifications are sent following Discover Applicable Updates tasks that find values below the defined thresholds.

Working with Email Notifications

From the ***Email Notifications*** page, you can define the email addresses that receive notifications. You can also define the events and values that trigger notification emails.

Configuring Alert Settings

Alert settings are values that trigger the HEAT PatchLink DataCenter for Microsoft System Center server to send email notifications. Define these values for preventive maintenance purposes.

Define alert settings from the ***Email Notifications*** page.

HEATsoftware

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Email Notifications**.

2. In the **Outgoing Mail Server (SMTP)** field, type the name of your outgoing mail server.

> **Note:** The outgoing mail server is not an alert setting value, but is necessary to define email notification addresses.

3. Define the **Low System Disk Space** options.

   This alert setting defines when email notifications are sent due to low system disk space.

   a) Type a value in the **Alert When Below *x* MB** field (1-99999).
   b) Type a value in the **Check Disk Space Every *x* Interval** field (1-999).
   c) Select an interval from the **Check Disk Space Every *x* Interval** list (**Minute(s)**, **Hours**, **Days**).

4. Define the **Low Storage Disk Space** options.

   This alert setting defines when email notifications are sent due to low storage disk space.

   a) Type a value in the **Alert When Below *x* MB** field (1-99999).
   b) Type a value in the **Check Disk Space Every *x* Interval** field (1-999).
   c) Select an interval from the **Check Disk Space Every *x* Interval** list (**Minute(s)**, **Hours**, **Days**).

5. Define the **Low Available License Count** options.

   This alert setting defines the number of available licenses that HEAT PatchLink DataCenter for Microsoft System Center must drop below before an email notification is generated.

   a) Type a value in the **Alert for any Module That Falls *x* Licenses** field. (1-999).
   b) If applicable, select the check box and type a value in the **While License Count Remains Low, Send a Reminder Email Every *x* Interval** field (1-99).

6. Define the **Upcoming License Expiration** options.

   This alert setting defines the number of days before an email notification is generated to upcoming license expiration.

   a) Type a value in the **Alert for any Licenses That Will Fall Within *x* Days** field (1-99).
   b) If applicable, select the check box and type a value in the **While Licenses Aren't Renewed After This Alert, Send a Reminder Email Every *x* Interval** field. (1-99).

7. Click **Save**.

Result: Your alert setting values are saved.

Creating Email Notifications

You can configure your mail server to alerts to people when system events occur. Define email notification recipients for preventative maintenance and administrative purposes.

Prerequisites:

Complete

Create email notifications from the *Email Notifications* page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Email Notifications**.

2. Click **Create**.

   Step Result: A new row displays in the **Email Notifications** table.

3. Type an email address in the **Notification Address** field of the new row.

   Note: The server does not validate email addresses.

4. Select the email notifications you want the address to receive.

5. Click **Save**.

Result: The email address and the selected notifications are saved. The address will receive a notification when system events occur.

Editing Email Notification Addresses

After an email notification address is created, you can edit the email address itself, or you can change notification types it receives.

Edit email notification addresses from the *Email Notifications* page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Email Notifications**.

2. From the **Notification Address** column, edit the desired email address fields.

3. Select or clear **E-Mail Notification** check boxes.

4. Click **Save**.

Deleting Email Notification Addresses

Delete email notification addresses that no longer need notification of HEAT PatchLink DataCenter for Microsoft System Center events.

Delete email notification recipients from the *Email Notifications* page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Email Notifications**.

2. Select the notification addresses that you want to delete.

   Step Result: The **Delete** button become active.

3. Click **Delete**.

   Step Result: The *Message from webpage* opens indicating the selected recipients have been removed.

HEAT software

4. Click **OK**.

Result: The notification address is deleted. An email that confirms the deletion is sent to the selected email addresses. Afterward, notification emails are no longer sent.

Exporting Email Notification Data

You can export email notification data to a comma separated value (`.csv`) file for reporting and analytical purposes.

All data on the page is exported. To export email notification data, select **Tools** > **Email Notifications** and click **Export**. For additional information, refer to Exporting Data on page 37.

Testing Email Notifications

Testing email notifications ensures that defined email addresses and HEAT PatchLink DataCenter for Microsoft System Center are properly configured for alerts. If a test fails, you should first verify that the email address is typed correctly in the **Email Notifications** table. If it is, you should then examine email and HEAT PatchLink DataCenter for Microsoft System Center settings.

Prerequisites:

An email address must be added to the **Email Notifications** table.

Test email notifications from the *Email Notifications* page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Email Notifications**.

2. Select the notification address(es) that you want to test.

Step Result: The **Test** button become active.

> **Tip:** When the **Select All** check box is selected, all items become checked within the list and the **Test** button becomes active.

3. Click **Test**.

Result: A notification informs you that the test email was sent. Acknowledge the notification by clicking **OK**. Access the applicable email address to ensure the notification was successful.

GSS Notifications

HEAT hosts a website that lists updates posted to the Global Subscription Service.

You can view these updates at http://gssnews.lumension.com/news/default.aspx?oem=Lumension .

Tip: Subscribe to the page RSS feed to receive regular GSS notifications.

Chapter

6

Licensing, Subscriptions, and Support

In this chapter:

- The Product Information Page
- The Product Licensing Page
- The Subscription Updates Page
- Working with Subscription Updates

While using HEAT PatchLink DataCenter for Microsoft® System Center (HEAT PatchLink DataCenter), you may need to request technical support or view information about your HEAT PatchLink DataCenter licenses.

View licensing information from the The Product Licensing Page on page 89. This page lists the HEAT PatchLink DataCenter modules you are licensed for.

View your subscription history from the The Subscription Updates Page on page 92. This page lists a history of replications with the Global Subscription Service.

Request technical support from the The Product Information Page on page 84. From this page you can request technical support and review technical information about your HEAT PatchLink DataCenter server.

HEAT software

The Product Information Page

This page contains links to various technical support pages. You can also use this page to give HEAT feedback for future product releases.

This page also lists system data about your HEAT Patch Manager DataCenter Server.
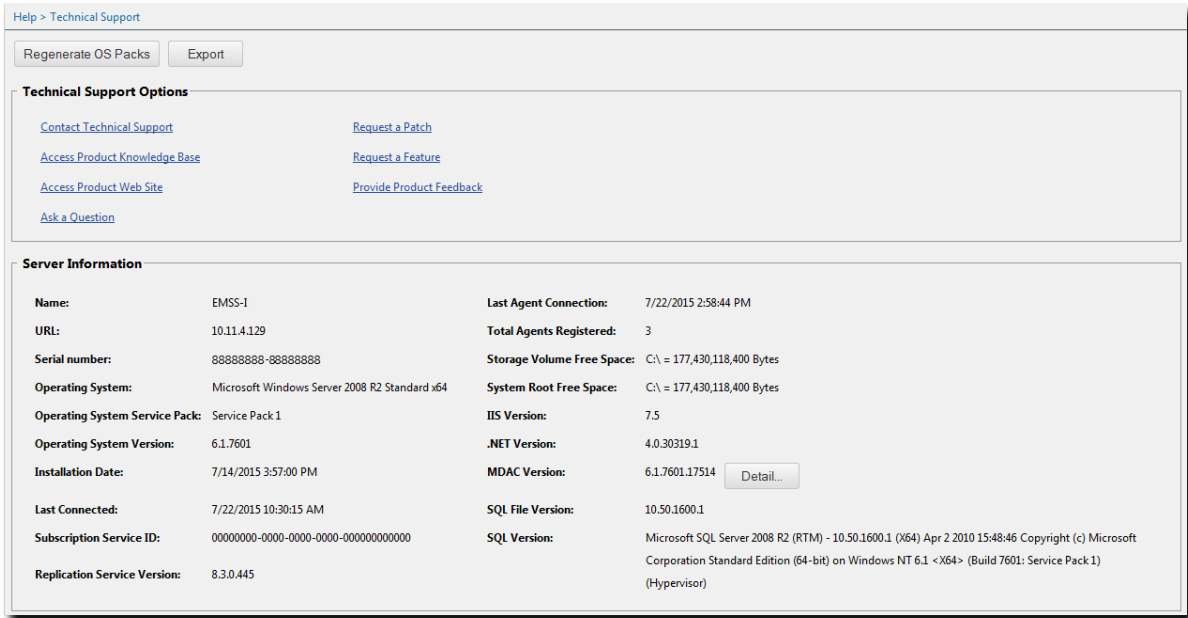
Figure 18: Product Information Page

Viewing the Product Information Page

Navigate to this page to access out-of-program technical support pages.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Product Information**.
2. Review the page.

Product Information Page Buttons

The *Technical Support* page features a button to download the most recent OS packs. OS packs are files used to detect operating systems.

The following table describes each button.

Table 45: Product Information Page Buttons

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Detail...	Opens a dialog that displays a detailed list of Microsoft Directory Access Components product and file versions. For additional information, refer to MDAC File Version Information on page 87.

Technical Support Options

HEAT provides access to various out-of-program technical support pages. Use these pages to communicate with HEAT. Click each link to open a new window to a support page.

Contact Technical Support	When having difficulty using HPL or any of its modules, send an email to HEAT technical support to open a ticket. Support staff will help you resolve your issues.
Access Product Knowledge Base	The HEAT Knowledge Base contains release notes, defects, hotfixes, frequently asked questions, how-to procedures, and troubleshoot information for the HEAT software portfolio.
Access Product Web Site	The HEAT corporate Web site for HPL includes information about its software portfolio and how it can benefit your enterprise. It also contains helpful information about how to identify and prevent IT security issues.
Ask a Question	If you have questions about HPL or other HEAT software, contact us.
Request a Patch	If you need a patch to keep your enterprise secure, send a message using our feature request page.
Request a Feature	If you want a new feature to improve your HPL user experience, send your request using our feature request page.

HEAT®software

Provide Product Feedback	HEAT uses customer feedback to improve HPL. If you have an idea to improve it, see our customer feedback Web page.

Server Information

These fields list general information regarding the HEAT PatchLink DataCenter for Microsoft System Center Server.

The following table describes the **Server Information** fields.

Table 46: Server Information Fields

Field	Description
Name	The name of the server HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) is installed on.
URL	The URL of the server HEAT PatchLink DataCenter is installed on.
Serial Number	The serial number used by HEAT PatchLink DataCenter.
Operating System	The operating system installed and running on the HEAT PatchLink DataCenter server.
Operating System Service Pack	The service pack applied to the operating system, if applicable.
Operating System Version	The operating system version number.
Installation Date	The date and time HEAT PatchLink DataCenter was installed.
Last Connected	The date and time HEAT PatchLink DataCenter last connected to the Global Subscription Service (GSS).
Subscription Service ID	The ID assigned to HEAT PatchLink DataCenter upon registration with the GSS.
Replication Service Version	The replication service version number.
Last Agent Connection	The date and time a registered HEAT PatchLink DataCenter Agent last connected to the HEAT PatchLink DataCenter server.
Total Agents Registered	The total number of agents registered with HEAT PatchLink DataCenter.
Storage Volume Free Space	The amount of free disk space on your storage volume.
System Root Free Space	The amount of free disk space on your system volume.
IIS Version	The Internet Information Services (IIS) version installed.
.NET Version	The .NET Framework version(s) installed.

Field	Description
MDAC Version	The Microsoft Data Access Components (MDAC) version. The **Detail** button adjacent to the field opens the *MDAC File Version Information* dialog.
SQL File Version	The SQL Server file version installed.
SQL Version	The SQL Server version number followed by detailed information.

Viewing the MDAC File Version Information Dialog
Navigate to this dialog to view MDAC file version information.

You can access this dialog from the *Technical Support* page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Product Information**.

2. Click **Detail**.

    Step Result: The *MDAC File Version Information* dialog opens.

3. View the MDAC file version data.

MDAC File Version Information
The *MDAC File Version Information* dialog lists the individual `.dll` files included within the version of Microsoft Data Access Components (MDAC) installed on your HEAT PatchLink DataCenter for Microsoft System Center server.
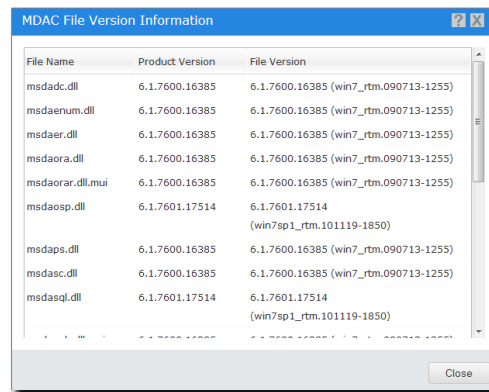
Figure 19: MDAC File Version Information Dialog

The following table describes the contents of the *MDAC File Version Information* dialog.

Table 47: MDAC File Version Information

Column	Description
File Name	The name of the MDAC `.dll` file.

HEAT software

Column	Description
Product Version	The product version number of the file.
File Version	The file version number of the file.

Suite Version Information

Suite Version Information displays the version number of HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter), each platform component installed, and each module component installed.

The following table describes each **Suite Version Information** field.

Table 48: Suite Version Information Fields

Field	Description
Server Suite Version	The version number of HEAT PatchLink DataCenter installed on your HEAT PatchLink DataCenter server.
Core Version	The version number of the HEAT PatchLink DataCenter core installed on your HEAT PatchLink DataCenter server.
***Module* Version**	The name and version number of a HEAT PatchLink DataCenter module installed on your HEAT PatchLink DataCenter server. A field appears for each module installed on your server.

Exporting Technical Support Data

You can export the data listed on the ***Product Information Page*** page for reporting and analytical purposes.

Exported data includes **Technical Support Options**, **Server Information**, and **Suite Version Information**. For additional information, refer to

The Product Licensing Page

Use this page to view, validate, and export license information. It summarizes product component licenses applicable to your endpoint management activities.

Figure 20: Product Licensing Page

Product information is updated during daily replication with the Global Subscription Service. Additionally, the page lists how many endpoint licenses you have, how many of those licenses are in use, and how many of those licenses are available.

Viewing the Product Licensing Page

Navigate to this page to view information about license validity and daily replication.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Product Licensing**.

2. View your product license data.

The Product Licensing Page Buttons

Use page buttons to initiate license replications or open HEAT Installation Manager. HEAT recommends initiating license replication after installing a new module.

The following table describes each button.

Table 49: Product Licensing Page Buttons

Button	Function
Validate	Initiates license replication. For additional information, refer to Initiating Subscription License Replication on page 91.
Launch Installation Manager...	Opens HEAT Installation Manager. For additional information, refer to Using HEAT Installation Manager on page 417 .

HEAT®software

Button	Function
Export	Exports the page data to a comma-separated value (.csv) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

The Product Licensing Page List

This list itemizes licensing information for each HEAT PatchLink DataCenter for Microsoft System Center module. View this table for an overview of license availability.

Table 50: Product Licensing Page List

Column	Description
Name	The product module name.
Version	The product module version number.
Vendor	The source of the license. Click the link to open the vendor home page.
Purchased (non-expired)	The total number of licenses purchased for the module that haven't expired.
In Use	The number of licenses in use for the module.
Pending	The number of licenses pending use or removal for the module.
Available	The number of licenses available for the module.

The list item for each product module can be expanded to display license group information. License groups are blocks of licenses purchased at a time. For example, you may have 3 license groups comprising 500 total licenses. Initially, a group of 300 licenses was purchased, and then 2 additional groups of 100 licenses were added during subsequent purchases.

To expand a list item, click its arrow (**>**).

Table 51: Expanded Product Licensing List Item

Column	Description
Purchase Date (Server)	The date and time the license group was purchased.
Effective Date (Server)	The date and time the license went into effect. This date is the first day that the licenses became valid, not necessarily the installation date.

Column	Description
Expiration Date (Server)	The date and time the license group expires.
Purchased	The total number of licenses purchased in the license group.

Initiating Subscription License Replication

Initiate replication to validate your licenses. Updates are made if your subscription has changed. Initiate replication after purchasing new modules.

Initiate license replication from the ***Product Licensing*** page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Product Licensing**.
2. Click **Validate**.

    Step Result: A dialog opens, prompting you to acknowledge the validation initiation.

3. Click **OK**.

Result: Replication begins. Completion may take several minutes.

Exporting Product Information

You can export product information data to a comma-separated value (.csv) file for reporting and analytical purposes.

For additional information, refer to

HEAT®software

The Subscription Updates Page

Periodically, your server downloads system updates from the Global Subscription Service. You can initiate these downloads, called *replications*, from the **Subscription Updates** page.

Figure 21: Subscription Updates Page

From this page, you can perform the following actions:

- Modify the subscription communication interval
- Initiate a replication
- Configure the subscription service
- View the subscription service replication history

Viewing the Subscription Updates Page

Navigate to the **Subscriptions Updates** page to view the subscription update history or to edit subscription settings.

You can access this page from the navigation menu.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.
2. [Optional] Perform a task listed in

Subscription Updates Page Toolbar

This toolbar controls the functions available from the **Subscription Updates** page. Click a toolbar button to initiate subscription function.

The following table describes each button's function.

Table 52: Subscription Updates Page Buttons

Button	Function
Save	Saves the page edits.
Update Now	Replicates all license, system, and content changes since the last replication with the Global Subscription Service (GSS). For additional information, refer to Updating HPL System Files and Content on page 100.
Reset	Resets the replication status. For additional information, refer to Resetting the Replication Status on page 101.
Configure...	Configures subscription communication settings. For additional information, refer to The Subscription Service Configuration Dialog on page 95.
Launch Installation Manager...	Opens HEAT Installation Manager. For additional information, refer to Using HEAT Installation Manager on page 417 .
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

Subscription Service Information

These fields list information about the Global Subscription Service and its communication history with your server.

Table 53: Subscription Service Information

Field	Description
Replication Host	The name and port of the Global Subscription Service (GSS).
Replication Status	The current replication status. Replication ensures that your server remains current with the latest content, package, and license information.

HEAT software

Field	Description
Account ID	Your account ID. The ID is uploaded to the GSS, which validates the update request. The account ID is created by your server when it registers with the GSS.
Communication Interval	The time your server connects to the GSS for replication. For additional information, refer to Editing the Communication Interval on page 102.
Last Poll	The date and time your server last replicated with the GSS.

Note: The **Communication Interval** field is the only setting within **Subscription Service Information** that can be edited.

Subscription Service History

This table lists a record of subscription license replications and content replications. Additional details for each replication are included.

Table 54: Subscription Service History Table

Column	Description	
Type	The type of replication. The types include:	
	Licenses	Verifies the validity of your system licenses.
	System	Downloads new core system files, including operating system definitions and agent upgrades.
	Package	Downloads the patch content (or packages) selected for caching. If automatic critical package caching is enabled, all critical packages are downloaded .
	Patch / Content	Updates the list of patch content available for download from the Global Subscription Service: • The operating systems you are licensed for. • The content languages you've selected.
	Patch / Components	Updates a file used during Discover Applicable Updates tasks that contains patch content definitions from vendors and the Global Subscription Service.

Column	Description
Status	The status of the replication task. The statuses include:
	`Initializing Replication` — Replications are initializing.
	`Downloading` — Replications are downloading.
	`Completed` — Replications are complete.
Start Date (Server)	The date and time on the server that the replication started.
Stop Date (Server)	The date and time on the server that the replication completed.
Duration	The duration of the replication.
Successful	The replication completion status (`True`, `False`, or `Failed`).

The Subscription Service Configuration Dialog

Use this dialog to configure communication behavior while your server is contacting the Global Subscription Service.
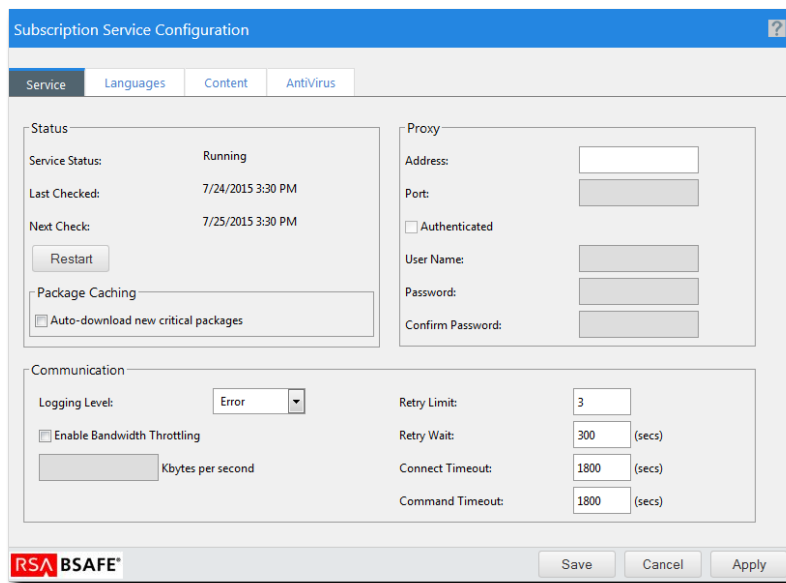
Figure 22: Subscription Service Configuration Dialog

HEAT software

Viewing the Subscription Service Configuration Dialog
Use this dialog to configure subscription service settings.

You can access this dialog from the **Subscription Updates** page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

2. Click **Configure**.

Result: The **Subscription Service Configuration** dialog opens.

The Service Tab
Using this tab, you can customize communication settings between your server and the Global Subscription Service.

You can use this tab to perform the following actions related to communications between your server and the Global Subscription Service:

• Select a logging level
• Configure a proxy
• Restart the subscription service

Status
The **Status** section lists whether the subscription service is running, as well as information about past and pending communication with the Global Subscription Service.

Table 55: Status Fields and Controls

Field or Control	Description
Service Status	The current status of the replication service on your server.
Last Checked	The last date and time on your server that the replication service last communicated with the GSS.
Next Check	The next scheduled date and time that the replication service will communicate with the GSS.
Restart	Restarts the replication service. For additional information, refer to Restarting the Replication Service on page 103.

Package Caching

This section lets you select whether packages related to critical vulnerabilities are automatically downloaded. Caching packages makes them available for immediate deployment, but consume additional storage space.

Table 56: Package Caching Option

Option	Description
Auto-download download critical packages	Indicates whether packages related to critical vulnerabilities are automatically downloaded. For additional information, refer to Configuring the Service Tab on page 102.

Proxy

When using a proxy for communication between the HEAT PatchLink DataCenter for Microsoft System Center server and the Global Subscription Service, you must define the applicable proxy information within HEAT PatchLink DataCenter for Microsoft System Center before communication can occur.

Define this proxy information from the **Subscription Service Configuration** dialog **Service** tab. The following table describes each setting.

Table 57: Proxy Setting Descriptions

Setting	Description
Address (field)	The IP address or name of the proxy used for communication between HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) and the Global Subscription Service (GSS).
Port (field)	The proxy port used for communication between HEAT PatchLink DataCenter and the GSS.
Authenticated (check box)	This check box enables the remaining fields when proxy authentication is required.
User Name (field)	A user name that will authenticate with the proxy.
Password (field)	The password associated with the user name.
Confirm Password (field)	The password retyped.

HEAT®software

Communication

When configuring replication service communication, you can set options for how your server communicates with the Global Subscription Service.

Define communication options from the **Subscription Service Configuration** dialog **Service** tab.

Table 58: Communication Option Descriptions

Option	Description
Logging Level	Defines the level of detail in logs recorded during communication between you server and the Global Subscription Service. The available values include:
	Debug — Logs errors, warnings, system actions, and debugging information.
	Note: This logging level is the most comprehensive. Only use this setting for troubleshooting purposes due to increased log size and replication times.
	Information — Logs errors, warnings, and system actions.
	Warning — Logs errors and warnings.
	Error — Logs only errors.
Enable Bandwidth Throttling	Limits the transmission speed during replication.
x Kbytes per second	Defines the maximum transmission speed when **Enable Bandwidth Throttling** is selected.
Retry Limit	The number of times your server attempts to reestablish communication with the GSS if the first attempt fails.
Retry Wait	The number of seconds between retries.
Connect Timeout	The number of seconds before a connection attempt is considered unsuccessful.
Command Timeout	The number of seconds of inactivity before a command is considered unsuccessful.

The Languages Tab

HEAT PatchLink DataCenter content and content definitions are available in multiple languages. From the **Languages** tab, you can define the languages that security content definitions are replicated for.

This tab is added after you install HEAT PatchLink DataCenter.

Generally, you should only select the languages that suit your network environment. The following languages are available:

Table 59: Agent Supported Languages

Description	Language Code	LCID string	Decimal	Hexadecimal
Chinese - China (Simplified)	zh	zh-cn / za-chs	2052	0804
Chinese - Taiwan (Traditional)	zh	zh-tw / zh-cht	1028	0404
Danish	da	da	0406	1030
Dutch - Netherlands	nl	nl-nl	1043	0413
English - United States	en	en-us	1033	0409
English - United Kingdom	en	en-gb	0809	041d
English - South Africa	en	en-za	7177	1c09
Finnish - Finland	fi	fi	1035	040b
French - France	fr	fr-fr	1036	040c
German - Germany	de	de-de	1031	0407
Italian-Italy	it	it-it	1040	0410
Japanese - Japan	ja	ja	1041	0411
Korean - Korea	ko	ko	1042	0412
Norwegian - Nynorsk	no	no-no	1044	0414
Portuguese - Brazil	pt	pt-br	1046	0416
Russian - Russia	ru	ru	1049	0419
Spanish - Spain (Modern Sort)	es	es-es	3082	0c0a
Swedish - Sweden	sv	sv-se	1053	041d

HEAT® software

The Content Tab

This tab lists Websites that your server can access through its firewall to download content directly from vendors rather than the Global Subscription Service.

- In some cases, you may need to download content directly from vendor Websites rather than the Global Subscription Service. This process expedites your access to new content within HEAT PatchLink DataCenter.
- Click **Export** to export the external sites listed on the tab.

Working with Subscription Updates

You can configure how the HEAT PatchLink DataCenter for Microsoft System Center server receives subscription updates from the Global Subscription Service by using the **Subscription Updates** page.

Updating HPL System Files and Content

You can update the latest HPL system components and content by completing a process call *Replication*. Replication downloads any system components, content definitions, or licensing information posted to the Global Subscription Service since the previous replication. Although the system automatically replicates once daily, you may occasionally need to replicate manually.

Initiate replications from the **Subscriptions Updates** page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

2. Click **Update Now**.

   Step Result: A notification dialog opens.

3. Acknowledge the replication by clicking **OK**.

Result: Replication begins immediately. All license and content changes since the last replication are downloaded. This process may take several minutes, and no Discover Applicable Update tasks run during completion.

Resetting the Replication Status

Resetting the replication status forces the HEAT PatchLink DataCenter for Microsoft System Center server to re-download (or update) the licenses, packages, and content.

Reset the replication status from the *Subscription Updates* page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

2. Click **Reset**.

    Step Result: The *Reset Replication* dialog opens.

3. Select a replication option.

> **Note:**
>
> *   The options available in the *Reset Replication* dialog change based on whether the **Auto-download new critical packages** option is selected. For additional information, refer to Package Caching on page 97.
> *   If you have cached packages for content that is disabled, those packages are not updated during replication if a new version is available.

Context	Options
If the Auto-download new critical packages option is selected	Select from the following options: • Cache metadata and critical packages for only new and changed content. • Cache metadata and critical packages for all historical content.
If the Auto-download new critical packages option is cleared	Select from the following options: • Cache both metadata and critical packages. • Only cache metadata.

4. Define when you want to begin replication.

    Click the applicable button.

    *   To begin replication immediately, click **Update Now**.
    *   To being replication at the next scheduled interval, click **Update Later**.

Result: You replication status is reset when the next replication begins.

Editing the Communication Interval

Edit the communication interval to control the daily time when you server downloads content and license data from the Global Subscription Service.

Edit the communication interval from the **Subscription Updates** page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.
2. Select a time from the **Communication Interval** list.

   This list includes a value for every half-hour.
3. Click **Save**.

   Step Result: A dialog opens, notifying that the new setting was saved.
4. Click **OK**.

Result: The selected communication interval is saved. Your server will replicate daily at the selected time.

Configuring the Service Tab

Configuring the **Service** tab defines communication, proxy, and log settings for replication.

Prerequisites:

Configure the **Service** tab from the **Subscription Service Configuration** dialog.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.
2. Click **Configure**.

   Step Result: The **Subscription Service Configuration** dialog opens.
3. Ensure the **Service** tab is selected.
4. To automatically download packages associated with content items with a status of critical, select the **Auto-download new critical packages** check box .
5. Define **Proxy** options.

   These options define the proxy information used for communication between the server and the Global Subscription Service (GSS).

   Tip: For additional information about each option, refer to Proxy on page 97.

   a) Complete the **Address** and **Port** fields.
   b) If your proxy server requires authentication, select the **Authenticated** check box and complete the **User Name**, **Password**, and **Confirm Password** fields.

6. Define **Communication** options.

These options define actions related to your server communication with the GSS.

> **Tip:**
> - For additional information about each option, refer to Communication on page 98.
> - Under most conditions, the **Retry Limit**, **Retry Wait**, **Connect Timeout**, and **Command Timeout** options require no editing.

a) Select a **Logging Level** from the list.
b) To limit communication speeds during replication, select the **Enable Bandwidth Throttling** check box and type a number in the **X Kbytes per second** field.
c) Type a number in the **Retry Limit** field.
d) Type a number in the **Retry Wait** field.
e) Type a number in the **Connect Timeout** field.
f) Type a number in the **Command Timeout** field.

7. Click **Save** to apply your changes.

> **Tip:** If you want to continue using the *Configuration Settings* dialog, click **Apply** instead of **Save**.

Result: Your edits are saved. These edits will take effect the next time HEAT PatchLink DataCenter communicates with the GSS.

After Completing This Task:
If you edited the **Logging Level**, you must restart the replication service before the changes take place. For additional information, refer to Restarting the Replication Service on page 103.

Restarting the Replication Service

You can restart the replication service on your server using the Web console.

You can restart the subscription service from the *Subscription Service Configuration* dialog *Service* tab.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

2. Click **Configure**.

   Step Result: The *Subscription Service Configuration* dialog opens.

3. Ensure the *Service* tab is selected.

4. Click **Restart**.

5. Acknowledge the notification by clicking **OK**.

Result: The replication service is restarted on your server.

HEAT software

Configuring the Languages Tab

Selecting language options downloads new localized content definitions to your server. You can deploy their content later. Select additional languages when you administrate an environment that uses multiple localizations.

Select language options from the **Subscription Server Configuration** dialog **Languages** tab.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

2. Click **Configure**.

    Step Result: The **Subscription Service Configuration** dialog opens.

3. Select the **Languages** tab.

4. Select the check boxes for each language you want content item definitions. Clear any unused languages.

    > **Note:**
    > - Selecting multiple languages increases the number of content definitions downloaded, slowing replication times.
    > - The **English** check box cannot be cleared.

5. Click **Save**.

    > **Tip:** If you want to continue working withing the **Subscription Server Configuration**, click **Apply** instead.

Result: Your edits are saved. Content definitions for the selected languages are downloaded during the next replication.

Exporting Enhanced Content Data

While viewing the **Content** tab, you can export the listed content URLs to a comma separated value (.csv) file.

For additional information refer to Exporting Data on page 37.

Exporting Subscription Update Data

You can export data displayed on the **Subscription Updates** page to a comma separated value (.csv) file for reporting and analysis.

Both **Subscription Service Information** and **Subscription Service History** are exported. To export this data, go to the **Administration** workspace, select **HEAT PatchLink DataCenter for Microsoft System Center** > **Configuration** > **Subscription Updates** and click the **Export** button. For additional information refer to Exporting Data on page 37.

Chapter

7

Using Endpoints

In this chapter:

- About Endpoints
- The Endpoints Page
- Working with the Endpoints Page
- The Endpoint Details Page
- Working with the Endpoint Details Page

While using HEAT PatchLink DataCenter for Microsoft® System Center (HEAT PatchLink DataCenter), you can view and manage network endpoints after installing agents.

The **Endpoints** page contains a listing of all endpoints that have an agent registered with the HEAT PatchLink DataCenter server. From this list of endpoints, you can access the endpoint details. The endpoint details include endpoint-specific information.

About Endpoints

The **Endpoints** page is used to manage the computers and devices, referred to as *endpoints*, on your network. The HEAT PatchLink DataCenter for Microsoft System Center server manages your endpoints by sending user-defined and automated commands to your endpoints' agents. When the agent contacts the server, the commands are executed.
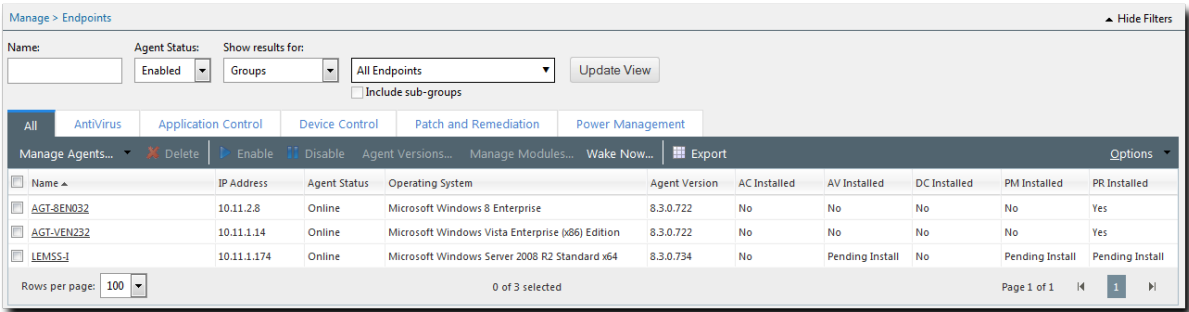
Figure 23: Endpoints Page

The **Endpoints** page lists all endpoints registered to the HEAT PatchLink DataCenter server. The page displays general information about the endpoint, such as the endpoint name, status, operating system, and agent version.

The Endpoints Page

The **Endpoints** page contains information about the managed endpoints on your network. From the **Endpoints** page, you can use features associated with endpoints.
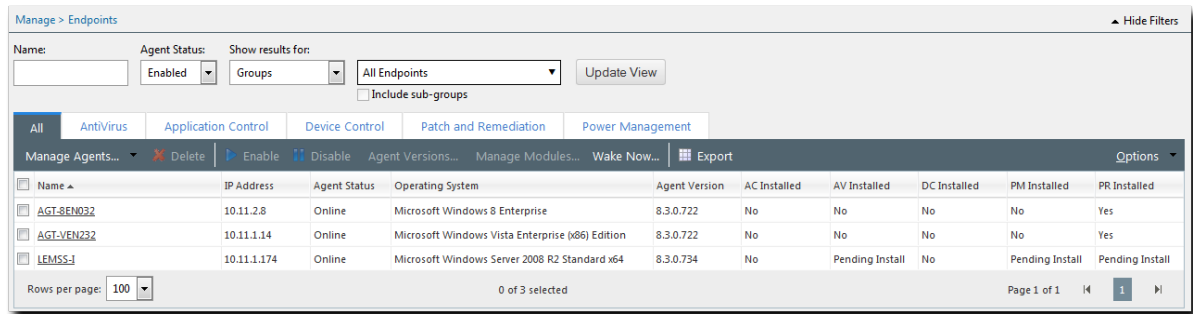
Figure 24: Endpoints Page

The Endpoints Page Toolbar

The Endpoints Page toolbar contains the tasks and functions that are available for you to perform for managed endpoints with HEAT PatchLink DataCenter features enabled.

The following table describes the Endpoints Page toolbar functions.

Table 60: Endpoints Page Toolbar Functions

Button	Function
Deploy...	Launches the **Deployment Wizard**, which allows you to create a deployment for the selected endpoints. For additional information, refer to Deploying Content to Endpoints on page 112.
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting an Endpoint on page 113.
Enable Agent	Enables a disabled endpoint. For additional information, refer to Enabling the HEAT PatchLink DataCenter Agent for Linux/UNIX on page 114.
Disable Agent	Disables an enabled endpoint. For additional information, refer to Disabling the HEAT PatchLink DataCenter Agent for Linux/UNIX on page 114.

Button	Function
Scan Now...	Prompts the Discover Applicable Updates task to launch immediately (within the agent hours of operation) and scan all agent-managed endpoints within your network for vulnerabilities. This scan queues an inventory of vulnerabilities that will run the next time the agent checks in with the server. For additional information, refer to Using Scan Now to Scan Inventory on page 114.
Reboot Now...	Prompts the selected endpoint to reboot. For additional information, refer to Rebooting Endpoints on page 115.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options	Opens the **Options** menu. For more information, see The Options Menu on page 30.

The Endpoints Page List

The HEAT PatchLink DataCenter tab list itemizes identification data, server connectivity, operating system, and agent information for endpoints with the HEAT PatchLink DataCenter agent module.

The following table describes the columns within the **Endpoints** page.

Table 61: HEAT PatchLink DataCenter Tab List Columns

Column	Description
Name	The name of the endpoint. Clicking the **Name** link displays the applicable **Endpoint Details** page. See The Endpoint Details Page on page 116 for additional information.
IP Address	The IP address of the endpoint.
Status (icon)	The icon representing the HEAT PatchLink DataCenter module status. You can mouse over the icon to display description of the HEAT PatchLink DataCenter status. For additional information, refer to Agent Module Status Icons on page 110.

HEAT®software

Column	Description
Agent Status	Indicates the status of the endpoint. The following list defines column values:

	Online	The agent is able to communicate with the HEAT PatchLink DataCenter server in the predefined time period. Refer to Configuring the Agents Tab on page 65 for additional information on configuring agent default behavior.
	Offline	The agent is unable to communicate with the HEAT PatchLink DataCenter server in the predefined time period. In an Offline status, the agent still enforces all policies.
		Note: A **Warning** (🔖) icon next to an Offline status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is either offline or has an update required status. Click the icon to find out additional status details and EDS server information.
	Disabled	The agent will no longer enforce any module policies or complete tasks. All endpoints must show a Disabled status in order to delete the endpoint. Refer to Disabling the HEAT PatchLink DataCenter Agent for Linux/UNIX on page 114.
Last Connected Date (Server)	Exported comma separated value (.csv) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.	

Column	Description
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values:

	Started	EDS server has started and is in an operational state accepting workloads.
	Starting	EDS server is in the process of starting its service.
	Stopped	EDS server has stopped and is not accepting workloads.
	Stopping	EDS server is in the process of stopping so as to not accept workloads.
	Offline	EDS server is offline as it has not contacted the database in the configured amount of time.

Column	Description
HPL Status	The status for HEAT PatchLink DataCenter module on the endpoint (`Working`, `Idle`, `Sleeping`, `Offline`, `Disabled`).
DAU Status	The status of the Discover Applicable Updates (DAU) scan when last run. The status is also a link to the applicable ***Deployment Results*** page. Status values include: `Success` or `Failure` followed by the failure code, and `Not Available`, which indicates that the endpoint has not checked in.
	Note: The `Not Available` **DAU Status** is not a hyperlink
Last DAU Scan (Server)	The date and time of the last successful DAU scan (server side). A value of `Not Available` indicates the endpoint has not completed a DAU scan.
Operating System	The operating system the endpoint is running.
HPL Running Version	The HEAT PatchLink DataCenter module version number running on the endpoint.
Agent Type	The type of agent that is running on the endpoint and communicating with HEAT PatchLink DataCenter for Microsoft System Center.

/HEAT®software

Column	Description
Agent Version	Indicates the version of the agent that the endpoint is currently running.
	Note: A icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.

Agent Module Status Icons

Within HEAT PatchLink DataCenter for Microsoft System Center, icons are used to indicate agent statuses regarding agent activity. These icons appear on various pages. By understanding these icons, you can understand what activity is occurring on any specified patch endpoint.

The following table defines agent (endpoint) status and associated icons.

Table 62: Endpoint Status Icons

Active	Pending	Description
	N/A	The agent is currently working on a deployment (animated icon).
		The agent is idle, and has pending deployments.
		The agent is offline.
	N/A	The agent is offline because the Endpoint Distribution Service the endpoint is connected to is offline or requires an update.
		The agent is sleeping due to its hours of operation settings.
		This agent is disabled.
		The agent is offline and is in a chain status (can accept chained deployments until only after reboot).

Active	Pending	Description
		The agent is offline and is in a reboot status (can accept no more deployments until after it reboots).
		The agent is in a chain status (the agent can accept chained deployments only until after a reboot).
		The agent is in a reboot status (the agent can accept no more deployments until after it reboots).
		The agent is in a chain status (the agent can accept chained deployments only until after a reboot) and is sleeping due to its hours of operation settings.
		The agent is in a reboot status (the agent can accept no more deployments until after it reboots) and is sleeping due to its hours of operation settings.
	N/A	Unable to identify the agent status.

For more information about reboot and chained endpoint status, refer to Reboot and Chained State on page 291.

Viewing the Endpoints Page

The **Endpoints** page has filters that allow you to customize your view of the computers and other devices that are managed on your network.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. [Optional] Complete a task listed in Working with the Endpoints Page on page 111.

Working with the Endpoints Page

You can perform a number of tasks related to endpoints using toolbar buttons on the **Endpoints** page. Click a button to perform a task. Some buttons are not available until one or more list item is selected.

HEAT software

The following list displays the tasks that you can perform from the **Endpoints** page.

Deploying Content to Endpoints

Within HEAT PatchLink DataCenter for Microsoft System Center, content can be deployed from a number of pages, including the **Endpoints** page. When deploying from this location, the **Deployment Wizard** is preconfigured to deploy to endpoints selected from the list.

You can deploy content from the **Endpoints** page. For additional information about deployments, refer to About Deployments on page 289.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. [Optional] Select the endpoints you want to deploy content to.

3. Click **Deploy**.

After Completing This Task:
Review Using the Deployment Wizard on page 303 and complete the subsequent tasks.

Installing an Agent

Before you can manage a network endpoint, you must install an agent. You can install an agent manually or using a wizard.

There are two ways in which you can install an agent on an endpoint:

- Install an agent locally by browsing to the HEAT PatchLink DataCenter server from the endpoint that you want to manage and downloading the agent installer. For additional information, refer to Downloading the Agent Installer on page 112.

Downloading the Agent Installer

You can install an agent locally by connecting to the HEAT PatchLink DataCenter for Microsoft System Center, downloading the agent installer, and running the installer on the endpoint that you want to manage.

The following procedure describes the steps required to download the agent installer to the endpoint that you want to manage using HEAT PatchLink DataCenter for Microsoft System Center. The agent system requirements and installation procedure varies by operating system.

1. Log in to the target computer as the local administrator (or a member of the **Local Administrators** group).

2. Log into your HEAT PatchLink DataCenter for Microsoft System Center.

   For additional information, refer to Logging In.

3. From the **Navigation Menu**, select **Tools** > **Download Agent Installer**.

4. Select the endpoint operating system from the **Operating System** drop-down list.

5. Select the agent version that you want to install on the endpoint from the **Agent Version** drop-down list.

   > **Note:** The agent versions available for selection are defined by the **Agent Version Options**, which you can edit from the *Options* page *Agents* tab. For additional information, refer to Agent Versions on page 62.

6. Click **Download**.

Result: A *Download File* dialog opens, prompting you to save or open the installer.

Deleting an Endpoint

Deleting an endpoint removes its record from the HEAT PatchLink DataCenter for Microsoft System Center.

Prerequisites:

The endpoints you want to delete must be disabled. For additional information, refer to Disabling the HEAT PatchLink DataCenter Agent for Linux/UNIX on page 114.

Delete endpoints from the *Endpoints* page *All* tab.

> **Note:** Deleting an endpoint removes its record from the HEAT PatchLink DataCenter for Microsoft System Center database, but it does not remove the agent on the endpoint.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Ensure the **All** tab is selected.

3. Ensure the page is filtered to display disabled agents.
   For additional information, refer to Using Filters on page 33.

4. Select one or multiple endpoints with disabled agents.

5. In the toolbar, click **Delete**.

   Step Result: A *delete confirmation* dialog displays.

6. Click **OK** to confirm the deletion.

Result: The endpoint is deleted from the list.

HEAT®software

Enabling the HEAT PatchLink DataCenter Agent for Linux/UNIX

Disabled HEAT PatchLink DataCenter Agent for Linux/UNIXs can be reenabled at any time. Enabling a HEAT PatchLink DataCenter Agent for Linux/UNIX allows it to be included in the security management activities of the HEAT PatchLink DataCenter for Microsoft System Center.

Enable endpoints from the *Endpoints* page.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.
2. Select the disabled endpoint(s) you want to enable.
3. Click **Enable Agent**.

Result: The agent and all modules are enabled.

Disabling the HEAT PatchLink DataCenter Agent for Linux/UNIX

Once the HEAT PatchLink DataCenter Agent for Linux/UNIX on an endpoint is disabled, the installed modules no longer function. Disabled HEAT PatchLink DataCenter Agent for Linux/UNIXs remain listed and can be re-enabled at any time.

Disable endpoints from the *Endpoints* page.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.
2. Select the enabled endpoint(s) you want to disable.
3. Click **Disable Agent**.

Result: The endpoint is displayed in the list of endpoints identified with the disabled icon in the **Status** column. After disabling an agent, the endpoint can be deleted from HEAT PatchLink DataCenter for Microsoft System Center.

> **Note:** Once disabled, the endpoint may not appear in the list based on the **Status** filter settings. To include disabled endpoints in the list, ensure you select **Disabled** or **All** in the **Agent Status** filter.

Using Scan Now to Scan Inventory

You can initiate a Discover Applicable Updates task at any time. When you initiate this task, the agent scans its host endpoint for vulnerabilities and inventory. Scan results are then uploaded to the HEAT PatchLink DataCenter for Microsoft System Center server, which you can view.

You can launch a Discover Applicable Updates task for all network endpoints or selected network endpoints from the *Endpoints* page.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Schedule a DAU task for all endpoints or selected endpoints.

Use one of the following methods.

Method	Steps
To schedule a DAU task for all endpoints:	**1.** Click **Scan Now**. **2.** Select **Yes, scan all members of the selected** group check box.
To schedule a DAU tasks for selected endpoints:	**1.** From the toolbar, select the check boxes associated with the desired endpoint(s). **2.** Click **Scan Now**. **3.** Select the **Yes, scan the selected endpoints** check box.

3. Click **Schedule**.

4. Acknowledge the scheduling by clicking **Close**.

Result: The scan is scheduled. As with all deployments, the Discovery Applicable Updates task is scheduled for immediate execution. Deployment occurs the next time the target endpoints communicate with the server.

Rebooting Endpoints

You can use HEAT PatchLink DataCenter for Microsoft System Center to reboot the managed endpoints on your network. This function is useful after installing content.

Reboot endpoints from the *Endpoints* page **HEAT PatchLink DataCenter Server for Microsoft System Center** tab.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Select the endpoints you want to reboot.

3. Click **Reboot Now**.

Step Result: The *Reboot Now* dialog opens.

4. Select the **Yes, Reboot the selected endpoint** check box.

5. Click **Reboot**.

Step Result: The system schedules the reboot.

6. Click **Close**.

Result: The dialog closes and the devices reboot the next time they check in with the server.

HEAT software

Exporting Endpoint Information

You can export the endpoint information generated in the HEAT PatchLink DataCenter for Microsoft System Center so that it can be used in other applications.

The export utility lets you export endpoint information to a comma-separated value (`.csv`) file format. For additional information, refer to Exporting Data on page 37.

The Endpoint Details Page

The **Endpoint Details** page lists general endpoint information, agent information, the modules installed on the endpoints, the groups the endpoint is included in, and the group policies applied to it. This page also includes a tab for each module installed.
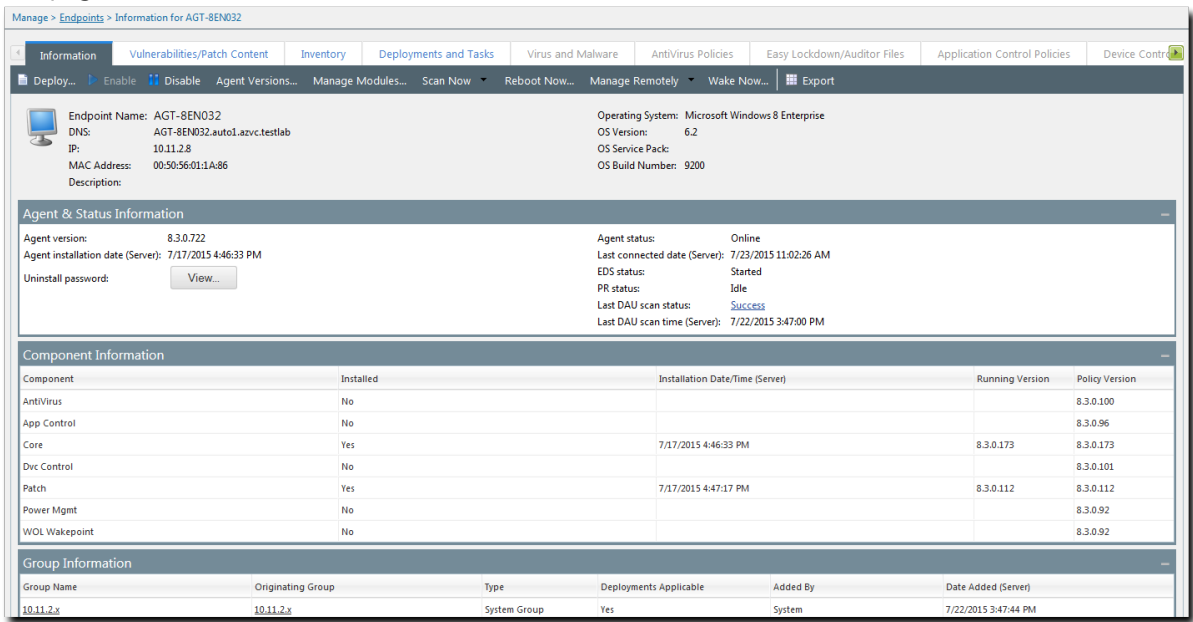
Figure 25: Endpoint Details Page

This page features the following tabs:

- The Information Tab on page 117
- The Vulnerabilities/Patch Content Tab on page 123
- The Deployments and Tasks Tab on page 127

Viewing the Endpoint Details Page

The **Endpoint Details** page contains comprehensive details for an endpoint and its activity within the HEAT PatchLink DataCenter for Microsoft System Center system.

View the **Endpoint Details** page for an endpoint by clicking an endpoint name link from the **Endpoints** page.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Click the **Name** link associated with the endpoint details you want to review.

   Step Result: The **Endpoint Details** page opens to the **Information** tab.

3. [Optional] Complete a task listed in

The Information Tab

The **Information** tab displays information about a selected endpoint. The page displays general information organized into endpoint, agent, status, component, group, and policy sections.

Figure 26: The Information Tab

Tip:

- Each **Information** tab section can be collapsed and expanded.
- Each section can also be dragged higher or lower on the page. Place more frequently used information high on the page.

HEAT® software

The Information Tab Toolbar

The **_Information_** tab toolbar contains the endpoint assessment tasks and functions that are available for you to perform on managed endpoints.

The following table describes the buttons available in the **_Information_** tab toolbar.

Table 63: Information Tab Toolbar Buttons

Toolbar Button	Description
Deploy...	Opens with **_Deployment Wizard_**, which lets you deploy content to the applicable endpoint. For additional information, refer to Deploying Content (Endpoint Details Page) on page 132.
Enable	Enables the endpoint (if it is disabled). For additional information, refer to Enabling an Endpoint on page 132.
Disable	Disables the endpoint (if it is enabled). For additional information, refer to Disabling an Endpoint on page 133.
Scan Now	Prompts the Discover Applicable Updates task to immediately check the endpoint. For additional information, refer to Using Scan Now (Endpoint Details Page) on page 135.
Reboot Now...	Prompts the selected endpoint to reboot. For additional information, refer to Rebooting Endpoints on page 115.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

Tip: For additional information about using core features, refer to _The Information Tab Toolbar_ in the HEAT Endpoint Management and Security Suite User Guide (http://portal.lumension.com) .

Endpoint Information

The fields that appear in this section of the *Information* tab contain identifier and operating system details, such as the IP address and the operating system.

The **Endpoint Information** section displays the following endpoint data:

Table 64: Endpoint Information Field Descriptions

Field	Description
Endpoint Name	The name of the endpoint.
DNS	The DNS name of the endpoint.
IP	The IP Address of the endpoint.
MAC Address	The MAC address of the endpoints.
Description	The description of the endpoint, if available.
Operating System	The abbreviated name of the operating system detected on the endpoint.
OS Version	The version number of the operating system running on the endpoint.
OS Service Pack	The service pack level of the endpoint.
OS Build Number	The build number of the operating system running on the endpoint.

Agent and Status Information

The fields that appear in the **Agent and Status Information** section of the *Information* tab contain status and connectivity details for the agent installed on the endpoint.

The following fields are added to **Status Information** after HEAT PatchLink DataCenter is installed.

Table 65: Status Information Field Descriptions

Field	Description
Agent version	The version of the agent that the endpoint is currently running.
Agent installation date (Server)	The date and time on the server when the agent registered with HEAT PatchLink DataCenter for Microsoft System Center. This is typically the date the agent was installed on the endpoint.

HEAT software

Field	Description		
Agent status	Indicates the status of the endpoint. The following list defines column values:		
	Online		The agent is able to communicate with the HEAT PatchLink DataCenter server in the predefined time period. Refer to Configuring the Agents Tab on page 65 for additional information on configuring agent default behavior.
	Offline		The agent is unable to communicate with the HEAT PatchLink DataCenter server in the predefined time period. In an `Offline` status, the agent still enforces all policies.
			Note: A **Warning** () icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) the endpoint connects to is offline. Click the icon to find out additional status details.
	Disabled		The agent will no longer enforce any module policies or complete tasks. All endpoints must show a `Disabled` status in order to delete the endpoint. Refer to Disabling the HEAT PatchLink DataCenter Agent for Linux/UNIX on page 114.
Last connected date (Server)	The date and time on the server that the agent last communicated with HEAT PatchLink DataCenter for Microsoft System Center.		
EDS Status	The status of the Endpoint Distribution Service on the server. Service statuses include **Started** and **Stopped**.		
HPL status	The HEAT PatchLink DataCenter status for the endpoint.		
Last DAU scan status	The status of the Discover Applicable Updates (DAU) scan when last run. The status also serves as a link to the ***Deployment Results*** page. Status values include: `Success`, `Failure` followed by the failure code, and `Not Available`, which indicates that the endpoint has not checked in.		
	Note: The `Not Available` **Last DAU Status** does not serve as a hyperlink.		
Last DAU scan time (server)	The time of the last successful DAU scan. A value of `Not Available` indicates the endpoint has not completed a DAU scan.		

Component Information

This table lists which module components are installed on the endpoint.

The following table describes each **Component Information** table column.

Table 66: Component Information Table

Column	Description
Component	Indicates the name of the applicable module.
Installed	Indicates whether the module is installed on the endpoint.
Installation Date/Time (Server)	Indicates the date and time on the server that the user initiated a module install.
Running Version	Indicates the version of the module installed on the agent.
Policy Version	Indicates the version of the module that is should be installed based on the agent version defined in the applicable agent policy set.

Group Information

The columns that appear in the **Group Information** section of the *Information* tab contain group membership details for the endpoint.

The **Group Information** section displays the following group data for an endpoints.

Table 67: Group Information Column Descriptions

Column	Description
Group Name	The group that the endpoint holds membership in, either through direct assignment or inheritance. Click the group name to open *Group Information* page.
Originating Group	The name of the group in the parent hierarchy from which the the endpoint inherits membership. If the endpoint is directly assiged to the group, the **Originating Group** value is identical to the **Group Name**. Click the originating group name to go to the *Group Information* page.
Type	The group type, which can include: • **System Group**: a group created by HPL • **Custom Group**: a group created by a user • **My Groups**: an indication that the group is within the group hieracrchy
Deployments Applicable	Indicates that there are applicable deployments available for this endpoint.
Added By	The HPL user who added the endpoint to the group. If the endpoint was added by HPL, the column contains a value of `System`.

HEAT®software

Column	Description
Date Added (Server)	The date and time that the endpoint was added to the group.

Note:
- If the values in the **Group Name** and the **Originating Group** columns are identical, then the endpoint is directly assigned to that group and is not inherited.
- Groups listed in gray indicate that the endpoint holds group membership through inheritance.

Policy Information

The fields that appear in the **Policy Information** section of the *Information* tab contain details about the policies used by the endpoint during a deployment.

New HEAT PatchLink DataCenter Server for Microsoft System Center policies are listed if they have been applied to the endpoint.

These policies are the results of applying each of the policies defined by the endpoint's group membership and filling in any undefined policies from the Global Policy. Conflict resolution rules are applied when applicable.

Table 68: Policy Information Column Descriptions

Column	Description
Name	The name of the policy applied to the endpoint.
Value	The value of the policy applied to the endpoint.
Description	The description of the policy.

Tip: For a description of all agent policies, including agent policies not applied to the endpoint, refer to The Agent Policy Sets Page List on page 224.

The Vulnerabilities/Patch Content Tab

The **Vulnerabilities/Patch Content** tab displays vulnerability information associated with the selected endpoint. The tab displays the same information shown on each **Patch Content** page (My Default Patch View, Vulnerabilities, Software, and so on). However, this tab is filtered for the endpoint.
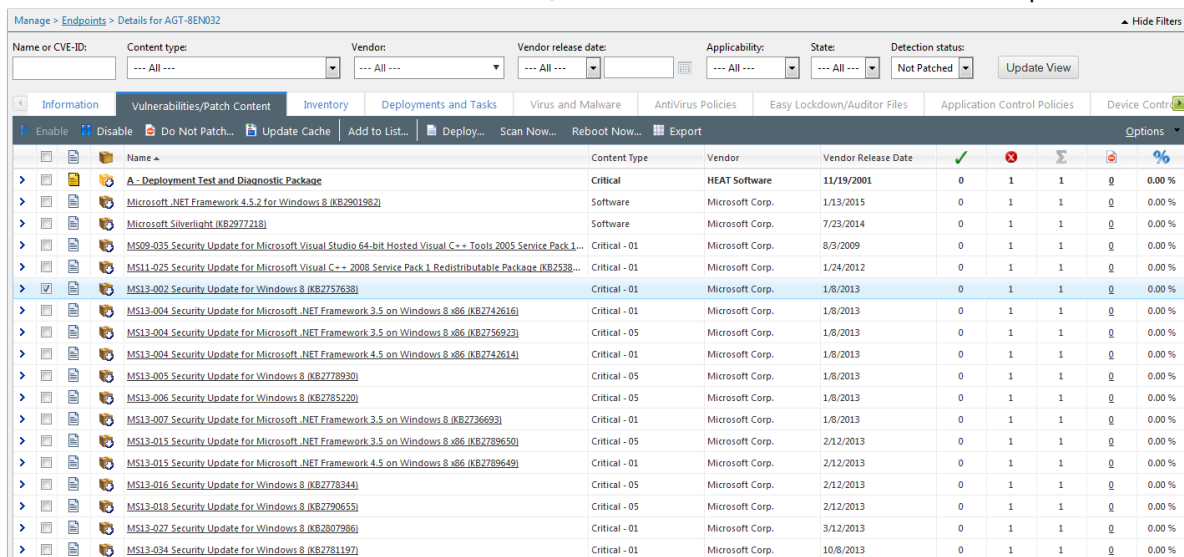
Figure 27: The **Vulnerabilities/Patch Content** Tab

The Vulnerabilities/Patch Content Tab Toolbar

The **Vulnerabilities/Patch Content** tab toolbar contains the tasks and functions that are available for you to perform on managed endpoints.

Table 69: Vulnerabilities/Patch Content Tab Toolbar Functions

Button	Function
Enable	Enables a selected disabled vulnerability. For additional information, refer to Enabling Content on page 130.
Disable	Disables a selected enabled vulnerability. For additional information, refer to Disabling Content on page 130.
Do Not Patch...	Disables the selected patch for specific groups and endpoint that you select. For more information, see Disabling Content for Groups/Endpoints on page 355.
Update Cache	Updates the package cache for selected packages. For additional information refer, to Updating the Cache on page 131.
Deploy...	Opens the **Deployment Wizard**. For additional information, refer to Deploying Content (Endpoint Details Page) on page 132.

HEAT software

Button	Function
Scan Now...	Prompts the Discover Applicable Updates task to launch immediately and scan all agent-managed endpoints within your network for vulnerabilities. For additional information, refer to Using Scan Now (Endpoint Details Page) on page 135.
Reboot Now...	Prompts the selected endpoint to reboot. For additional information, refer to Rebooting the Endpoint on page 136.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Vulnerabilities/Patch Content Tab List

The **Vulnerabilities/Patch Content** tab list tracks package name, cache status, content type, and deployment data.

The following table describes each list column.

Table 70: Column Definitions

Column	Icon	Definition
State	📄	The content item state, which indicates when the server downloaded the content item metadata. For additional information, refer to Content Status and Type on page 349.
Package Status	📦	The cache status for the content item, which indicates if the server downloaded the content item packages. For additional information, refer to Content Icons and Descriptions on page 350.
Name	N/A	The content item name, which links to the **Patch Status** of the item. For additional information, refer to The Patch Status Page on page 361.

Column	Icon	Definition
Content Type	N/A	Indicates the content item type. For more information, see one of the following topics: • Vulnerabilities on page 341 • Software Content on page 342 • Other Content on page 342
Vendor	N/A	The name of the vendor that created the software in the content item.
Vendor Release Date	N/A	The date and time that the vendor released the software in the content item.
Number of endpoints which came up Patched	✓	The number of endpoints patched with the content item.
Number of endpoints which came up Not Patched	✗	The number of endpoints not patched with the content item.
Total applicable	Σ	The number of endpoints that the content item applies to.
Number of endpoints which came up Do Not Patch	⊟	The number of endpoints that administrators have created a patch exception for.
Percent patched	%	The the percentage of applicable endpoints patched with the content item.

Additionally, you can expand each content item by clicking its arrow (**>**). The following table describes each field that displays when you expand a content item.

The following detail information appears on this page.

Table 71: Content Item Field Descriptions

Name	Description
Beta	Indicates if the content item is in beta.
Downloaded on (UTC)	The date and time on which the content was downloaded.
Associated packages	The number of packages associated with the content item.
Package status	The cache status for the content item packages.
HPL ID	The HPL identifier for the content item.
State	The enabled/disabled/completed status of the content item.

HEAT®software

Name	Description
Enabled/Disabled by	The HPL user who last disabled or enabled the content.
Enabled/Disabled date (Server)	The date and time the content was disabled or enabled.
Enable/Disable reason	The reason the user provided for disabling or enabling the content. You can click the **Edit** link to change the reason.
Vendor product ID	The identifier given to the security content item by the vendor.
Vendor release date/time (UTC)	The date and time the vendor released the software in the content item.
Common Vulnerability Exploit (CVE) [1]	The CVE number for the content.
Vulnerability Code Description [1]	A description of the vulnerability associated with the content item.
Reference Text [1]	The reference text(s) associated with the content item vulnerability.
Description [1]	The narrative description of the distribution package. This section may include important notes about the content item and a link to more information.
[1]This meta data appears conditionally based on whether it was added for the content item. Additionally, there may be multiple instances of each meta data section.	

The Deployments and Tasks Tab

The **Deployments and Tasks** tab lists the deployments assigned to an endpoint and their status. Deployments remain listed until deleted.
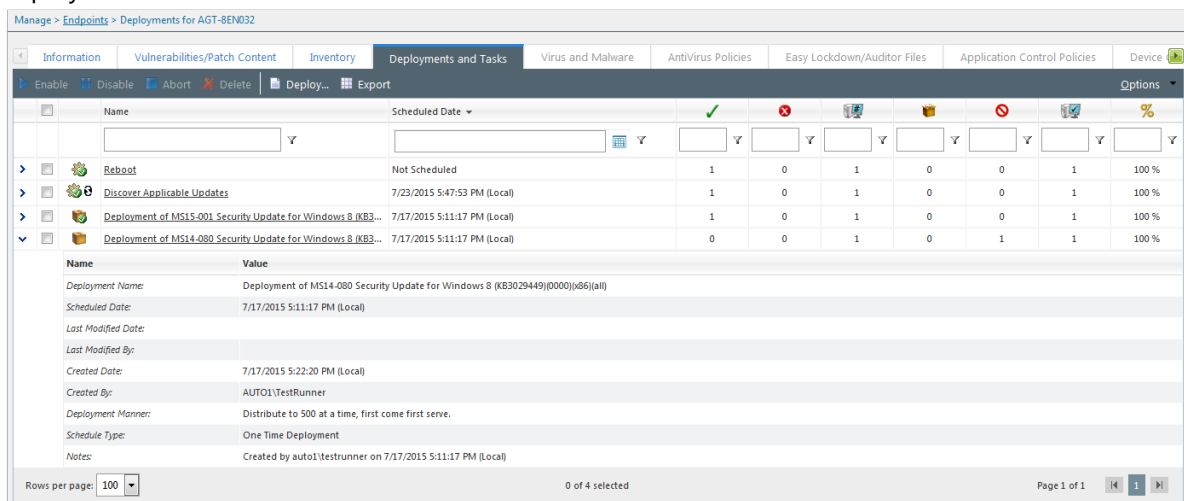
Figure 28: Deployments Tab

The Deployments and Tasks Tab Toolbar

The **Deployments and Tasks** tab toolbar contains buttons that let you control existing deployments and export deployment data.

The following table describes each toolbar button.

Table 72: Deployments and Tasks Tab Toolbar Functions

Menu Item	Function
Enable	Enables the selected disabled deployment. For additional information, refer Enabling Deployments on page 133.
Disable	Disables the selected deployment. For additional information, refer to Disabling Deployments on page 134.
Abort	Cancels the deployment or task for any endpoints which have not already received the deployment package. For additional information, refer to Aborting Deployments on page 134.
Delete	Removes the deployment from your HEAT PatchLink DataCenter for Microsoft System Center. For additional information, refer to Deleting Deployments on page 135.
Deploy...	Opens the **Deployment Wizard**. For additional information, refer to Deploying Content (Endpoint Details Page) on page 132.

HEAT software

Menu Item	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Deployments and Tasks Tab List

The **Deployments and Tasks** tab list contains a record of each deployment for the endpoint. Each list item remains until deleted.

The following table describes each list column.

Table 73: Deployments and Tasks Tab List Column Descriptions

Column	Icon	Description
Status Icon	N/A	An icon that indicates the status of the package deployment.
Name	N/A	The name of an individual package or task included in a deployment targeted at the endpoint (*not* the name of the deployment itself). Click the name to display **Deployment Details**. For more information, see The Deployment Details Page on page 335.
Scheduled Date	N/A	The date and time a user scheduled the package or task to deploy.
Number of endpoints/groups which were successful	✔	The total number of endpoints and groups that finished the deployment successfully.
Number of endpoints/groups which failed	⊗	The total number of endpoints and groups that finished the deployment unsuccessfully.
Number of endpoints/groups assigned to the deployment	🖥#	The total number of endpoints and groups that are assigned to the deployment.

Column	Icon	Description
Number of endpoints/groups which are in progress		The total number of endpoints and groups that are receiving the deployment.
		Note: If you deploy to a group using Agent Local Time, the deployment remains in progress until all time zones have passed. This behavior ensures any endpoints added to the group following deployment start also receive content. This behavior does not occur when using Agent UTC Time.
Number of endpoints/groups which were not deployed		The total number of endpoints and groups that were excluded from the deployment (because the package was already applied, not applicable, or marked *Do Not Patch*).
Number of endpoints/groups which have completed the deployment		The total number of endpoints and groups that finished the deployment.
Percentage Complete	%	The percentage of endpoints and groups that finished the deployment. Percentage = [Total Finished endpoints / Total Assigned endpoints]

Working with the Endpoint Details Page

You can perform a number of tasks related to endpoints from the **Endpoint Details** page. You perform most of these tasks regardless of the tab selected. However, certain tasks are specific to certain tabs.

To perform most tasks associated with endpoints, click a toolbar button. To perform some tasks, selecting one or multiple endpoints from the page list may be necessary.

HEAT software

The following list displays the tasks you can perform from the **Endpoint Details** page.

Enabling Content

After disabling a content item, you can renable it from the **Vulnerabilities/Patch Content** tab. You can only deploy enabled content.

You can re-enable content from the **Endpoint Details** page **Vulnerabilities/Patch Content** tab.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint for which you want to enable content for.

    Step Result: The **Endpoints Details** page opens with the **Information** tab selected by default.

3. Select the **Vulnerabilities/Patch Content** tab.
4. [Optional] Use the page filters to sort content.
5. Select one or multiple disabled content items from the list.
6. Click **Enable**.

Result: The content item displays with the **Enabled** icon in the status column.

Disabling Content

Disabling a content item will prevent that content item from being deployed.

You can disable content from the **Endpoint Details** page **Vulnerabilities/Patch Content** tab.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint for which you want to disable content for.

    Step Result: The **Endpoints Details** page opens with the **Information** tab selected by default.

3. Select the **Vulnerabilities/Patch Content** tab.

4. [Optional] Use the page filters to sort content.

5. Select one or multiple content items from the list.

6. Click **Disable**.

> **Note:** If you disable a content item that's already been cached, the package will not be updated if a new version of the content item is released.

Result: The content item displays with the **disabled** icon in the status column.

Updating the Cache

Updating the cache initiates a process that gathers the packages associated with the selected vulnerability and copies those packages to your HEAT PatchLink DataCenter Server for Microsoft System Center Server.

You can update the cache for content from the **Endpoint Detail** page **Vulnerabilities/Patch Content** tab.

> **Note:** For optimum installation order, HEAT recommends caching content prior to deployment. Failure to cache content prior to deployment may result in repeated endpoint reboots that interrupt work flow on those endpoints.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Click the link in the **Name** column that corresponds to the endpoint for which you want to cache content for.

   Step Result: The **Endpoints Details** page opens with the **Information** tab selected by default.

3. Select the **Vulnerabilities/Patch Content** tab.

4. [Optional] Use the page filters to sort content.

5. Select the check boxes associated with the content to cache.

6. Click **Update Cache**.

   Step Result: The **Warning** dialog box opens, informing you that the update request and this action may take an extended period of time.

   > **Note:** The cache will not be updated for disabled content items that have had a new version released.

7. Click **OK**.

Result: The selected content begins caching.

HEAT software

Deploying Content (Endpoint Details Page)

Within HEAT PatchLink DataCenter for Microsoft System Center, content can be deployed from a number of pages, including the tabs of the **Endpoints Details** page. When deploying from this page, the **Deployment Wizard** is preconfigured according to the tab you deploy from.

For additional information, refer to About Deployments on page 289.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Click the link in the **Name** column that corresponds to the endpoint for which you want to deploy content.

   Step Result: The **Endpoints Details** page opens.

3. Deploy content.

   To deploy content, select a tab and complete the applicable substeps. Tab selection controls how the **Deployment Wizard** is preconfigured for deployment.

Tab	Steps
To deploy content from the Information tab:	1. Ensure the **Information** tab is selected. 2. Click **Deploy** The **Deployment Wizard** opens, preconfigured to deploy content to the selected endpoint.
To deploy content from the Vulnerabilities/Patch Content tab:	1. Select the **Vulnerabilities/Patch Content** tab. 2. Select the content you want to deploy. 3. Click **Deploy** The **Deployment Wizard** opens, preconfigured to deploy the selected content to the selected endpoint.
To deploy content from the Deployments and Tasks tab:	1. Select the **Deployments and Tasks** tab. 2. Click **Deploy**. The **Deployment Wizard** opens without any options preconfigured.

After Completing This Task:
Review Using the Deployment Wizard on page 303 and complete subsequent tasks.

Enabling an Endpoint

Enabling an endpoint includes the endpoint in the content management activities of the HEAT PatchLink DataCenter for Microsoft System Center.

You can enable an endpoint from the **Endpoint Details** page.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Click the link in the **Name** column that corresponds to the endpoint that you want to enable.

   Step Result: The *Endpoints Details* page opens with the *Information* tab selected by default.

3. Click **Enable**.

Result: The endpoint is enabled.

Disabling an Endpoint

Disabling an endpoint stops agent functions on an endpoint. Disabled endpoints are not included in security management activity.

You can disable an endpoint from the *Endpoint Details* page.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Click the link in the **Name** column that corresponds with the endpoint you want to disable.

   Step Result: The *Endpoints Details* page opens with the *Information* tab selected by default.

3. Click **Disable**.

   Step Result: A *disable confirmation* dialog displays.

4. In the *confirmation* dialog box, click **OK**.

Result: The endpoint is disabled. After disabling an agent, the endpoint can be deleted from HEAT PatchLink DataCenter for Microsoft System Center.

> **Note:** Once disabled, the endpoint may not appear in the *Endpoints* page list based on the **Status** filter settings. To include disabled devices in the list, ensure you select **Disabled** or **All** in the **Status** filter.

Enabling Deployments

Enabling deployments resumes disabled (or paused) deployments to continue.

You can enable deployments from the *Endpoint Details* page *Deployments and Tasks* tab.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Click the link in the **Name** column that corresponds to the endpoint for which you want to enable deployments for.

   Step Result: The *Endpoints Details* page opens with the *Information* tab selected by default.

3. Select the *Deployments and Tasks* tab.

4. [Optional] Use the page filters to sort deployments.

5. Select the disabled deployments you want to enable.

HEAT®software

6. Click **Enable**.

Result: The selected deployments are enabled.

Disabling Deployments

Disabling deployments pauses deployments and stops the distribution of package(s) to an endpoint that has not already received the deployment.

You can disable deployments for a specific endpoint from the *Endpoint Details* page *Deployments and Tasks* tab.

Note: You cannot disable deployments of system task packages.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Click the link in the **Name** column that corresponds to the endpoint for which you want to disable deployments for.

   Step Result: The *Endpoints Details* page opens with the *Information* tab selected by default.

3. Select the *Deployments and Tasks* tab.

4. [Optional] Use the page filters to sort deployments.

5. Select the deployments you want to disable.

6. Click **Disable**.

Result: The selected deployments are disabled.

Aborting Deployments

Aborting deployments cancels deployments for the endpoint that has not already received the deployment.

Note: The endpoints that have already received the deployment will not be affected. The deployment will be aborted for endpoints that have not yet received the deployment.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Click the link in the **Name** column that corresponds to the endpoint for which you want to abort deployments for.

   Step Result: The *Endpoints Details* page opens with the *Information* tab selected by default.

3. Select the *Deployments and Tasks* tab.

4. [Optional] Use the page filters to sort deployments.

5. Select the deployments you wish to abort.

6. Click **Abort**.

   Step Result: A confirmation message displays, asking you to confirm that you want to abort the deployment.

7. Click **OK** to confirm that you want to abort the deployment.

Result: The selected deployment is canceled.

> **Note:** You cannot abort system tasks or Mandatory Baseline deployments.

Deleting Deployments

Deleting deployments removes them from HEAT PatchLink DataCenter for Microsoft System Center. Delete a deployment if you to prevent its content from reaching endpoints.

You can delete deployments for individual endpoints from their *Endpoint Details* page *Deployments and Tasks* tab.

> **Note:** Deleting deployments has no effect on endpoints that have already received the deployments. You cannot delete system task deployments.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Click the link in the **Name** column that corresponds to the endpoint for which you want to delete deployments for.

   Step Result: The *Endpoints Details* page opens with the *Information* tab selected by default.

3. Select the *Deployments and Tasks* tab.

4. [Optional] Use the page filters to sort deployments.

5. Select the deployments you want to delete.

6. Click **Delete**.

> **Note:** Before you can delete a deployment in progress, you must abort the deployments.

   Step Result: A confirmation message displays, asking you to confirm that you want to delete the selected deployments.

7. Click **OK** to delete the deployments.

Using Scan Now (Endpoint Details Page)

You can initiate a Discover Applicable Updates task at any time. When you initiate this task, the agent scans its host endpoint for vulnerabilities. Scan results are then uploaded to the HEAT PatchLink DataCenter for Microsoft System Center server, which you can view.

You can schedule a Discover Applicable Updates task for the selected endpoint the *Endpoint Details* page.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

HEAT software

2. Click the *Endpoint Name* link of the endpoint you want to schedule a Discover Applicable Updates task for.

    Step Result: The ***Endpoint Details*** page for the endpoint opens.

3. Select one of the following tabs:

    - ***Information***
    - ***Vulnerabilities/Patch Content***

4. From the toolbar, click **Scan Now**.

5. Select the **Yes, scan the selected endpoint** check box.

6. Click **Schedule**.

7. Acknowledge the scheduling by clicking **Close**.

Result: The scan is scheduled. As with all deployments, although the Discovery Applicable Updates task is scheduled for immediate execution. It will not actually occur until the next time the agent checks in.

Rebooting the Endpoint

You may reboot an endpoint at any time. Rebooting an endpoint may be necessary following some deployments.

You can reboot an individual endpoint from its ***Endpoint Details*** page ***Information*** tab.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Click the link in the **Name** column that corresponds with the endpoint you want to reboot.

3. Select one of the following tabs:

    - The **Information** tab
    - The **Vulnerabilities/Patch Content** tab

4. Click **Reboot Now**.

    Step Result: The ***Reboot Now*** dialog opens.

5. Select the **Yes, Reboot the selected device** check box.

6. Click **Reboot**.

    Step Result: The system schedules the reboot.

7. Click **Close**.

Result: The window closes.

Exporting Endpoint Information

You can export the endpoint information generated in the HEAT PatchLink DataCenter for Microsoft System Center so that it can be used in other applications.

The export utility lets you export endpoint information to a comma-separated value (`.csv`) file format. For additional information, refer to Exporting Data on page 37.

HEAT software

Chapter

8

Using Groups

Within HEAT PatchLink DataCenter for Microsoft® System Center, you can organize endpoints into groups, which are collections of endpoints. Organizing endpoints into a group lets you manage them as a single object.

About Groups

A *group* is a collection of endpoints that you can manage collectively. Within HPL you can create custom groups to administer all endpoints as a single object.

Groups are organized into a tree hierarchy in which groups are nested; groups can contain other groups. This structure allows for inheritence of group members and policies, helping to minimize endpoint maintenance.

•   For more information about the controls used to managed groups, see The Groups Page Browser on page 141.
•   For more information about how you can use groups and their hierarchy to simplify HPL administration, see Group Hierarchy on page 142.
•   For more information about the different types of groups in HPL, see Defining Groups on page 143.

HEAT software

The Groups Page

Use this page to control groups. The functions from many other HEAT PatchLink DataCenter for Microsoft System Center pages are available from this page (the **Endpoints** page, the **Users and Roles** page, and so on). However, the functions performed on the **Groups** page pertain primarily to the selected group's endpoints.

Groups are selected from the **Browser**, a **Groups** page pane. The browser displays an expandable tree that lists parent and child groups. From this browser, you can access group information by clicking a group. Information for the selected group displays in the main pane.
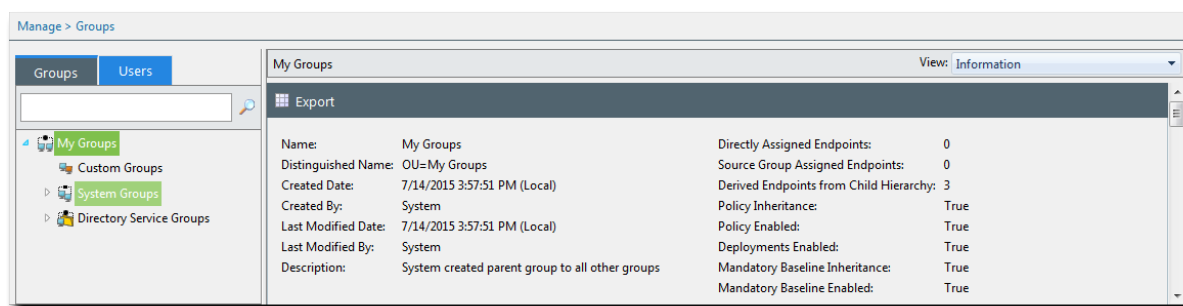
Figure 29: Groups Page

Unlike most other HEAT PatchLink DataCenter for Microsoft System Center pages, which are organized by tabs, the **Groups** page is organized by views, which are selectable from the **View** list. The information displayed for a selected group changes according to view.

The views are:

- The Information View on page 144
- The Group Membership View on page 149
- The Endpoint Membership View on page 157
- The Mandatory Baseline View on page 164
- The Vulnerabilities/Patch Content View on page 185
- The Deployments and Tasks View on page 191
- The Agent Policy Sets View on page 196
- The Roles View on page 204
- The Dashboard View on page 209
- The Settings View on page 211

The Groups Page Browser

Interact with all groups in HPL by using the *Groups* page **Browser**, which organizes your groups into a tree hierarchy.
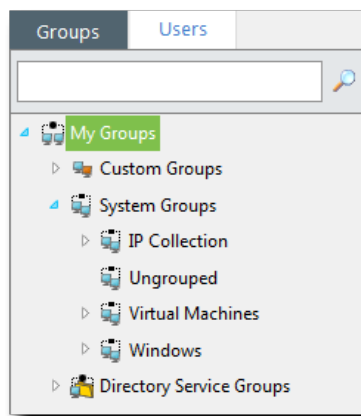
Figure 30: Browser

You can interact with the **Browser** in a variety of ways:

- You can expand the group hierarchy by clicking the **triangle**.
- You can collapose the group hierarchy by clicking click the **triangle** again.
- You can interact with a group by selecting it and using the *Groups* page features.
- You can create a new group, add endpoints to the selected group, or change views for the selected group by right-clicking it and making a selection from the menu.
- You can drag and drop custom groups by dragging the custom groups *icon* (not the group name) into another group.

> **Note:** Remember a couple of thing when you are dragging and dropping groups:
>
> - You can't drag a group down within its own child hierarchy. Groups can be moved to other group hierarchys however.
> - If you drag a group with a child hierarchy into another group, the child hierachy gets moved as well.
> - If the group you are moving is inheriting Agent Policy Sets, moving that group will change the policies it inherits. Before moving the group, check what Agent Policy Sets the group is inheriting, because moving a group without understanding its inherited policies can result in *big* changes to endpoint behavior!

Group Hierarchy

Within the *Groups* page **Browser**, groups are organized into a tree hierarchy. This hierarchy creates a structure similar to a family tree. This structure allows you to aggregate group membership and settings through inheritance. Familiarize yourself with examples of group hierarchy in this topic to understand how groups impact endpoint group membership and settings.
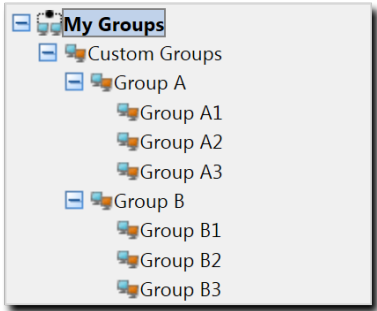
Figure 31: Group Tree Example

Root Group	In the HPL group tree structure, the root group is the group of origin, which has no parents or ancestors. Within HPL, **My Groups** is the root group, and all other groups are its descendent.
Parent Group	A parent group is a group that is one branch higher in the tree than the groups below it. In the figure above, **Group A** is parent of **Group A1**, **Group A2**, and **Group A3**. A parent group can have multiple child groups, and these children inherit the parent group settings.
Child Group	A child group is a group that is one branch lower in the tree than its parent. In the figure above, **Group A1** is the child of **Group A**. Each child group can only have one parent, and the child group inherits its parent settings by default.
Sibling Groups	Sibling groups are groups that share a parent group. In the figure above, **Group A** and **Group B** are siblings. Any group can have zero, one, or more siblings.
Ancestor Groups	Ancestors groups are all the groups above a group in the tree hierarchy for a single lineage. In the figure above, **Group A1** has ancestor groups of **Group A**, **Custom Groups**, and **My Groups**. **Group B** *is not* an ancestor group for **Group A1**.
Descendent Groups	Descendent groups are all the groups below a group in the tree hierarchy. In the figure above, **Customs Groups** has descendants in **Group A** (and all its child groups) and **Group B** (and all its child groups).
Leaf Group	A leaf group is a group that has no children. In the figure above, **Group A1** is a leaf group.

Inheritance	Inheritance is the mechanism that allows groups to aggregate endpoint membership and settings.

- Endpoint membership is inherited *up* the tree. For example, endpoints added to **Group A3** are aggregated to with the endpoints directly assigned to **Group A**.
- Settings (such as mandatory baselines and agent policies) are inherited *down* the tree. For example, an Agent Policy Set assigned to **Custom Group**s is also assigned to **Group A**, as well as groups **A1**, **A2**, and **A3**. Setting inheritance is enabled by default, but you can also disable it. Each group has its own inheritance settings. See Editing Group Settings on page 212.

Note: Within the **Browser**, `System Groups` and `Directory Service Groups` hierarchies cannot be modified. For additional information on group types, refer to Defining Groups on page 143.

Defining Groups

Within HEAT PatchLink DataCenter for Microsoft System Center, there are several types of groups. Some groups are created by users, while others are created by the HEAT PatchLink DataCenter for Microsoft System Center system. When working with groups, only user-created groups can be deleted.

Groups are categorized into the following classifications.

Table 74: Group Definitions

Groups	Group Type	Icon	Description
My Groups	Custom Groups	(Parent) and (Child)	Custom groups are created and managed by the user.
	System Groups[1]	(Parent) and (Child)	These groups are system created groups.
	Directory Service Groups	(Parent) and (Child)	These groups are created when an agent submits a directory service hierarchy that does not already exist in HEAT PatchLink DataCenter for Microsoft System Center. You cannot modify **Directory Service Groups** or their hierarchies.

HEAT software

Groups	Group Type	Icon	Description
(1) Endpoints identified in your network are automatically assigned a group membership based on IP address, Active Directory (AD) membership, or operating system. Not all IP ranges, AD groups, or operating systems may be shown. This omission is because HEAT PatchLink DataCenter for Microsoft System Center creates system groups based on only the endpoints present in your network.			

Note: An **Ungrouped** group is a group of endpoints that have not yet been added to a custom group. A **Virtual Machines** group is a group that is created for endpoints that are in a virtual machine environment (VMware, Citrix, etc). You cannot modify **System Groups** or their hierarchies.

Viewing Groups

Navigate to the *Groups* page to work with groups. After navigating to the page, select a group and a view.

You can select this page from the navigation menu at any time.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. Expand the **Browser** tree to the desired group.

3. Select the group you want to view.

    Step Result: The selected group's information displays.

4. Select the desired view from the **View** list.

    Tip: You may right-click within the **Browser** tree and select either the **Create Group** option, **Add Endpoints to Groups** option, or a specific view. You must be on **Custom Groups** to utilize the **Create Group** or **Add Endpoints to Groups** option.

Result: The selected group's information displays on the main pane. Select a different view from the **View** list to change the information displayed.

The Information View

This view includes basic information about the selected group's membership, hierarchy, agent policy sets, roles, and so on. Select this view for a comprehensive listing of group settings.

Group settings and information appear in sections. Each section displays information for each type of group settings. Empty sections indicate undefined settings.

The **Information** view features the following sections:

The following table describes the **Information** view buttons.

Table 75: Information View Button

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

Group Information

The first section in the **Information** view displays general information about the selected group's settings. These settings are controlled within the various **Groups** page views. Select this view when you want to see a group's settings from a single source.

The following table describes the first fields within the first section of the **Information** view.

Table 76: Group Information

Field	Description
Name	Indicates the name of the group.
Distinguished Name	Indicates the system-created name based upon the group's parent hierarchy.
Created Date	Indicates the date and time the group was created.
Created By	Indicates the user who created the group.
Last Modified Date	Indicates the date and time the group was last modified.
Last Modified By	Indicates the user who last modified the group.
Description	Indicates the description of the group.

HEAT software

Field	Description
Directly Assigned Endpoints	Indicates the number of endpoints assigned to the group. Inherited endpoints are not included.
Source Group Assigned Endpoints	Indicates the number of endpoints assigned to the source group.
Derived Endpoints from Child Hierarchy	Indicates the number of endpoints inherited from child groups.
Policy Inheritance	Indicates if agent policy sets are inherited from the group's parent (`True` or `False`).
Policy Enabled	Indicates if agent policy sets can be assigned to the group (`True` or `False`).
Deployment Enabled	Indicates if deployments can be created for the group (`True` or `False`).
Mandatory Baseline Inheritance	Indicates if Mandatory Baseline settings are inherited from the group's parent (`True` or `False`).
Mandatory Baseline Enabled	Indicates if Mandatory Baseline deployments are created based upon the group's Mandatory Baseline configuration (`True` or `False`).

Email Notification Addresses

After a group is created, it can be assigned an email address. This email is intended to be attributed to the group.

Email addresses are not assigned from the ***Information*** view; this view merely displays the assigned addresses. For additional information on assigning an email address to a group, refer to

The following reference describes the **Email Notification Addresses** table.

Table 77: Email Notification Addresses Table

Column	Description
Notification Address	The email addresses of the group owner.

Child Groups

This section lists the direct Child Groups. Only direct children are listed; deeper descendants such as grandchild groups are not listed.

Tip: This section only lists direct Child Groups; to assign direct Child Groups to a group use the *Group Membership* view.

Table 78: Child Groups Table

Column	Description
Type	The group type (`Custom Group`, `System Group`, or `Directory Service Group`).
Group Name	The name of the child group.
Distinguished Name	The system-created name of the group, which is based upon the group's parent hierarchy.
Description	The description of the group.

Mandatory Baseline Items

Tip: This section only lists group Mandatory Baseline items; to assign items to a group, use the *Mandatory Baseline* view.

Table 79: Mandatory Baseline Items Table

Column	Description
Name	The Mandatory Baseline item name. The name doubles as a link the item's *Review* page.
Content Type	The content type of the Mandatory Baseline item. For a description of each impact, refer to one of the following pages based on the applicable type of Mandatory Baseline item: • Vulnerabilities on page 341 • Software Content on page 342 • Other Content on page 342
Vendor	The name of the vendor that created the software in the Mandatory Baseline item.
State	The state of the Mandatory Baseline item (`Enabled` or `Disabled`).
OS List	The operating systems that the Mandatory Baseline item applies to.

HEAT software

Agent Policy Sets

This section lists the Agent Policy Sets assigned to the selected group, and whether or not that policy set is directly assigned or assigned via inheritance.

Tip: This section only lists group Assigned Policy Sets; to Assign Policy Sets to the selected group use the *Policies* view.

Table 80: Agent Policy Sets Table

Field	Description
Policy Set Name	Indicates the name of the Agent Policy Set.
Assigned	Indicates if the Agent Policy Set is directly assigned to the group or inherited. A value of `True` indicates the Agent Policy Set is directly assigned.

Note: When a group **Policy Enabled** setting is enabled, the group will use the Global System Policy set to define undefined policies. For additional information, refer to Defining Agent Policy Inheritance Rules on page 219.

Resultant Agent Policy Set Information

When a group is assigned two or more Agent Policy Sets, some of the policies may conflict. When conflicts occur, the system applies the agent policy conflict resolution rules to determine which policy to apply. This section lists the resultant policies used when there is Agent Policy Sets conflict.

The following table describes the *Resultant Agent Policy Set Information* information.

Table 81: Resultant Agent Policy Set Information

Field	Description
Name	The name of the agent policy.
Value	The agent policy value. When determining the policy value, directly assigned policies supersede inherited policies. Additionally, directly assigned policies that conflict are resolved by the conflict resolution rules.
Description	The description of the agent policy.

Note: Only agent policies inherited or directly assigned to the group are displayed in **Resultant Agent Policy Set Information**. To see a complete listing of all policies assigned to a managed endpoint, refer to The Information Tab on page 117.

Roles

You can restrict user access to specific groups based on roles. This section lists the user roles that can access the selected group.

Tip: This section only lists the Roles that can access the group; to assign Roles to a group, use the *Roles* view.

Table 82: Roles Table

Field	Description
Role Name	Indicates the name of the user role that can access the group.
Role Source	Indicates the name of the group that the assigned role is inherited from. If the role source contains no value, the role is directly assigned to the selected group.
Assigned	Indicates if the role is inherited or directly assigned to the group. A value of `True` indicates the role is directly assigned to the group.

Exporting Information View Data

To export the information displayed within the *Information* view to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 37.

The Group Membership View

This view lets you view the selected group's direct child groups. If the selected group is a custom group, you can also create new custom child groups that you can populate with the desired endpoints. Custom groups also let you edit or delete any listed preexisting child groups.

This view only lists direct child groups; you cannot manage grandchild groups or further descendants.

The Group Membership View Toolbar

This toolbar contains buttons related to the creation and management of groups.

The following table describes the toolbar functions. Some functions are common to all the *Groups* page views.

Table 83: Group Membership Toolbar

Button	Function
Create	Creates a new group. For additional information, refer to Creating a Group on page 151.

HEAT®software

Button	Function
Delete	Deletes a group. For additional information, refer to Deleting Groups on page 152.
Move...	Assigns a group to a new parent group. For additional information, refer to Moving a Group on page 153.
Deploy...	Deploys content to selected groups. For additional information, refer to Deploying Content to Groups (Group Membership View) on page 155.
Scan Now	Prompts the Discover Applicable Updates task to launch immediately and check a group for vulnerabilities. For additional information, refer to Using Scan Now to Scan Groups on page 156.
Reboot Now...	Initiates the Reboot task for endpoints in the selected group. For additional information, refer to Rebooting Groups on page 156.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Group Membership View List

This list displays the selected group's direct child groups. Each listing contains group identification information and icons used to edit identification information or delete the group altogether.

The following table displays the **Group Membership** view list details.

Table 84: Group Membership View

Column	Icon	Description
Action	N/A	Contains **Edit** and **Delete** icons. Use these icons to edit or delete the associated group.
Groups	🖥	Contains an icon that indicates the type of the group: • `System` (🖥) • `Custom` (🖥) • `Directory Service` (🖥)
Name	N/A	Indicates the name of the child group.

Column	Icon	Description
Description	N/A	Indicates the description of the group.
Distinguished Name	N/A	Indicates the system-created name based upon the group's parent hierarchy.
Endpoints	N/A	Indicates the number of endpoints assigned to the group.

Note: *System* and *Directory Service* groups cannot have their child group or endpoint memberships edited. However, their assigned agent policy sets can be edited.

Creating a Group

HEAT PatchLink DataCenter for Microsoft System Center provides preconfigured groups. However, you can also create custom groups. Populate custom groups with desired endpoints. You can only create custom groups within the **Browser** custom group hierarchy.

Create groups from the *Group Membership* view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. Select the *Custom Group* from the directory tree that you want to create a child group for.
4. Click **Create**.

   Step Result: A new row appears on the page.

5. In the **Name** field, type a name for the group.
6. [Optional] Type a brief description about the group in the **Description** field.
7. Click the **Save** icon associated with the new group.

Result: The group is saved to the list and is added to the directory tree. A *Distinguished Name* is generated for the group.

After Completing This Task:
Add endpoints to the group. For additional information, refer to

Editing Groups

You can edit the names and descriptions for custom groups.

You may edit the name and description for groups within the **Custom Groups** hierarchy. Edit groups from the *Group Membership* view.

Note: For **System Groups** and **Directory Service Groups** only the **Description** field can be edited, not the **Name** field.

HEAT software

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Group Membership**.

3. From the **Group Browser**, select a group within the **Custom Groups** hierarchy you want to edit.

4. Click the **Edit** icon (🖉).

   Step Result: The **Name** and **Description** field displays.

5. [Optional] Edit the **Name** field associated with the group.

6. [Optional] Edit the **Description** field associated with the group.

7. Click the **Save** icon associated with the new group.

Result: The group changes are saved.

> **Note:** Within the *Group Membership* view, you can only edit the group name and description. To edit group behavior, use the *Groups* page views.

Deleting Groups

Delete a group when you no longer need to manage its endpoints collectively. Only custom groups can be deleted. After deleting a group, you cannot recover it; you must recreate the group.

Delete custom groups from the *Groups Membership* view.

> **Note:** Deleting a group does not prevent an endpoint within that group from rebooting, deploying, or scanning; these tasks occur at the endpoint level.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Group Membership**.

3. From the directory tree, select the parent group of the group(s) you want to delete.

> **Note:** Only groups within the **Custom Groups** hierarchy can be deleted.

4. Delete the desired group(s).

   Use one of the following methods.

> **Note:** If the group you want to delete has a child hierarchy, the group cannot be deleted until the child groups have been deleted or moved.

Method	Steps
To delete a single group:	Click the **Delete** icon associated with the group you want to delete.

Method	Steps
To delete multiple groups:	1. Select the check boxes associated with the groups you want to delete. 2. From the toolbar, click **Delete**.

> **Step Result:** A dialog appears asking you to acknowledge the deletion.

5. Click **OK**.

Result: The selected group(s) are deleted.

Moving a Group

After creating a group, you can change its position within the **Browser** tree.

Move groups from the *Group Membership* view on the *Groups* page.

> **Note:** When moving a group, if the group is configured to inherit agent policies, roles, or any other settings, the group inherits those values from its new parent.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. From the **Browser**, select the parent group of the group you want to move.
4. Select the group you want to move.

HEAT software

5. Click **Move**.

> **Note:** You cannot move groups in **System Groups** or **Directory Service Groups**.

Step Result: The *Move Groups* dialog opens.
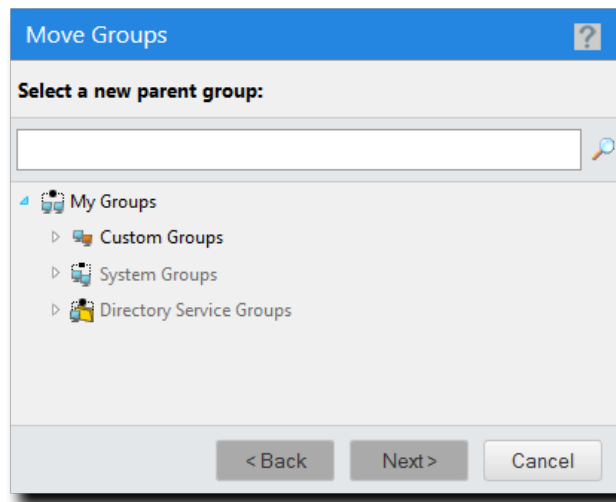
Figure 32: Move Groups Dialogs

6. Select a new parent group.

7. Click **Next**.

Step Result: The group is moved to the new parent group.

> **Note:** If the group you are moving contains a child hierarchy, those groups are moved as well.
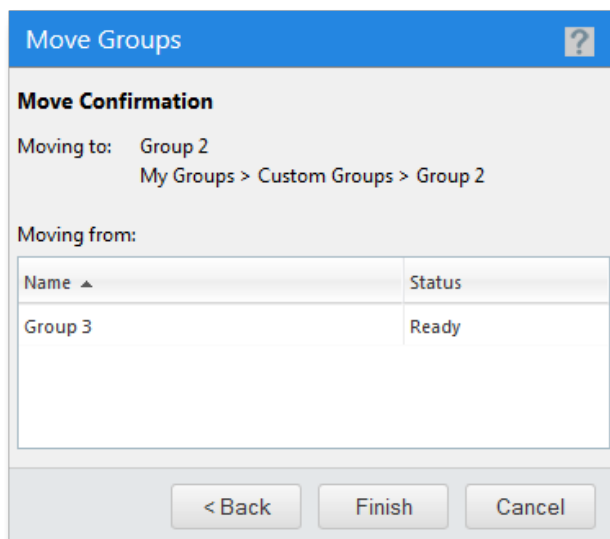
Figure 33: Move Confirmation

8. Click **Finish**.

9. Click **Close**.

Result: The select group is moved to its new place in the group hierarchy.

Deploying Content to Groups (Group Membership View)

Within HEAT PatchLink DataCenter for Microsoft System Center, content can be deployed from a number of pages, including the *Groups* page *Group Membership* view. When deploying from this view, the *Deployment Wizard* is preconfigured to deploy to the selected group.

For additional information, refer to About Deployments on page 289.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Group Membership**.

3. From the directory tree, select the group you want to deploy content to.

HEAT software

4. Click **Deploy**.

Result: The *Deployment Wizard* opens, preconfigured to deploy to the selected group.

After Completing This Task:
Review and complete subsequent tasks.

Using Scan Now to Scan Groups

You can initiate a Discover Applicable Updates (DAU) task for all endpoints in a selected group. When you initiate this task, the agent scans its host endpoint for vulnerabilities and inventory. Scan results are then uploaded to HEAT PatchLink DataCenter for Microsoft System Center, which you can view.

You can launch a DAU task for managed endpoints in a selected group. Perform this task from the *Groups* page *Group Membership* view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Group Membership**.

3. From the directory tree, select the group you want to scan.

4. Click **Scan Now** > **Discover Applicable Updates**.

   Step Result: The *Scan Now* dialog opens.

5. Select the **Yes, scan all members of the selected group**.

6. [Optional] Select the **Include child groups in the scan**.

7. Click **Schedule**.

8. Acknowledge the scheduling by clicking **Close**.

Result: The scan is scheduled. As with all deployments, although the Discovery Applicable Updates task is scheduled for immediate execution, it will not actually occur until the next time the agent checks in.

Rebooting Groups

Within HEAT PatchLink DataCenter for Microsoft System Center, you can reboot all endpoints within a given group.

Reboot entire groups from the *Group Membership* view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Group Membership**.

3. From the directory tree, select the group you want to reboot.

4. Click **Reboot Now**.

   Step Result: The *Reboot Now* dialog opens.

5. Select the **Yes, reboot all members of the selected group** check box.

6. [Optional] Select the **Reboot child groups** check box.

7. Click **Reboot**.

8. Acknowledge the reboot scheduling by clicking **Close**.

Result: The reboot is scheduled. As with all deployments, although the reboot is schedule for immediate execution, it will not actually occur until the next time the agent checks in.

Exporting Group Membership View Data

To export information displayed in the *Group Membership* view list to a comma separated value (.csv) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 37.

The Endpoint Membership View

This view lists the endpoints that hold membership in the selected group. If the group selected is a custom group, you can also use this view to add endpoints. Use this view to manage endpoints assigned to the selected group. This view contains features similar to those available from the *Endpoints* page.

The Endpoints View Toolbar (Groups Page)

The *Endpoints View* toolbar contains the tasks and functions that are available for you to perform for managed endpoints with HEAT PatchLink DataCenter features enabled.

The following table describes the toolbar functions used in the *HEAT PatchLink DataCenter* tab on the *Groups* page *Endpoint Membership* view.

Table 85: Endpoints View Toolbar (Groups Page)

Button	Description
Membership	Launches the *Membership Wizard*, which allows you to add endpoints to the group. For additional information, refer to Adding Endpoints to a Group on page 160.
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting Endpoints (Groups Page) on page 163.
Enable	Enables a disabled endpoint. For additional information, refer to Enabling the HEAT PatchLink DataCenter Agent for Linux/UNIX on page 114.
Disable	Disables an enabled endpoint. For additional information, refer to Disabling the HEAT PatchLink DataCenter Agent for Linux/UNIX on page 114.

HEAT software

Button	Description
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Endpoints View List (Groups Page)

The **Endpoints View** tab list itemizes endpoint identification data, server connectivity, operating system, and agent information.

The following table describes the columns within the **Endpoints View** tab on the **Groups** page **Endpoint Membership** view.

Name	The name of the endpoint. Clicking the **Name** link displays the applicable **Endpoint Details** page. See The Endpoint Details Page on page 116 for additional information.
IP Address	The IP address of the endpoint.

Agent Status	Indicates the status of the endpoint. The following list defines column values:
	Online — The agent is able to communicate with the HEAT PatchLink DataCenter server in the predefined time period. Refer to [Configuring the Agents Tab](#) on page 65 for additional information on configuring agent default behavior.
	Offline — The agent is unable to communicate with the HEAT PatchLink DataCenter server in the predefined time period. In an `Offline` status, the agent still enforces all policies.
	Note: A **Warning** (⚠) icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is either offline or has an update required status. Click the icon to find out

Operating System	The operating system the endpoint is running.
Module **Installed**	Indicates whether a module is installed on the endpoint. A new *Module* **Installed** column is added for each module installed on your HEAT Patch Manager DataCenter Server. The following list defines column entry values:

	Yes	The module is installed.
	No	The module is not installed.
	Pending Install	The module is in the process of installing.
	Pending Uninstall	The module is in the process of uninstalling.
	Error	There was an error while installing or uninstalling the module. Click the for additional information about the error.
	Expired	The module license has expired.

Adding Endpoints to a Group

You can manage endpoints collectively by adding them to custom groups.

Add endpoints to a group from the *Groups* page.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **Groups** tree, right-click a group in the **Custom Groups** hierarchy and select **Add Endpoints to Group**.

Remember: Endpoints can only be added to custom groups.

Step Result: The *Membership* dialog opens.
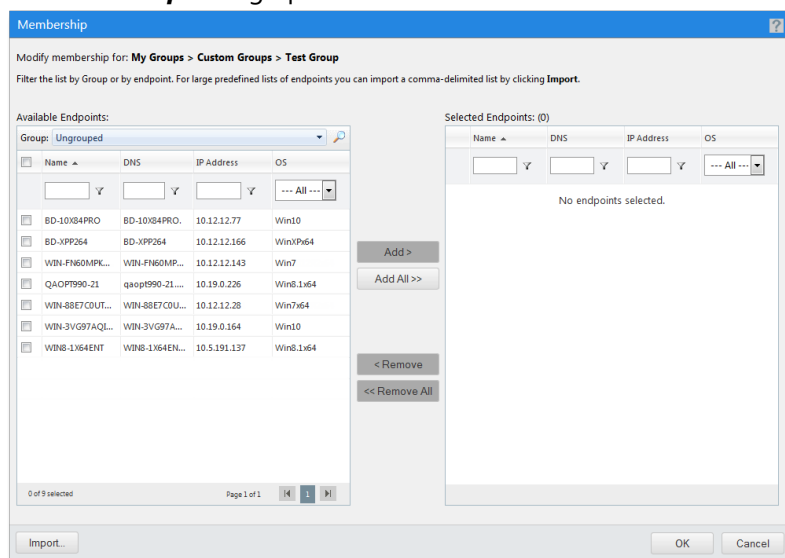
Figure 34: Membership Dialog

3. Add endpoints to the group.

a) [Optional] To filter the endpoints that are listed down to a pre-existing group, select a **Group** from the drop-down list and click 🔍.

b) [Optional] To filter the endpoints that are listed, type filter criteria in the table fields and click ▽ to select an operator.

c) Select endpoints and click **Add**.

> **Tip:**
> - Click **Add All** to include the entire list.
> - You can add endpoints to the group by importing them from a list. Click **Import** to use this feature.
> - Use the **Remove** and **Remove All** buttons to remove endpoints from the list.

d) Review the list of endpoints to confirm it is correct.

4. Click **OK**.

Result: The selected endpoints are added to the group. Select **Endpoint Membership** from the **View** list to confirm they are added.

HEAT software

Importing Endpoints into Groups

If you are adding a large number of endpoints to a group, importing a list of endpoints can be faster than than selecting them individually within the ***Membership*** dialog.

Import Rules

- You can only import endpoints using their host names. IP Addresses cannot be imported.
- You must separate each endpoint with a comma.
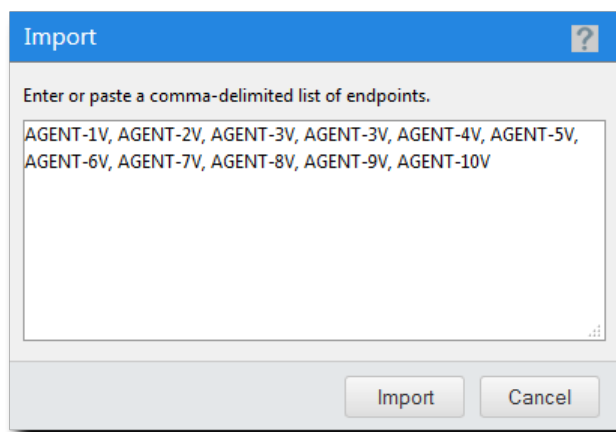
Figure 35: Import List Example

Tip: You can use HPL to easily obtain a list of endpoints to import. To create a list:

1. Open the ***Endpoints*** page.
2. Using the page filters to display the endpoints you want to add to your group.
3. Click **Export**.
4. Open the exported .csv file and copy and paste the endpoint names into the **Import** dialog. Add a comma between each name.

Downloading the Agent Installer

You can install an agent on a local endpoint from the ***Endpoint Membership*** view.

For additional information, refer to

Deleting Endpoints (Groups Page)

From the *Groups* page, you can delete an endpoint from the HEAT PatchLink DataCenter for Microsoft System Center database.

Prerequisites:

The endpoints you want to delete must be disabled. For additional information, refer to Enabling or Disabling HEAT PatchLink DataCenter Agent for Linux/UNIXs within a Group on page 163.

Delete endpoints from the *Endpoint Membership* view.

Note: Deleting an endpoint removes its record from the HEAT PatchLink DataCenter for Microsoft System Center database, but it does not remove the agent on the endpoint.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Endpoint Membership**.

3. Select a group from the directory tree.

    Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy that is disabled.

4. Select the endpoint listings you want to delete.

    Tip: You can delete endpoints from any module tab.

5. Click **Delete**.

    Step Result: A confirmation dialog opens.

6. Click **OK** to confirm the deletion.

Result: The selected endpoints are deleted.

Enabling or Disabling HEAT PatchLink DataCenter Agent for Linux/UNIXs within a Group

Disabling an agent deactivates its functionality. Disabled agents do not contact the HPL server, use HPL features, or occupy HPL licenses. Disable an agent if it will be unused for a prolonged period. You can re-enable an agent at any time.

Enable or disbale an agent within a group from the *Endpoint Membership* view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Endpoint Membership**.

3. From the **Browser**, select a group within either the **Custom Groups** or **Systems Groups** hierarchy.

4. If necessary, define filter criteria and click **Update View**.

HEAT®software

5. Select the endpoints on which you want to enable or disable the agent:

Use one of the following methods.

Method	Steps
To enable a disabled endpoint:	Click **Enable**.
To disable an enabled endpoint:	**1.** Click **Disable**. **2.** Acknowledge the disablement by clicking **OK**.

Result: The applicable agents are enabled or disabled. The ***Endpoint Membership*** view and ***Endpoints*** page reflect your changes.

> **Note:** Disabling an agent within a group is not limited to the group; the agent is completely disabled within the HPL.

Exporting Endpoint Membership View Data

To export information displayed in the ***Endpoint Membership*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 37.

The Mandatory Baseline View

This view lets you add content to the selected group's Mandatory Baseline. It also lists each content item included in the group's Mandatory Baseline. The list also shows whether or not each endpoint within the group has that content item installed.

Use this view to define the selected group's Mandatory Baseline.

About Mandatory Baselines

A *Mandatory Baseline* is a minimum set of content that *must* be installed on a group's endpoints. Composed of user-defined content items deemed essential to the group, this baseline continually verifies that the applicable items are installed on group endpoints. If a group endpoint is found in a *non-compliant* state (does not have an item defined in the baseline installed), HEAT PatchLink DataCenter for Microsoft System Center automatically deploys the applicable content until the endpoint is once again compliant. Mandatory Baselines ensure group endpoints are never without essential security content.

For example, you can set a Mandatory Baseline for all endpoints within a group that must have Microsoft Windows Messenger installed. If Messenger is deleted on a group member's endpoint, HEAT PatchLink DataCenter for Microsoft System Center reinstalls Messenger.

Remember the following rules when working with Mandatory Baselines:

- Mandatory Baseline inheritance indicates that a group's endpoints (both inherited and assigned) are included by the parent group when evaluating its own baseline items and inheritance.
- If endpoints receive a Mandatory Baseline item via inheritance, the Mandatory Baseline item will also be displayed on the child group's ***Mandatory Baseline*** view. However, the inherited baseline items will be unavailable, indicating the Mandatory Baseline originates from a parent group.
- Disabling Mandatory Baseline deployments only applies to the Mandatory Baseline items that are directly assigned to the group, and will prevent those directly assigned items from being inherited by the group's child hierarchy.
- Disabling Mandatory Baseline deployments does not disable the deployments created through Mandatory Baseline inheritance. Additionally, disabling the baseline deployments will not remove the baseline items from the group's ***Mandatory Baseline*** view.

Note: Unless stringent hours of operation agent policies are in effect, do not apply Mandatory Baselines to groups of mission-critical servers or other endpoints where unscheduled reboots would disrupt daily operations.

About Mandatory Baseline Import/Export

Within HEAT PatchLink DataCenter for Microsoft System Center, you can import or export Mandatory Baselines. Importing and Exporting Mandatory Baselines simplifies application of Baselines to different groups.

After establishing a Mandatory Baseline, you can export the baseline from HEAT PatchLink DataCenter for Microsoft System Center. After exporting a baseline, you can then import the baseline to a different group or HEAT PatchLink DataCenter for Microsoft System Center installation.

HEAT recommends using the Mandatory Baseline import/export feature in the following situations:

- When reinstalling HEAT PatchLink DataCenter for Microsoft System Center. Export Mandatory Baselines before beginning reinstallation, and then import Mandatory Baselines to groups after installation. This use of import/export eliminates the manual reestablishment of baselines, easing administrative burden.
- When establishing similar or identical Mandatory Baselines for multiple groups. Rather than manually creating baselines for each group, export a Mandatory Baseline and then import it to other groups. Use this method to quickly establish baselines for multiple groups. After importing a baseline, you can then edit it to suit a group's particular requirements.

The Mandatory Baseline Process

After content items are added to a group's Mandatory Baseline, HEAT PatchLink DataCenter for Microsoft System Center schedules a series of scans and deployments until the group complies with the baseline.

The following chart depicts the Mandatory Baseline process following the addition of a content item to a baseline.

HEAT®software
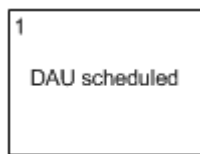
HEAT PatchLink DataCenter for Microsoft System Center automatically schedules a Discover Applicable Updates (DAU) task for all endpoints within the applicable group.
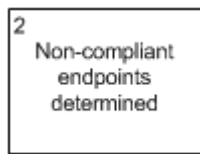
Following the DAU, HEAT PatchLink DataCenter for Microsoft System Center determines which endpoints are not compliant with the Mandatory Baseline.
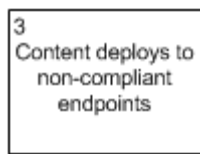
Necessary content is deployed to non-compliant endpoints as soon as possible.

Note: Some content requires both reboots and an administrator-level log in to complete. If these or similar content items are added to a baseline, the deployment will stop until the log in occurs.

Viewing a Group Mandatory Baseline

Navigate to a group's Mandatory Baseline to see the content items that all its members must have installed.

See the Mandatory Baseline for a selected group from the *Mandatory Baseline* view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. Select the desired group from the directory tree.

3. From the **View** list, select **Mandatory Baseline**.

Result: The Mandatory Baseline associated with the group is displayed.

The Mandatory Baseline View Toolbar

This toolbar contains buttons related to the management of Mandatory Baselines. It also contains a button that lets you cache content items after adding them to the baseline. This caching process ensures swift content installations if an endpoint falls out of compliance.

The following table lists the available toolbar buttons and their functions.

Table 86: Mandatory Baseline View Toolbar

Button	Function
Manage	Adds or removes content to or from the group's Mandatory Baseline. For additional information, refer to either Adding Content to Mandatory Baselines on page 170 or Removing Content from Mandatory Baselines on page 174.
Update Cache	Caches (downloads) the package associated with the selected Mandatory Baseline item(s) (or the scripts associated with downloading the package). For additional information, refer to Updating the Mandatory Baseline Cache on page 180.
Import	Imports an Mandatory Baseline template into the group, defining Mandatory Baseline item. For additional information, refer to Importing Mandatory Baseline Templates on page 180.
Export (menu)	Opens the **Export** menu.
CSV file (**Export** menu item)	Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
Template (*.XML) (**Export** menu item)	Exports the group Mandatory Baseline as a template in `.xml` format. For additional information, refer to Exporting Mandatory Baselines Templates on page 184.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

HEAT software

The Mandatory Baseline View List

This list displays the content items included in the selected group's Mandatory Baseline. You can also filter this list to display different types of content.

The following table describes the **Mandatory Baseline** view list.

Table 87: Mandatory Baseline View List

Column	Icon	Description
Item Type	📄	An icon that indicates the Mandatory Baseline item status and type. For a description of each Mandatory Baseline item icon, refer to Content Status and Type on page 349.
Mandatory Baseline Compliance	M	An icon that indicates compliance status for the item. For a description of each compliance icon, refer to Mandatory Baseline Item Compliance Icons on page 169.
		Note: If the Mandatory Baseline fails to deploy more than twice, it will be recorded as an error in the **Status** column. However, this notification will only show in the **Mandatory Baseline** view.
Mandatory Baseline Item	N/A	The Mandatory Baseline item name. The name doubles as a link the item's **Review** page.
Content Type	N/A	The content type of the Mandatory Baseline item. For a description of each impact, refer to one of the following pages based on the applicable type of Mandatory Baseline item: - Vulnerabilities on page 341 - Software Content on page 342 - Other Content on page 342
Vendor	N/A	The name of the vendor that created the software in the Mandatory Baseline item.
State	N/A	The state of the Mandatory Baseline item (`Enabled` or `Disabled`).
OS List	N/A	The operating systems that the Mandatory Baseline item applies to.

Note: The **Mandatory Baseline Item**, **Content Type**, **Vendor**, **State**, and **OS List** are identical to the content items that the Mandatory Baseline items represent.

Each item on the **Mandatory Baseline** view list can be expanded to display additional details about the item. This information lists each endpoint in the group, and whether or not these endpoints comply with the expanded Mandatory Baseline item. Click the arrow (**>**) next to a Mandatory Baseline item to view these details.

The following table describes each column within the details of a Mandatory Baseline item.

Table 88: Package Column Definitions

Column	Icon	Description
Endpoint Status Icon	🖥	Displays an icon that indicates the current status of the applicable endpoint. For additional information, refer to Agent Module Status Icons on page 110.
Mandatory Baseline Icon	Ⓜ	Displays an icon that indicates the status of the endpoint in relation to the expanded Mandatory Baseline item. For additional information, refer to Mandatory Baseline Item Compliance Icons on page 169.
Name	N/A	Indicates the name of the endpoint within the selected group.
OS	N/A	Indicates the operating system that runs on the endpoint.
Compliance	N/A	Indicates whether the endpoint complies with the expanded Mandatory Baseline item. If the item is marked *Do Not Patch* for the endpoint, the endpoint is considered compliant.

Mandatory Baseline Item Compliance Icons

Each item on the **Mandatory Baseline** view list contains an icon that indicates if all applicable endpoints within the group have the associated content installed. Familiarizing yourself with these icons will help you understand if the selected group currently complies with its Mandatory Baseline. Additionally, after expanding a Mandatory Baseline items, compliance icons also appear for each endpoint.

The following table describes the compliance icons for Mandatory Baseline items.

Table 89: Mandatory Baseline Item Compliance Icons

Icon	Status
🔵	Indicates one or more group members are either detecting, obtaining the package, awaiting detection, or is in a deployment-not-started state.
🟢	Indicates one or more group members are deploying the package.
⬜	Indicates all group members are disabled.
🟢	Indicates all group members are either not applicable or in compliance with this package (some can also be disabled).
🔴	Indicates one or more group members are not compliant and had an error during deployment. Error information displays in the mouseover text.

HEAT®software

Icon	Status
🗑	Indicates that the patch is marked *Do Not Patch* for the group.
	Note: • If a group marked *Do Not Patch* for a content item is later marked *OK to Patch*, the Mandatory Baseline automatically installs the content on that group. • If a group has content added to its Mandatory Baseline that is later marked *Do Not Patch*, that content *is not* automatically uninstalled.

The following table describes the compliance icons for endpoints (which appear when a Mandatory Baseline item is expanded).

Table 90: Endpoint Compliance Icons

Icon	Status
🖥	Indicates the group member is either detecting, obtaining the package, awaiting detection, or is in a deployment-not-started state.
🖥	Indicates the group member is receiving the package.
🖥	Indicates the Mandatory Baseline item does not apply to the group member.
🖥	Indicates the group member complies with the Mandatory Baseline item.
🖥	Indicates the group member does not comply with the Mandatory Baseline item.
🖥	Indicates that group member is marked *Do Not Patch* for the Mandatory Baseline item.
	Note: • If an endpoint marked *Do Not Patch* for a content item is later marked *OK to Patch*, the Mandatory Baseline automatically installs the content on that endpoint. • If an group endpoint has content added to its Mandatory Baseline that is later marked *Do Not Patch*, that content *is not* automatically uninstalled.

Adding Content to Mandatory Baselines

Add content to a group Mandatory Baseline to monitor the endpoints for installation of the content. If an endpoint does not have it installed, HPL installs it following the next Discover Applicable Updates task.

Add content to a Mandatory Baseline from the ***Mandatory Baseline*** view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Mandatory Baseline**.

3. From the **Group Browser**, select the desired group.

4. Click **Manage**.

5. [Optional] Filter the **Vulnerabilities** table. There are two ways to filter:

- Click the **Show/Hide Filters** link to toggle the built-in table filters.
- Click the **Filter** button at the bottom of the table to open the *Needed Detection Vulnerabilities* dialog, which only shows content applicable to the group that hasn't been installed (content that's not applicable or marked *Do Not Patch* for the group aren't displayed).
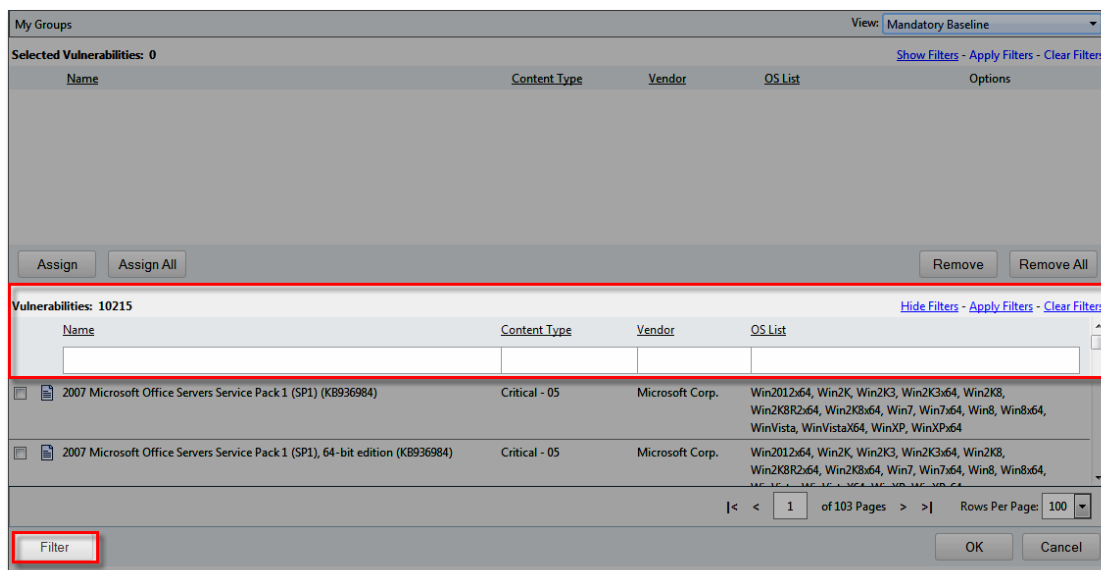
6. Select the content you want to add to the baseline and click the **Assign** button.

> **Note:**
> - Don't use the **Assign All** button until you've filtered the **Vulnerabilities** table. Adding all the available content creates excessive network traffic.
> - Don't add locally created packages to the baseline. They don't contain the fingerprint files that the baseline requires to monitor for packages.

Step Result: Your content is added to the **Selected Vulnerabilities** table.

7. Click **OK**.

8. If vendor license agreements are displayed, select the **I ACCEPT the terms and conditions of this end user license agreement** option and click **OK**.

/HEAT software

9. [Recommended] Click the **Update Cache** button to download the content.

> **Note:** Skipping the cache update may result in endpoint reboots that interrupt employee work. Cache the content now to optimize package installation order. While caching, click **Refresh** to check for progress.
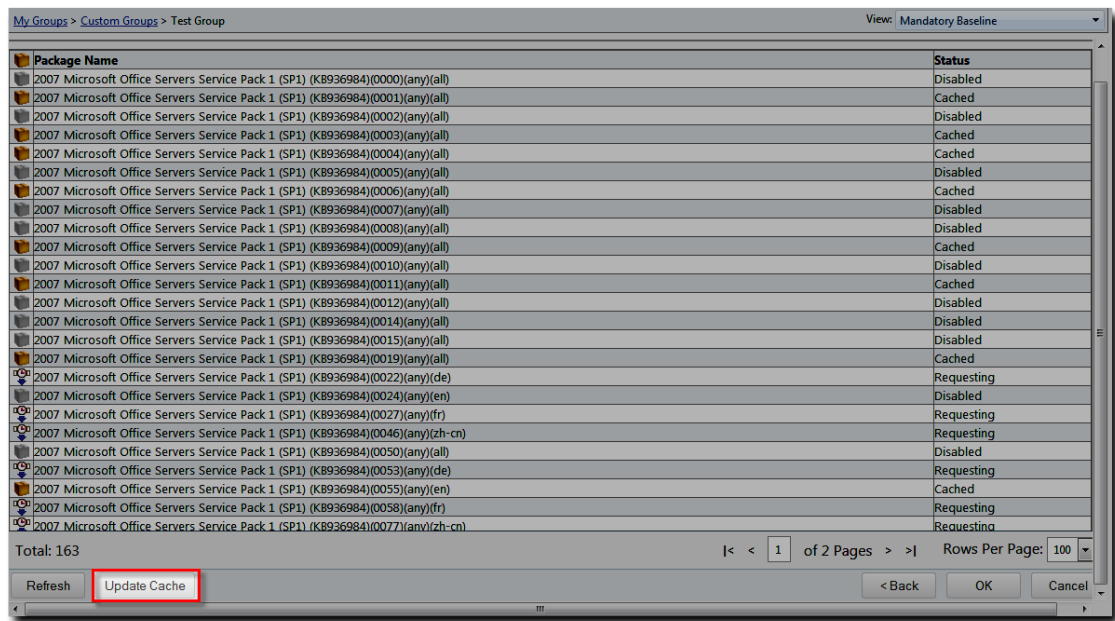
10. [Optional] From the **Select Vulnerabilities** table, click the **Option** button to set deployment options for a content item.

    You can do this for each content item added to the baseline.
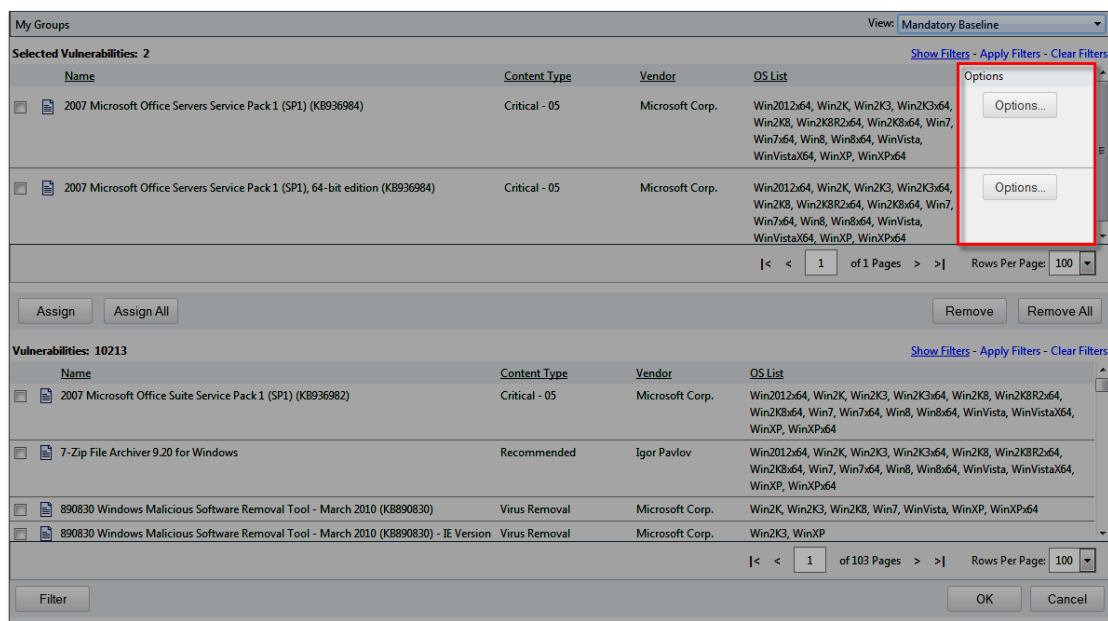
11. Click **OK**.

Result: The content is added to the group Mandatory Baseline.

> **Note:** To deploy Mandatory Baseline items, the group **Mandatory Baselines enabled** setting must be set to `True`. For additional information, refer to Editing Group Settings on page 212.

Filtering the Vulnerabilities Table for Applicable Content
When adding content to a Mandatory Baseline, click the filter button to open the *Needed Detection Vulnerabilities* dialog. This dialog filters the default the Vulnerabilities table to show only content that applies to the group that hasn't been installed yet.

Prerequisites:

Start Adding Content to Mandatory Baselines on page 170 and complete up to step 5.

HEAT software

1. Click the **Filter** button.

   Step Result: The *Needed Detection Vulnerabilities* dialog opens.
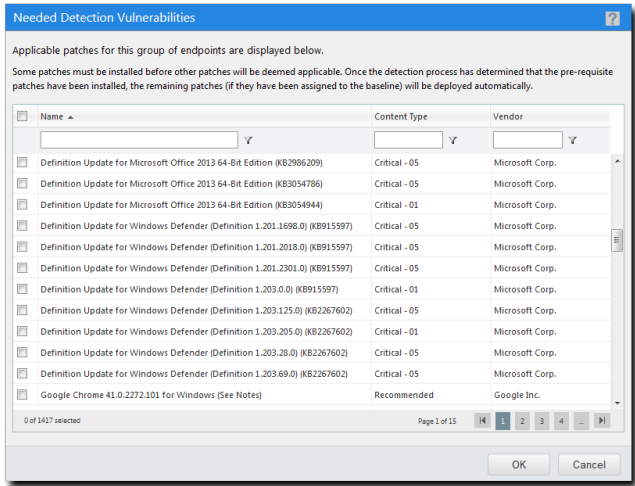
Figure 36: Needed Detection Vulnerabilities Dialog

2. [Optional] Use the column filters to narrow down content.

   Only applicable content is listed. Content that is not applicable or marked *Do Not Patch* for the group isn't displayed.

3. Select the content items you want to add to the Mandatory Baseline and then click **OK**.

Result: The *Needed Detection Vulnerabilities* dialog closes and the selected content items are added to the **Selected Vulnerabilities** table.

Removing Content from Mandatory Baselines

When a group of endpoints no longer requires the constant presence of specific content, remove the applicable content items from that group's Mandatory Baseline. Removing content from a Mandatory Baseline does not remove it from the group's endpoints.

Remove content from Mandatory Baselines from the *Mandatory Baseline* view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Mandatory Baseline**.

3. From the directory tree, select the desired group.

4. Click **Manage**.

5. Remove content from the Mandatory Baseline.

Use one of the following methods.

Method	Steps
To remove individual content items:	1. From the **Selected Vulnerabilities** table, select the check boxes associated with the content items you want to remove from the Mandatory Baseline. 2. Click **Remove**.
To remove all content items:	Click **Remove All**.

Step Result: Content items are removed from the **Selected Vulnerabilities** table according to your input.

6. Click **OK**.

Result: The selected content is removed from the selected group's Mandatory Baseline. The ***Groups*** page reflects your changes.

Setting Mandatory Baseline Deployment Options

Like other deployments, automated Mandatory Baseline deployments also have customizable options. After adding content items to a group's Mandatory Baseline, you can set deployment options for each item. Configuring these options defines the manner in which Mandatory Baseline packages are deployed.

Prerequisites:

• A content item must be added to a group Mandatory Baseline.

Configure Mandatory Baseline package deployment options from the ***Mandatory Baseline*** view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. Select the desired group from the directory tree.

3. From the **View** list, select **Mandatory Baseline**.

4. Click **Manage**.

◢**HEAT**®software

5. Click the **Options** button associated with the Mandatory Baseline item for which you want to define deployment options.

Step Result: The *Package Deployment Options* dialog opens.
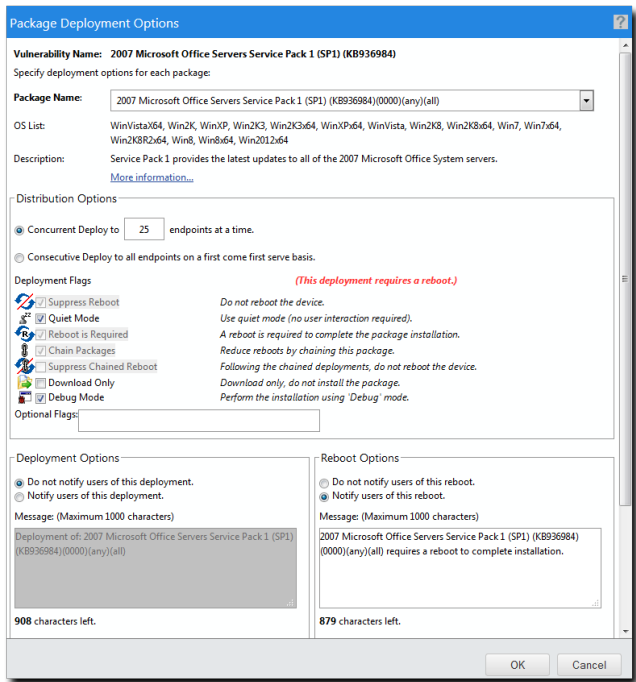
Figure 37: Package Deployment Options Dialog

6. From the **Package Name** list, ensure the desired package is selected.

7. Define **Distribution Options**.

Choose from the following options.

Option	Steps
To deploy concurrently:	**1.** Select the **Concurrent** option. **2.** In the field, type the desired number of endpoints to receive simultaneous deployments.
To deploy consecutively:	Select the **Consecutive** option.

8. If available, select the desired **Deployment Flags**.

For additional information, refer to Behavior Icon Definitions on page 323.

9. If needed, type additional deployment flags in the **Optional Flags** field.

For additional information, refer to Package Flag Descriptions on page 325.

10. Select a **Deployment Option**.

  - **Do not notify users of this reboot**.
  - **Notify users of this reboot**.

11. If you selected **Notify users of this deployment** option, complete the following substeps.

  a) [Optional] Type a notification in the **Message** field.
  b) Select whether you want to manually define remaining notification options or use the default settings defined in the Global Policy Set.

  - To manually define remaining notification options, ensure the **Use Policies** check box is cleared and continue to the next substep.
  - To use the default notification option settings defined in the agent policy set associated with the target endpoints, select the **Use Policies** check box and continue to the next step.

  c) Define the **Allow user to cancel** option.

  - To manually define this option, select *yes* or *no* from the **Setting** list.
  - To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

  d) Define the **Allow use to snooze** option.

  - To manually define this option, select *yes* or *no* from the **Setting** list.
  - To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

  e) Define the **Notification on top** option.

  - To manually define this option, select *yes* or *no* from the **Setting** list.
  - To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

    For additional information about this option, refer to

  f) Define the **Deploy within** option.

  - To manually define this option, type a value in the field and select a value from the list (*minutes*, *hours*, *days*).
  - To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

12. Select a **Reboot Option**.

  - **Do not notify users of this reboot**.
  - **Notify users of this reboot**.

13. If you selected **Notify users of this reboot** option, complete the following substeps.

  a) [Optional] Type a notification in the **Message** field.

HEAT software

b) Select whether you want to manually define remaining notification options or use the default settings defined in the agent policy set associated with the target endpoints.

- To manually define remaining notification options, ensure the **Use Policies** check box is cleared and continue to the next substep.
- To use the default notification option setting defined in the agent policy set that applies to the target endpoints, select the **Use Policies** check box and continue to the next step.

c) Define the **Allow user to cancel** option.

- To manually define this option, select **yes** or **no** from the **Setting** list.
- To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

d) Define the **Allow use to snooze** option.

- To manually define this option, select **yes** or **no** from the **Setting** list.
- To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

e) Define the **Notification on top** option.

- To manually define this option, select **yes** or **no** from the **Setting** list.
- To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

  For additional information about this option, refer to

f) Define the **Reboot within** option.

- To manually define this option, define the field and list (**minutes**, **hours**, **days**).
- To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

Result: The **Package Deployment Options** dialog closes. Repeat these instructions for additional Mandatory Baseline items if necessary.

Removing Deployments Created by Mandatory Baselines

Occasionally, deployments associated with a Mandatory Baseline may need to be stopped. However, how you stop the deployment will change based on context; in some instances, you may want to stop the deployment for all endpoints within the group; in others, you may only want to stop the deployment for specific endpoints within the group.

Mandatory Baseline deployments can be stopped one of two ways: either stop the deployment itself or disable the endpoints receiving the deployment.

The removal of Mandatory Baseline deployments does not take place within the **Mandatory Baselines** view. Rather, it takes place within the **Deployments and Tasks** view.

Note: If the Mandatory Baseline still applies, the deployment will be recreated.

Removing a Mandatory Baseline Deployment from a Group
In the event that a Mandatory Baseline deployment needs to be removed for all endpoints within a group, delete the deployment itself. Using this method prevents packages associated with the baseline from being installed on all endpoints within the group.

Stop Mandatory Baseline deployments using this method from the ***Deployments and Tasks*** view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Deployments and Tasks**.

3. Select the applicable group from the directory tree.

4. Select the check box associated with the Mandatory Baseline deployment you want to delete.

5. Click **Delete**.

   Step Result: A dialog displays, asking you to acknowledge the deletion.

6. Click **OK** to acknowledge the deletion.

   Note: If the Mandatory Baseline(s) still applies, the deployment(s) is recreated.

Result: The Mandatory Baseline deployment is stopped. It no longer appears in the ***Deployments and Tasks*** view.

Stopping a Deployment for Specific Endpoints
In the event that a Mandatory Baseline deployment needs to be stopped for specific endpoints within a group, disable those endpoints. Using this method prevents packages associated with the baseline from being installed on specific endpoints within the group rather than all endpoints within the group.

Stop Mandatory Baseline deployments using this method from the ***Deployments and Tasks*** view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Deployments and Tasks**.

3. Select a group from the directory tree.

4. Click the desired deployment name link.

5. Select the check box(es) associated with the desired endpoint(s).

6. Click **Disable** to disable the deployment(s) for the selected endpoint(s).

   Note: If the Mandatory Baseline still applies, the deployment is recreated.

Result: The selected endpoints are disabled, preventing them from receiving the Mandatory Baseline deployment. Remember to re-enable the endpoints to resume vulnerability management activities following management of the Mandatory Baseline.

HEAT®software

Updating the Mandatory Baseline Cache

You can cache content that you have included in a group's Mandatory Baseline. Updating the cache for content items downloads the packages (or the scripts that will download the packages) associated with those items. Cached content items can be deployed immediately.

Cache content for Mandatory Baseline items from the *Mandatory Baseline* view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the *View* list, select **Mandatory Baseline**.

3. From the directory tree, select the group with Mandatory Baseline items (content items) that you want to cache.

4. If necessary, designate filter criteria for the desired Mandatory Baseline item and click **Update View**.

5. Select the check boxes associated with the Mandatory Baseline item you want to cache.

6. Click **Update Cache**.

Result: The selected content begins caching.

Importing Mandatory Baseline Templates

After a Mandatory Baseline template has been exported, import the template and apply it to a new group. Importing a Mandatory Baseline template is faster than creating a new, identical Mandatory Baseline.

Import Mandatory Baseline templates from the *Mandatory Baseline* view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Mandatory Baseline**.

3. From the directory tree, expand to the group with which you want to import a Mandatory Baseline template.

4. From the toolbar, click **Import**.

    Step Result: The *Import Mandatory Baseline Wizard* opens to the *Welcome to the Import Mandatory Baseline Wizard* page.

Welcome to the Mandatory Baseline Import Wizard

This wizard will help you import a Mandatory Baseline template file. Once imported, the Mandatory Baseline will automatically be enforced and create the necessary deployments for the group.

☐ Do not display this page in the future

[Next >] [Cancel]
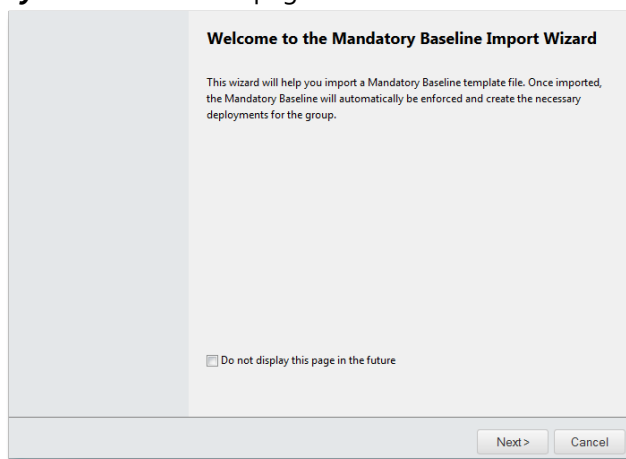
Figure 38: Welcome Page

5. Click **Next**.

    Step Result: The *Import Mandatory Baseline* page opens.

6. Define the Mandatory Baseline template that you want to import.

    a) Click **Browse**.

        Step Result: The *Choose file* dialog opens.

    b) Browse to the Mandatory Baseline template you want to import.

    c) Click **Open**.

    Step Result: The Mandatory Baseline template name displays in the **Mandatory Baseline template (*.XML)** field.

7. If you do not want to import the deployment options associated with the Mandatory Baseline and use the system defaults defined on your HEAT PatchLink DataCenter Server for Microsoft System Center server, select the **Import without deployment options and use system default** check box.

8. Click **Next**.

HEAT software

9. Based upon the page or dialog that opens, complete the applicable steps.

Page/Dialog	Steps
If the *This group already has Mandatory Baseline items assigned* dialog opens:	1. Select either the **Append to the list of existing items and replace duplicates** option or the **Replace all existing items with new items** 2. Click **OK**.
If the *One or more of the Mandatory Baseline items are not available because they are not included in the server's content subscription* dialog displays:	Click **OK** to proceed with the import or **Cancel** to cancel the import.
If the *Review Mandatory Baseline Items* page opens:	Proceed to the next step.

10. Review the Mandatory Baseline items and edit them as needed.
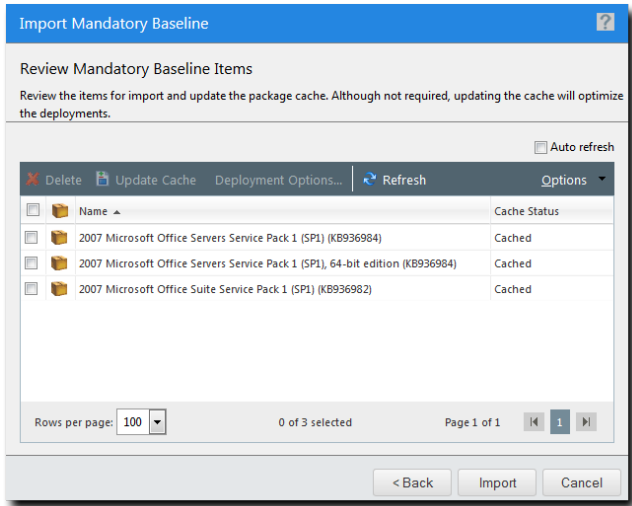
Figure 39: Review Mandatory Baseline Items Page

The following table describes each page column.

Column	Description
Mandatory Baseline Icon	Displays an icon that indicates the cache status of the Mandatory Baseline item. For additional information, refer to Content Icons and Descriptions on page 350.

Column	Description
Name	Lists the name of the Mandatory Baseline item. The Mandatory Baseline item name is identical to the content item.
Cache Status	The cache status of the Mandatory Baseline item. The cache status indicates whether the content item has been downloaded to your HEAT PatchLink DataCenter Server for Microsoft System Center server (`Cached` or `Not Cached`).

11. [Optional] Edit the list.

Edit the list according to the following task steps.

Task	Steps
To delete items:	**1.** Select the check box(es) associated with the applicable Mandatory Baseline item(s). **2.** Click **Delete**.
To update the cache for items:	**Important:** Updating the cache for Mandatory Baseline items ensures they are deployed in the proper chain sequence. Failure to cache Mandatory Baseline items may result in multiple deployment recipient endpoint reboots. **1.** Select the check box(es) associated with the applicable Mandatory Baseline item(s). **2.** Click **Update Cache**.
To configure deployment options for an item:	**1.** Select the check box associated with the applicable Mandatory Baseline item. **2.** Click **Deployment Options**. **3.** Complete Setting Mandatory Baseline Deployment Options on page 175 from step 6.
To refresh item cache statuses:	Click **Refresh**. **Tip:** If the **Auto Refresh** check box is selected, Mandatory Baseline item cache statuses will periodically refresh automatically.

12. Click **Next**.

Step Result: The *License Agreement* page opens.

HEAT software

13. Review the license agreement for each mandatory basline item and select **I ACCEPT the terms and condition of the end user license agreement** option.

Scrolling may be necessary to review and accept all license agreements.

14. Click **Finish**.

Step Result: The import process begins. A bar indicates progress.

15. Click **Close**

Result: The Mandatory Baseline is imported to the selected group. List items for applicable Mandatory Baseline items appear within the *Mandatory Baseline* view. All endpoints within the group are now subject to the Mandatory Baseline.

Exporting Mandatory Baselines Templates

You can export Mandatory Baseline templates in an XML format. This feature is useful for setting up Mandatory Baselines across multiple groups and HEAT PatchLink DataCenter for Microsoft System Centers via importation.

Export Mandatory Baselines templates from the *Mandatory Baseline* view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Mandatory Baseline**.

   Step Result: The *Mandatory Baseline* view displays.

3. From the directory tree, select the group assigned the Mandatory Baseline you want to export.
   Expand the tree as necessary.

4. From the toolbar, select **Export** > **Template (*.XML)**.

   Step Result: The *File Download* dialog opens.

5. Click **Save**.

   Step Result: The *Save As* dialog opens.

6. Define the filepath where you want to save the Mandatory Baseline.

7. [Optional] Edit the **File name** field.

8. Click **Save**.

9. If you want to export Mandatory Baselines for additional groups, repeat the Mandatory Baseline exportation process from step 4.

Result: Your Mandatory Baseline(s) are exported.

Exporting Mandatory Baseline View Data

To export information displayed in the *Mandatory Baseline* view list to a comma separated value (`.csv`) file, select **Export** > **CSV File** from the toolbar. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 37.

The Vulnerabilities/Patch Content View

The *Groups* page view contains identical functionality to *Patch Content* page, but from this view, you can apply patch content to the endpoint groups you have created. Unlike the *Patch Content* page, this view will display only patch content applicable to the selected group.

The Vulnerabilities/Patch Content View Toolbar

This toolbar contains buttons related to the management of content. You can also launch deployments using this toolbar.

The following table describes the *Vulnerabilities/Patch Content* view toolbar functions.

Table 91: Vulnerabilities/Patch Content View Toolbar

Button	Function
Enable	Enables the selected disabled content item(s). For additional information, refer to Enabling Content within a Group on page 189.
	Note: This button is only available when a disabled item is selected.
Disable	Disables the selected enabled content item(s). For additional information, refer to Disabling Content Globally on page 353.
	Note: This button is only available when a enabled item is selected.
Do Not Patch...	Disables the selected patch for specific groups and endpoint that you select. For more information, see Disabling Content for Groups/Endpoints on page 355.
Update Cache	Caches (downloads or re-downloads) the package associated with the selected content item(s) (or the scripts associated with downloading the package(s). For additional information, refer to Updating the Cache on page 359.
Deploy...	Deploys selected content. For additional information, refer to Deploying Selected Content (Vulnerabilities/Patch Content View) on page 190.
Scan Now	Prompts the Discover Applicable Updates task to immediately check the endpoints . For additional information, refer to Using Scan Now (Endpoint Details Page) on page 135.

HEAT software

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Vulnerabiliites/Patch Content View List

This list displays content that applies to the selected group. You can also filter this list to display specific content items. Additionally, each item lists identification information and endpoint statistics.

Note: You can filter the list by using Patch Content filters.

Table 92: Column Definitions

Column	Icon	Definition
State	📄	The content item state, which indicates when the server downloaded the content item metadata. For additional information, refer to Content Status and Type on page 349.
Package Status	📦	The cache status for the content item, which indicates if the server downloaded the content item packages. For additional information, refer to Content Icons and Descriptions on page 350.
Name	N/A	The content item name, which links to the **Patch Status** of the item. For additional information, refer to The Patch Status Page on page 361.
Content Type	N/A	Indicates the content item type. For more information, see one of the following topics: • Vulnerabilities on page 341 • Software Content on page 342 • Other Content on page 342
Vendor	N/A	The name of the vendor that created the software in the content item.
Vendor Release Date	N/A	The date and time that the vendor released the software in the content item.

Column	Icon	Definition
Number of endpoints which came up Patched	✓	The number of endpoints patched with the content item.
Number of endpoints which came up Not Patched	✖	The number of endpoints not patched with the content item.
Total applicable	Σ	The number of endpoints that the content item applies to.
Number of endpoints which came up Do Not Patch	⊟	The number of endpoints that administrators have created a patch exception for.
Percent patched	%	The the percentage of applicable endpoints patched with the content item.

Additionally, you can expand each content item by clicking its arrow (**>**). The following table describes each field that displays when you expand a content item.

The following detail information appears on this page.

Table 93: Content Item Field Descriptions

Name	Description
Beta	Indicates if the content item is in beta.
Downloaded on (UTC)	The date and time on which the content was downloaded.
Associated packages	The number of packages associated with the content item.
Package status	The cache status for the content item packages.
HPL ID	The HPL identifier for the content item.
State	The enabled/disabled/completed status of the content item.
Enabled/Disabled by	The HPL user who last disabled or enabled the content.
Enabled/Disabled date (Server)	The date and time the content was disabled or enabled.
Enable/Disable reason	The reason the user provided for disabling or enabling the content. You can click the **Edit** link to change the reason.
Vendor product ID	The identifier given to the security content item by the vendor.
Vendor release date/time (UTC)	The date and time the vendor released the software in the content item.

HEAT software

Name	Description
Common Vulnerability Exploit (CVE) [1]	The CVE number for the content.
Vulnerability Code Description [1]	A description of the vulnerability associated with the content item.
Reference Text [1]	The reference text(s) associated with the content item vulnerability.
Description [1]	The narrative description of the distribution package. This section may include important notes about the content item and a link to more information.
[1]This meta data appears conditionally based on whether it was added for the content item. Additionally, there may be multiple instances of each meta data section.	

Disabling Content within a Group

You can disable content items from the *Groups* page as well as the content pages. Disabled content moves to the bottom of the list and is noted with a disabled status icon. Disable content to prevent it from being deployed.

Note: Disabling content within the *Vulnerabilities* view also disables it on all content pages.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Vulnerabilities**.

3. Select a group from the **Group Browser**.

4. If necessary, define filter criteria and click **Update View**.

5. Select one or more content items that you want to disable.

Note: If you select the **Select All** checkbox, all content visible on the page is selected. However, you can select all available content by clicking the **Select All** link.
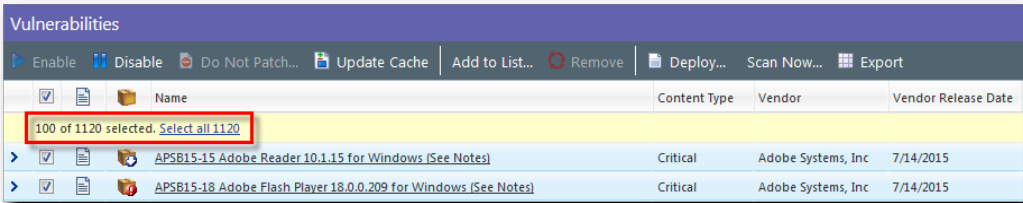
6. Click **Disable**.

Note: If you disable a content item that's already been cached, the package will not be updated if a new version of the content item is released.

Result: The selected content is disabled.

Enabling Content within a Group

After disabling a content item, re-enable it for deployment availability. You can re-enable content from the *Vulnerability* view regardless of where it was disabled. Enabled content is noted with an enabled status icon.

Note: Re-enabling a content item from the *Vulnerabilities* also re-enables it on all content pages.

---

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Vulnerabilities**.

3. Select a group from the **Group Browser**.

4. If necessary, define filter criteria and click **Update View**.

5. Select the disabled content items you want to enable.

Note: If you select the **Select All** checkbox, all content visible on the page is selected. However, you can select all available content by clicking the **Select All** link.
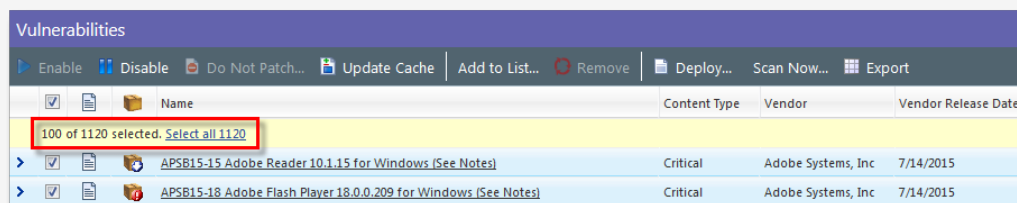
6. Click **Enable**.

Result: The selected content is re-enabled.

Updating the Groups Cache

From the *Vulnerabilities/Patch Content* view, you can update the cache for selected content items. Updating the cache for content items downloads the packages (or the scripts that will download the packages) associated with those items so you can deploy them immediately.

You can update the cache for content from the *Vulnerabilities* view, not just other content pages.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Vulnerabilities/Patch Content**.

HEAT software

3. From the directory tree, select the group with applicable vulnerabilities that you want to cache.

4. If necessary, designate filter criteria for the desired content and click **Update View**.

5. Select the check boxes associated with the content you want to cache.

6. Click **Update Cache**.

> **Step Result:** The **Warning** dialog opens, informing you that the update request and this action may take an extended period of time.
>
> > **Note:** The cache will not be updated for disabled content items that have had a new version released.

7. Click **OK**.

Result: The selected content begins caching.

Deploying Selected Content (Vulnerabilities/Patch Content View)

Within HEAT PatchLink DataCenter for Microsoft System Center, content can be deployed from a number of pages, including the **Groups** page **Vulnerabilities** view. When deploying from this page, the **Deployment Wizard** is preconfigured to deploy your selected content to the selected group.

For additional information, refer to About Deployments on page 289.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Vulnerabilities**.

3. From the **Group Browser**, select the group you want to deploy content to.

4. Select the content you want to deploy.

> **Note:** If you select the **Select All** checkbox, all content visible on the page is selected. However, you can select all available content by clicking the **Select All** link.
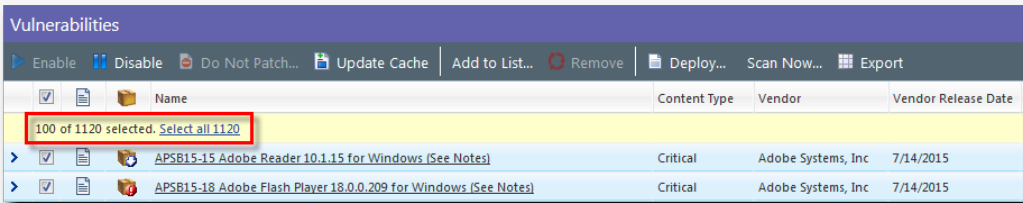
5. Click **Deploy**.

Result: The ***Deployment Wizard*** opens, preconfigured to deploy selected content to the selected group.

After Completing This Task:
Review Using the Deployment Wizard on page 303 and complete subsequent tasks.

Exporting Vulnerability/Patch Content View Data

To export information displayed in the ***Vulnerability*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 37.

The Deployments and Tasks View

The ***Deployments and Tasks*** view is similar to the ***Deployments and Tasks*** page because it lists pending, active, and completed deployments or tasks. However, unlike the ***Deployments and Tasks*** page (which lists all deployments), this view only lists the deployments that apply to the selected group. Additionally, you can use this view to manage and create deployments.

Note: This view does not display the deployments and tasks for each member; only the group's assigned deployments.

The Deployments and Tasks View Toolbar

This toolbar contains buttons that offer functionality related to the management and creation of deployments. Selection of list items associated with deployments may be necessary to use some buttons.

The following table describes the ***Deployments and Tasks*** view toolbar.

Table 94: Deployments and Tasks View Toolbar

Button	Function
Enable	Enables the selected disabled deployment or task. For additional information, refer to Enabling Group Deployments on page 193.
Disable	Disables the selected enabled deployment or tasks. For additional information, refer to Deleting Group Deployments on page 195.
Abort	Cancels the selected deployment or tasks for any endpoints that are yet to receive the deployment. For additional information, refer to Aborting Group Deployments on page 194.

HEAT®software

Button	Function
Delete	Removes the deployment or tasks from HEAT PatchLink DataCenter Server for Microsoft System Center. For additional information, refer to Deleting Group Deployments on page 195.
Deploy...	Deploys the selected packages. For additional information, refer to Deploying Content (Deployments and Tasks View) on page 195.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Deployments and Tasks View List

This list itemizes all deployments and deployment details applicable to the selected group.

View the **Deployments and Tasks View** list from the **Groups** page. The following table describes each **Deployments and Tasks View** list columns.

Table 95: Deployment and Tasks View List

Column	Icon	Description
Name	N/A	The name of the deployment.
Scheduled Date	N/A	The date and time the deployment was created.
Number of endpoints/ groups which were successful	✔	The total number of endpoints and groups that finished the deployment successfully.
Number of endpoints/ groups which failed	✖	The total number of endpoints and groups that finished the deployment unsuccessfully.
Number of endpoints/ groups assigned to the deployment	🖥#	The total number of endpoints and groups that are assigned to the deployment.

Column	Icon	Description
Number of endpoints/ groups which are in progress	📦	The total number of endpoints and groups that are receiving the deployment.
		Note: If you deploy to a group using Agent Local Time, the deployment remains in progress until all time zones have passed. This behavior ensures any endpoints added to the group following deployment start also receive content. This behavior does not occur when using Agent UTC Time.
Number of endpoints/ groups which were not deployed	🚫	The total number of endpoints and groups that were excluded from the deployment (because the package was already applied, not applicable, or marked *Do Not Patch*).
Number of endpoints/ groups which have completed the deployment	✅	The total number of endpoints and groups that finished the deployment.
Percentage Complete	%	The percentage of endpoints and groups that finished the deployment. Percentage = [Total Finished endpoints / Total Assigned endpoints]

Enabling Group Deployments

Within HEAT PatchLink DataCenter Server for Microsoft System Center, you can re-enable paused, group-specific deployments from the **Deployments and Tasks** view.

Enable group deployments from the **Deployments and Tasks** view, *not* the **Deployments and Tasks** page.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Deployments and Tasks**.

3. From the directory tree, select the group containing the deployment you want to enable.

4. Select the select the check box associated with the disabled deployment you want to enable.

5. Click **Enable**.

Result: The selected deployment is enabled.

HEAT software

Disabling Group Deployments

Within HEAT PatchLink DataCenter for Microsoft System Center, you can pause group-specific deployments from the **Deployments and Tasks** view.

Disable group deployments from the **Deployments and Tasks** view, *not* the **Deployments and Tasks** page.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Deployments and Tasks**.

3. From the directory tree, select the group containing the deployment you to disable.

4. Select the deployment you want to disable.

5. Click **Disable**.

Result: The selected deployment is disabled.

Aborting Group Deployments

Within HEAT PatchLink DataCenter for Microsoft System Center, you can abort group-specific deployments from the **Deployments and Tasks** view.

Abort group deployments from the **Deployments and Tasks** view, *not* the **Deployments and Tasks** page.

Note: The endpoints that have already received the deployment will not be affected. Only the endpoints that have not yet received the deployment will have the deployment aborted.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Deployments and Tasks**.

3. From the directory tree, select the group containing the deployment you want to abort.

4. Select the check box associated with the deployment you want to abort.

5. Click **Abort**.

Result: The selected deployment is aborted.

> **Note:** You cannot abort system tasks or Mandatory Baseline deployments.

Deleting Group Deployments

Within HEAT PatchLink DataCenter for Microsoft System Center, you can delete group-specific deployments from the ***Deployments and Tasks*** view.

Delete group deployments from the ***Deployments and Tasks*** view, *not* the ***Deployments and Tasks*** page.

Note: Deleting a deployment will have no effect on endpoints that have already received the deployment. You cannot delete system task deployments.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Deployments and Tasks**.

3. From the directory tree, select the group containing the deployment you want to delete.

4. Select the check box associated with the deployment you want to delete.

5. Click **Delete**.

Result: The selected deployment is deleted.

Deploying Content (Deployments and Tasks View)

Within HEAT PatchLink DataCenter for Microsoft System Center, content can be deployed from a number of pages, including the ***Groups*** page ***Deployments and Tasks*** view.

For additional information, refer to About Deployments on page 289.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Deployments and Tasks**.

3. From the directory tree, select the group deploy content to.

4. Click **Deploy**.

Result: The ***Deployment Wizard*** opens.

After Completing This Task:
Review Using the Deployment Wizard on page 303 and complete subsequent tasks.

Exporting Deployments View Data

To export information displayed in the ***Deployments and Tasks*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 37.

HEAT®software

The Agent Policy Sets View

After creating agent policy sets, you can apply them to a group using the **Agent Policy Sets** view. From this view you can add or remove existing agent policy sets to or from the selected group. Additionally, you can create policy sets from this view. However, this view, unlike the **Agent Policy Sets** page, does not let you edit policy sets or view their details. This view is only applicable to agent policy sets.

For additional information about agent policy sets, refer to About Agent Policies and Agent Policy Sets on page 217.

The Agent Policy Sets View Toolbar

This toolbar allows you to manage Agent Policy Sets for groups.

Table 96: Agent Policy Sets View Toolbar

Button	Function
Assign	Assigns an Agent Policy Set to the selected group and its child groups. For additional information, refer to Assigning an Agent Policy Set to a Group on page 197.
Unassign	Unassigns an Agent Policy Set to the selected group and its child groups. For additional information, refer to Unassigning an Agent Policy Set from a Group on page 198.
Create...	Creates an Agent Policy Set. For additional information, refer to Creating an Agent Policy Set (Groups Page) on page 199.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Agent Policy Sets View List

This list itemizes all agent policy sets and policy details assigned to the selected group.

View the **Agent Policy Sets View** list from the **Groups** page. The following table describes **Agent Policy Sets View** list.

Column	Description
Action	The **Unassign** icon indicates the Agent Policy Set may be unassigned.
	Note: You may use the **Unassign** icon to remove a policy set from the selected group. For additional information, refer to Unassigning an Agent Policy Set from a Group on page 198.
	The **Unassign Disabled** icon indicates the Agent Policy Set cannot be unassigned.
	Note: The **Unassign Disabled** icon indicates the policy is inherited. An inherited Agent Policy Set can not be unassigned from the group.
Name	The name of the Agent Policy Set.
	Note: You may select the **Name** column to sort the Agent Policy Set list.

Assigning an Agent Policy Set to a Group

Assigning an Agent Policy Set to a group defines functional rules for the group.

Prerequisites:

Create an Agent Policy Set. Refer to Creating an Agent Policy Set (Groups Page) on page 199 for details.

Assign Agent Policy Sets to groups from the *Agent Policy Sets* view.

Note: Groups that do not have an associated Agent Policy Set assigned, use the **Global System Policy**. Refer to About Agent Policies and Agent Policy Sets on page 217 for additional information.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Agent Policy Sets**.

3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Click **Assign**.

   Step Result: The **Select a Policy Set** list becomes active.

5. Select an agent policy set from the **Select a Policy Set** list.

HEAT software

6. Click the **Save** icon (🖫) to save your changes.

> **Step Result:** The **Select a Policy Set** list closes and your policy is assigned.

>> **Note:** The **Cancel** icon (🖫) cancels your changes and any edits are not saved.

Result: The policy set is saved and associated with the group.

Unassigning an Agent Policy Set from a Group

When desired, you can unassign an Agent Policy Set from a group.

Prerequisites:

An Agent Policy Set is assigned. Refer to Assigning an Agent Policy Set to a Group on page 197 for details.

Unassign the Agent Policy Sets to groups from the **Agent Policy Sets** view.

Note: Groups that do not have an associated Agent Policy Set assigned, use the **Global System Policy**. Refer to About Agent Policies and Agent Policy Sets on page 217 for additional information.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Agent Policy Sets**.

3. Select a group from the directory tree.

> **Note:** You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Remove the desired policy sets.

Use one of the following methods.

Method	Steps
To remove one Agent Policy Set:	Click the **Unassign** icon (↻) associated with the Agent Policy Set you want to remove.
To remove multiple Agent Policy Sets:	**1.** Select the check boxes associated with the Agent Policy Sets you want to remove. **2.** From the toolbar, click the **Unassign** button.

Note: An **Unassign Disabled** icon indicates you cannot remove an inherited Agent Policy Set. Instead, you must change the group policy inheritance setting or remove the inherited policy set from the parent group. Refer to *Policy Inheritance* in Editing Group Settings on page 212 for additional information.

Step Result: A dialog appears, prompting you to acknowledge the removal.

5. Click **OK**.

   Step Result: The selected policy set(s) are removed and the dialog closes.

Result: The Agent Policy Set(s) are no longer associated with the group.

Creating an Agent Policy Set (Groups Page)

You can create agent policy sets from the *Agent Policy Set* view. Agent policy sets are collections of values that can be assigned to groups to regulate how agents behave.

Note: When creating an agent policy set from the *Agent Policy Set* view, the created policy set will be immediately applied to the group selected in the directory tree.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Agent Policy Set**.

3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Click **Create**.

   Step Result: The *Create Agent Policy Set* dialog opens.

5. Type the applicable information in the **Policy Set Details** fields.

Field Name	Type
Policy Set Name	The name of the Agent Policy Set.
Policy Set Description	A description of the Agent Policy Set (optional).

6. Define the **Agent Hardening** option.

   These options define the steps required to delete an agent. For additional information, refer to About Agent Hardening on page 218.

Option	Description
Agent uninstall protection (list)	Select from the list to define whether the agent requires a password to be uninstalled. The default value is **On**.

HEAT software

7. Define the **Agent Logging** options.

The following table describes each option.

Option	Step
Logging level (button)	Click to open the *Logging Level* dialog. Use this dialog to select the agent logging level. For additional information, refer to Defining Agent Policy Logging Levels on page 244.
Maximum log file size (field)	Type the amount of disk space that triggers the agent to delete its log (1-500 MB). A value of *10* is the default setting.

8. Define the **Bandwidth Throttling** options.

Option	Step
Maximum Transfer Rate (field)	Type the maximum amount of network bandwidth (in Kbps), per endpoint that can be used by the agent for content download (0-1024). The default value of *0* disables bandwidth throttling.
Minimum File Size (field)	Type the threshold (in KB) at which a file will be managed by bandwidth throttling (0-1024). Files smaller than the defined value will not be managed by bandwidth throttling. The default value is *100*.

9. Define the **HEAT PatchLink DataCenter Agent for Linux/UNIX Communication** options.

The following table describes each option.

Options	Step
Use HTTP for file download (list)	Select whether packages are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and HEAT PatchLink DataCenter (*True* or *False*). The default value is *True*.
Send interval (list)	Select the amount of time that the agent should wait before sending an event to the HEAT PatchLink DataCenter server (0-5 seconds). A value of *2 seconds* is the default setting.
Receive interval (field and list)	Type and select the amount of time that the agent should delay before reattaching events from the HEAT PatchLink DataCenter Server. This value cannot exceed seven days. A value of *0 seconds* is the default setting.

Options	Step
Timeout interval **(field and list)**	Type and select the amount of time the agent should stay attached to the HEAT PatchLink DataCenter server before disconnecting (1 minute-7 days). A value of *12 hours* is the default setting.
Heartbeat interval **(field and list)**	Type and select the amount of time between agent check-ins with the HEAT PatchLink DataCenter server (1 minute-1 day). A value of *15 minutes* is the default setting.

10. Define the **HEAT PatchLink DataCenter Agent for Linux/UNIX Notification Defaults** options.

The following table describes each option.

Option	Description
Hide Agent Control Panel	This option controls whether the *Agent Control Panel* (and all associated dialogs and notifications) are hidden or accessible to an endpoint user after logging on (**True** or **False**).
	Note: • This policy will not take effect until the agent is restarted. • This policy can hide only the HEAT PatchLink DataCenter Agent for Windows. Agents installed on Linux, Unix, or Mac endpoints cannot be hidden. • When set to **True**, endpoint users can still open the *Agent Control Panel* using *Windows Control Panel*. • This policy cannot hide the Patch Agent or the LES Agent.
Show Alerts on Endpoint	This option control whether the associated dialogs and notifications for the *Agent Control Panel* are hidden or accessible to an endpoint user after logging on (**True** or **False**).

11. Define the **Reboot Behavior Defaults** option.

An endpoint module installation or feature may require an endpoint to restart (such as the Device Control module). This option defines how the reboot is performed.

a) From the **Reboot behavior** list, select a behavior.

Notify user, user response required before reboot	All logged-on endpoint users must agree unanimously to a restart. After the final user agrees to the reboot it will start immediately.
Notify user, automatically reboot within 5 minute timer	All users logged on to the endpoint are notified by a dialog that a restart will take place in five minutes.

HEAT software

Don't notify user, wait for next user-initiated reboot	No dialog notifies users that a reboot is required, and the policy does not take effect until the next time the endpoint is rebooted.

12. Define the **Patch Agent Communication** options.

The following table describes each option.

Option	Step
Use SSL for agent to server communication **(list)**	Select whether the Patch Agent uses HTTPS when communicating with the HEAT PatchLink DataCenter server.
Use HTTP for package download **(list)**	Select whether files are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and HEAT PatchLink DataCenter (*True* or *False*). The default value is *False*.
Agent Listener Port **(field)**	Select the agent listener port number. When the agent is contacted using this port, it responds with the agent version number and initiates communication with HEAT PatchLink DataCenter. The default value of *0* disables the agent listener.
Agent Scan Mode **(list)**	Select the mode that the Discover Applicable Updates (DAU) task runs in. These modes include: <table><tr><td>**Normal**</td><td>Performs the DAU task normally, which uses the least amount of resources.</td></tr><tr><td>**Initial Only**</td><td>Performs the first DAU task in fast mode, but subsequent DAU tasks in normal mode.</td></tr><tr><td>**Fast Scan**</td><td>Performs the DAU task faster, but uses more resources.</td></tr></table> The default value is *Normal*.
Communication Interval **(field and list)**	Type and select the interval (in minutes, hours, or days) between agent and HEAT PatchLink DataCenter communication (1 minute-1 day). The default value is *15 minutes*.
Inventory Collection Options **(button)**	Click to open the **Select Inventory Collection** dialog. Use this dialog to select the inventory values for recording during agent scanning. For additional information, refer to Defining Inventory Collection Options on page 246.

Option	Step
Resume Interrupted Downloads (list)	Select whether the agent resumes interrupted downloads at the point of interruption (*True* or *False*). The default value is *True*.
Hours of Operation (button)	Click to open the ***Edit Agent Hours of Operation*** dialog. Hours of operation are based on agent local time, allowing for further definition of the agent start and end times. For additional information, refer to Defining Agent Hours of Operation on page 248.

13. Define the **HEAT PatchLink DataCenter Deployment Notification Defaults** options.

Option	Step
User May Cancel (list)	Select whether the deployment recipient can cancel the deployment (**True** or **False**). The default value is **False**.
User May Snooze (list)	Select whether the deployment recipient can snooze the deployment (**True** or **False**). The default value is **True**.
Deploy Within (field)	Select the default time (in minutes) between the creation of the deployment and the deployment deadline (1-1440). The default value is **5 minutes**.
Always On Top (list)	Select whether deployment notifications display as the topmost window (**True** or **False**). The default value is **True**. For additional information about the **Always on Top** policy, refer to About the Show on Top Option on page 329.

14. Define the **HEAT PatchLink DataCenter Reboot Notification Defaults**.

Option	Step
User May Cancel (list)	Select whether the deployment recipient can cancel the reboot (**True** or **False**). The default value is *True*.
User May Snooze (list)	Select whether the deployment recipient can snooze the reboot (**True** or **False**). The default value is *True*.
Reboot Within (field)	Type the default time (in minutes) between the creation of the deployment and the reboot deadline (1-1440). The default value is **5 minutes**.

HEAT software

Option	Step
Always on Top (list)	Select whether reboot notifications display as the topmost window (**True** or **False**). The default value is **True**. For additional information about the **Always on Top** policy, refer to About the Show on Top Option on page 329.

15. Define the **Discover Applicable Updates (DAU)** option.

Option	Step
Scheduling Frequency (field)	Type the frequency (in hours) of the DAU task (1-8760). The default value is *26 hours*.

16. Define the **FastPath Servers** options.

For additional information, refer to About FastPath on page 251.

Option	Step
Interval (field and list)	Type the time interval (in minutes, hours, or days) between FastPath server validations (0 minutes-7 days). The default value of *0* disables the option.
Servers (button)	Click **Define** to open the ***Edit FastPath Servers*** dialog. Use this dialog to add FastPath servers. For additional information, refer to Adding/Editing FastPath Servers on page 251.

17. Click **Save**.

Result: Your agent policy set is saved and assigned to the selected group. You can also assign the agent policy set to other endpoint groups or edit the set.

Exporting Agent Policy Sets View Data

To export information displayed in the ***Agent Policy Sets*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 37.

The Roles View

This view lists the user roles that can access the selected group. This view is similar to the ***Roles*** page, but applies only to the selected group rather than the entire system. From this view, you can manage which roles have access to the selected group.

The Roles View Toolbar

This toolbar contains buttons that let you add (or remove) roles that can access the selected group. You can also use it to create new user roles.

The following table describes the functionality of each **Roles** view toolbar button.

Table 97: Roles View Toolbar

Button	Function
Add	Adds a role to the group. For additional information, refer to Adding a Role to a Group on page 206.
Remove	Removes a role from the group. For additional information, refer to Removing a Role from a Group on page 206.
Create...	Creates a new user role. For additional information, refer to Creating User Roles (Roles View) on page 207.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Roles View List

This list displays the roles that can access the selected group. Use the **Action** column to remove user roles. Additionally, you can filter this table using the filter row.

The following table describes each **Roles** view list column.

Table 98: Roles View List

Column	Description
Action	Contains a **Remove** icon. Use this icon to remove a role from the associated group.
Status	Contains an icon that indicates the type of role. For additional information, refer to one of the following topics: • Predefined System Roles on page 273 • Custom Roles on page 274

HEAT®software

Column	Description
Name	Indicates the name of the user role.
Source Group	Indicates the group from which the role was created.

Adding a Role to a Group

Add a user role to a group to grant it group access. If the selected group's **Policy inheritance** setting is set to **true**, the added user role will also be able to access the selected group's descendant groups.

Add roles to a group from the *Roles* view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Roles**.

3. Select a group from the directory tree.

4. Click **Add**.

5. Select a role from the **Select a Role** list.

   Select from the following roles:

   - **Administrator**
   - **Manager**
   - **Operator**
   - **Guest**
   - *Custom Role(s)*

   Note: *Custom Role(s)* are only available if a custom role has been created.

6. Click the **Save** icon.

Result: The role is saved and associated with the group.

Removing a Role from a Group

Remove a user role from a group to deny its associated users group access. If the selected group has **policy inheritance** set to **true**, removing a role will remove the role from the selected group's descendant groups as well.

Remove user roles from a group using the *Roles* view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Roles**.

3. Select a group from the directory tree.

4. Remove roles from the group.

Use one of the following methods.

Method	Steps
To remove a single role:	Click the **Remove** icon associated with the role you want to remove from the group.
To remove multiple roles:	**1.** Select the check boxes associated with the roles you want to remove from the group. **2.** From the toolbar, click **Remove**.

Note: Inherited roles cannot be removed. To remove inherited roles, either edit the group's inheritance policy or remove the roles from the applicable parent group. To understand group policy inheritance and its effects, refer to Defining Agent Policy Inheritance Rules on page 219.

Step Result: A dialog displays, asking you to acknowledge the removal.

5. Acknowledge the removal by clicking **OK**.

Result: The role is removed and is no longer associated with the group.

Creating User Roles (Roles View)

Custom roles let you select individual access rights, accessible groups, and accessible endpoints for that role. Create a custom role when predefined system roles do not contain the access rights needed for a particular user. Creating a custom role is also useful when you require a role that can only access specific groups or endpoints.

You can create roles from the *Roles* view as well as the *Roles* tab.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Roles**.

3. Select a group from the directory tree.

Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Click **Create**.

Step Result: The *Create Role* dialog appears with the *Information* tab selected by default.

5. Type a name in the **Name** field.

6. Type a description in the **Description** field.

7. Select a role template from the **Role Template** list.

Any existing role can be used as a template. The selected role determines initial access rights. You can later change which access rights are assigned to the role.

HEAT software

8. Select the *Access Rights* tab.

9. Select or clear the desired access rights.

   For additional information, refer to Predefined System Roles on page 273.

   Tip: Select or clear the **All** check box to globally select or clear all access rights. Additionally, child access rights are unavailable until their parent access rights are selected.

10. Select the *Groups* tab.

11. Assign the desired accessible endpoint groups to the role.

    Use one of the following methods to assign groups.

Method	Steps
To assign individual groups:	1. From the **Available Groups** table, select the check box(es) associated with the group(s) you want to assign. 2. Click **Assign**.
To assign all groups:	Click **Assign All**.

Tip: Remove groups using **Remove** and **Remove All**.

12. Select the *Endpoints* tab.

13. Assign the desired accessible endpoints to the role.

    Use one of the following methods to assign endpoints.

Method	Steps
To assign individual endpoints:	1. From the **Available Endpoints** table, select the check box(es) associated with the endpoint(s) you want to assign. 2. Click **Assign**.
To assign all endpoints:	Click **Assign All**.

Tip: Remove endpoints using **Remove** and **Remove All**.

14. Click **OK**.

Result: The new role is saved and assigned to the selected group.

Note: A created role can be edited from the *Users and Roles* page *Roles* tab. Refer to Editing User Roles on page 284.

In addition, a new role can be assigned to users. Refer to Editing Users on page 265.

Exporting Roles View Data

To export information displayed in the **Roles** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 37.

The Dashboard View

Similar to the **Home** page dashboard, the **Dashboard** view displays widgets depicting HEAT PatchLink DataCenter for Microsoft System Center activity. However, unlike the **Home** page dashboard, the **Dashboard** view widgets include only information about endpoints within the selected group and its child hierarchy.

Widgets graphs and information are generated based on the latest HEAT PatchLink DataCenter for Microsoft System Center server and agent data available.

Note: The widgets displayed in the **Dashboard** view include data from the selected group's child hierarchy. Configuration changes made to the dashboard settings apply to all groups; not just the selected group.

Group Dashboard Widgets

Most widgets available on the **Home** page dashboard are also available from the **Dashboard** view. The data depicted on each dashboard changes according to which group is selected.

The following table describes the available widgets.

Table 99: Group Dashboard Widgets

Widget	Description
Agent Module Installation Status	Displays the installation and licensing statistic of each agent module.
Agent Status	Displays all agents grouped by status.
Applicable Content Updates	Displays applicable content updates grouped by content updates.
Critical Patch Status by Endpoint	Displays the patch status of all endpoints with applicable vulnerabilities grouped by when they were released.
Discovery Scan Results: Agents	Displays the total number of agent-supported endpoints discovered in the last-run Discovery Scan Job and identifies how many have an agent installed.
Endpoints with Unresolved Updates	Displays all endpoints with applicable content updates that have not yet been applied, grouped by content type.

HEAT software

Widget	Description
Incomplete Deployments	Displays all deployments with elapsed start dates and a status of not started or in progress.
Mandatory Baseline Compliance	Displays the percentage of endpoints grouped by Mandatory Baseline compliance.
Offline Patch Agents	Displays all offline agents grouped by the amount of time since they last checked in.
Patch Agent Module Status Widget	Displays all agents with the HEAT PatchLink DataCenter modules installed, which are grouped by HEAT PatchLink DataCenter status.
Scheduled Deployments	Displays endpoints with applicable content updates grouped by content type and the deployment status within each category.
Time Since Last DAU Scan	Displays all active agents (not including disabled or offline) grouped by the amount of time since their last Discover Applicable Updates task.
Un-remediated Critical Vulnerabilities	Displays the total number of un-remediated critical vulnerabilities that are applicable to your environment grouped by age.

Tip: For information about how to edit the group dashboard, refer to Editing the Dashboard on page 49.

Widget Setting and Behavior Icons

Setting and behavior icons are user interface controls that let you manage widgets and the dashboard within the *Groups* view. Click these controls to maximize, minimize, hide, and refresh widgets.

The following table describes each icon action.

Table 100: Widget Setting and Behavior Icons

Icon	Action
	Opens the **Dashboard Settings** dialog.
	Opens the dashboard in print preview mode.
	Collapses the associated widget.
	Expands the associated collapsed widget.
	Hides the associated widget.

Icon	Action
⟳	Refreshes the associated widget (or the entire dashboard).

Note: Not all widgets contain **Refresh** icons.

Previewing and Printing the Dashboard

As with the *Home* page dashboard, you can preview and print the *Group* page *Dashboard* view. *Dashboard* view widgets display data that applies only to the selected group.

To preview the *Dashboard* view, select the applicable group from the **Browser** and click the print icon.

For additional information, refer to Previewing and Printing the Dashboard on page 49.

Editing the Dashboard

Just as with the *Home* page dashboard, you can edit the widgets displayed on the *Group* page *Dashboard* view. *Dashboard* view widgets display data that only applies to the selected group.

To edit the widgets displayed within the *Dashboard* view, select the applicable group from the **Browser** and click the edit icon.

For additional information, refer to Editing the Dashboard on page 49.

The Settings View

This view lets you edit various basic settings for the selected group. The settings in this view are miscellaneous settings that cannot be grouped with other settings.

The following table describes *Settings* view button functions.

Table 101: Settings View Toolbar

Button	Function
Save	Saves the settings defined in the page.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

HEAT®software

Editing Group Settings

If different settings are required, you can edit the default settings for a group. Modifying group settings not only modifies settings for the selected group, but also potentially determines settings for descendant groups.

Modify group settings from the *Settings* view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Settings**.

3. Select the desired group from the directory tree.

4. [Optional] Under **General**, edit the following as necessary.

Option	Description
Group Name (field)	The group name.
	Note: Only `Custom` group names can be edited.
Distinguished Name	A system-created group name that represents the group's parent hierarchy.
	Note: The **Distinguished Name** cannot be edited.
Group Description (field)	The group description.
Q Chain Mode (list)	Defines chain behavior during Mandatory Baseline deployments. Select from the following options: • **Standard -- Set Individually** • **Auto QChain with Manual Reboots** • **Auto QChain with Automatic Reboots**
Deployments Enabled (list)	Defines whether deployments may be created for the group. A `True` value allows authorized users to create deployments for the group.

Note: The **Deployments Enabled** list only impacts the ability to create deployments for a group. Deployments created prior to disabling group deployments will still occur as scheduled. Additionally, any deployments created for the endpoint will occur as scheduled.

5. [Optional] Under **Mandatory Baseline**, edit the following as necessary.

List	Description
Mandatory Baseline Inheritance	Defines whether the group inherits the agent policies assigned to the group's parent hierarchy. A `True` value sets the group to inherit its parent hierarchy's Mandatory Baseline settings.
Mandatory Baseline Enabled	Defines whether Mandatory Baselines may be assigned to the group. A `True` value allows users to create Mandatory Baseline deployments for the group.

Important: The **Mandatory Baselines enabled** setting applies only to the selected group. Therefore, if the selected group has a parent group with a **Mandatory Baselines enabled** setting of `True`, the selected group will receive its parent group Mandatory Baseline items regardless of its own **Mandatory Baselines enabled** setting.

6. Under **Policy**, edit the following lists as necessary.

List	Description
Policy Inheritance	Defines whether the group inherits the agent policies assigned to the group's parent hierarchy. A `True` value sets the group to inherit its parent hierarchy's agent policy settings.
	Note: To understand agent policy inheritance and its effects, refer to Defining Agent Policy Inheritance Rules on page 219.
Policies Enabled	Defines whether agent policies may be assigned to the group. A `True` value allows users to assign agent policies directly to the group.

7. Under **Other**, edit the following fields as necessary.

Field	Description
Group Owners	User-defined email addresses indicating the owners of the group.
Source Groups (button)	User-defined group or groups whose agents are dynamically assigned to the group. For additional information, refer to Assigning a Source Group to a Custom Group on page 215.

8. Click **Save**.

Result: The new settings are saved and applied to the group.

HEAT software

Defining Source Groups

Source groups are groups that automatically assign managed endpoints to a associated custom group. Use a source group to maintain multiple endpoint memberships by editing only a single group. This feature simplifies maintenance of endpoint membership among groups.

When working within the **Groups** page **Settings** view, you can assign the selected view a source group. By assigning the selected group a source group, the selected group will be modified when the source group has endpoints added or removed. Source groups only affect endpoint membership, not group agent policies and settings.
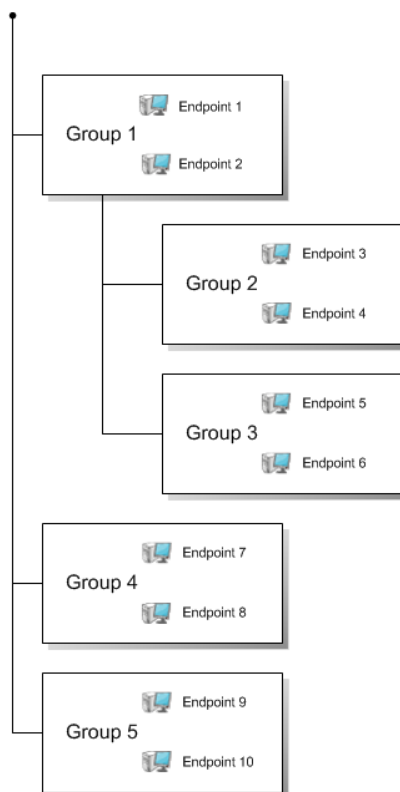
Figure 40: Source Group Diagram

When selecting a source group, all endpoints within the source group's child hierarchy are included, regardless of whether the child groups are selected. Additionally, if the source group (or any of its child groups) has a source group, those endpoints are also included. Source groups can only be assigned to custom groups.

The preceding diagram and the following bullets clarify how group sources operates.

- If group 3 uses group 5 as a source group, then group 3 would include endpoints 9 and 10, as well as endpoints 5 and 6.
- Because group 3 is in group 1's hierarchy, group 1 also includes endpoints 9 and 10.
- If group 4 uses group 1 as a source group, group 4 would include endpoints 7 and 8 (through direct assignment), endpoints 1 and 2 (through a directly assigned source group), endpoints 3, 4, 5, and 6 (through group 1's hierarchy), and endpoints 9 and 10 (through an indirectly assigned source group for [group 5 is a source group for group 3]).

Assigning a Source Group to a Custom Group

When a custom group is created, you can assign it a *source group*, which is a group that automatically assigns managed endpoints to associated groups. For example, if you assign *Group 1* as a source group to *Group 2*, any agents assigned to *Group 1* are automatically assigned to *Group 2*.

Assign a group a source group from the **Settings** view.

Note: Source groups can only be assigned to custom groups.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Settings**.

3. Select a custom group from the directory tree.

4. Under **Other**, click **Modify**.

   If necessary, scroll to the button.

   Step Result: The **Edit Source Groups** dialog opens.
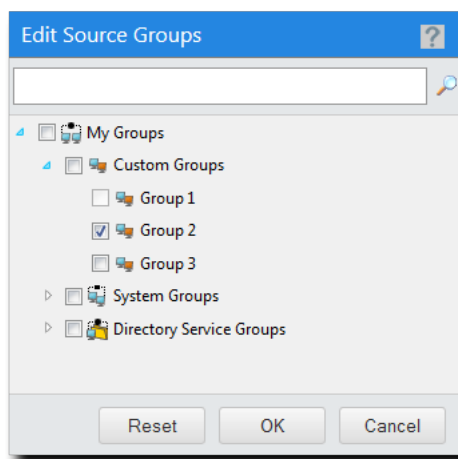
Figure 41: Edit Source Groups Dialog

5. Expand the directory tree or use the search field to locate the group you want to use as a source.

HEAT software

6. Select the groups you want to use as sources.

> **Note:** When selecting a source group, all endpoints within the source group's child hierarchy are included, regardless of whether the child groups are selected. Additionally, if the source group (or any of its child groups) has a source group, those endpoints are also included. For additional information, refer to Defining Source Groups on page 214.

7. Click **OK**.

Result: The custom group now uses the selected groups as sources. As new agents are added to (or removed from) the source group, they are also added to (or removed from) the custom group.

Exporting Settings View Data

To export information displayed in the **_Settings_** view to a comma separated value (`.csv`) file, click **Export**. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 37.

Chapter

9

Managing Agent Policy Sets

In this chapter:

- The Agent Policy Sets Page
- Working with Agent Policy Sets

Within HEAT PatchLink DataCenter for Microsoft® System Center, use *Agent Policy Sets* to control agent behavior. Agent Policy Sets are basic rules which define how agents behave.

Apply the *Agent Policy Sets* to groups to implement your policies to groups. There is a policy for every agent function.

The Agent Policy Sets Page

You can control agent behavior by creating and assigning Agent Policy Sets. Use the **Agent Policy Sets** page to define agent rules of behavior.

You can access this page at any time from the navigation menu.

Figure 42: Agent Policy Sets Page

About Agent Policies and Agent Policy Sets

Agent Policies are rules that govern agent behavior. Agent Policy Sets are a collections of agent policy values.

Assign agent policies to groups using the *Agent Policy Sets* view. Based on group membership, agents operate according to the values in assigned Agent Policy Sets. Assignment of Agent Policy Sets is optional.

HEAT software

Groups without assigned Agent Policy Sets have their behavior defined by the **Global System Policy**. The **Global System Policy** does the following:

- Defines behavior for groups with no assigned policy set.
- Defines policy values for incomplete agent policy sets.

When agents holding multiple group memberships are assigned conflicting agent policy values, they are resolved with conflict resolution rules. These rules are a set of protocols that determine which policy value an agent uses when conflicts occur. For additional information, refer to Defining Agent Policy Conflict Resolution on page 219.

About Agent Hardening

Agent Policy Sets include **Agent Hardening** policies, which are policies used to prevent unauthorized HEAT PatchLink DataCenter Agent for Linux/UNIX.

Agent Hardening (when set to On)	- It prevents the HPL Agent installation location (`C:\Program Files\HEAT\EMSSAgent` by default) from being renamed, edited, or deleted. - The Agent is *hardened*, meaning the agent cannot be intentionally or unintentionally modified. - When hardening is in place, you can still upgrade or uninstall the agent after entering the **agent uninstall password** or the **global uninstall password**, which is only necessary when modifying the agent locally from the endpoint. For additional information about defining **Agent Hardening** policies, refer to the following topics: - Creating an Agent Policy Set on page 230 - Editing an Agent Policy Set on page 236
Global uninstall password	**Important:** The **Global uninstall password** option is only available when editing the **Global System Policy** agent policy set. Refer to Changing the Global Uninstall Password on page 242 for additional information. The **Global uninstall password** is a universal password that temporarily disables agent uninstall protection. This password works on all network endpoints. You are prompted for this password when manually upgrading or uninstalling hardened agents. **Note:** HEAT *does not* recommend providing end users with the global uninstall password in uninstall scenarios. The **Global uninstall password** should be used by the HEAT PatchLink DataCenter for Microsoft System Center Administrator only.

Viewing the Agent Policy Sets Page

Navigate to this page to view Agent Policy Sets and their policy settings. Expand policy sets to view the individual policy settings.

You can access this page any time using the navigation menu.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Agent Policy Sets**.
2. [Optional] Complete a task listed in Working with Agent Policy Sets on page 230.

Defining Agent Policy Inheritance Rules

You can configure a group to inherit policies from its parent hierarchy using the **Policy inheritance** setting.

Because a group can inherit policies and have them directly assigned, policy conflicts may arise. The following rules apply when a group has **Policy Inheritance** set to `True`:

1. Any conflicting policies are assigned to the parent, but not the child. Conflicting policies are resolved at the parent level using the conflict policy resolution rules.
2. Agent Policy Set values directly assigned to a group supersede inherited Agent Policy Set values.
3. Any conflicting policies that are assigned directly to the child group are resolved by conflict resolution rules.
4. Any Agent Policy Set values that are undefined by the group's directly assigned policy are defined by the parent's group policy.
5. Policy values still undefined are defined by the **Global System Policy** set.

For more information on how to enable a group's *Policy Inheritance* setting, refer to Editing Group Settings on page 212.

For more information on *Conflict Policy Resolution* rules, refer to Defining Agent Policy Conflict Resolution on page 219.

Defining Agent Policy Conflict Resolution

On occasion, a group or endpoint may be assigned two different Agent Policy Sets that have conflicting policies. When this occurs, the system determines which policy to use based on the *Agent Policy Conflict Resolution* rules.

Conflicting policies are resolved in the following order.

1. **Group Policies** - Conflicting policy sets assigned to a group are resolved before conflicting policy sets assigned to an agent are resolved.

   The following rules apply if a group has **Policy Inheritance** set to `False`:

   a. The group does not inherit its parent policy set. Therefore, only policy sets assigned directly to the group require resolution.
   b. Conflicting policies are resolved according to the agent policy conflict resolution rules.

   The following rules apply if a group has **Policy Inheritance** set to `True`:

◢HEAT software

    a. The group inherits its parent policy set. Any conflicting policy sets that are resolved at the parent level prior to assignment to the child level.

    b. Conflicting policies are assigned directly to the group are resolved using the agent policy conflict resolution rules. Any policy set values assigned directly to a group supersede inherited policy set values.

    c. Finally, any policies that are undefined by direct assignment are defined by inheritance.

2. **Agent Policies** - After resolving the group policies, the conflicting policies assigned to an endpoint (using its group membership) are resolved. The following rules apply:

    a. The resultant policies of all groups the endpoint is a member are resolved according to the agent policy conflict resolution rules.

    b. Any policy values that have not been defined using the agent group membership are populated based on the policy settings defined in the **Global System Policy**.

Note: Conflict resolution rules do not apply to the **Global System Policy**.

The following table defines the rules used when resolving conflicting policy settings:

Table 102: Agent Policy Conflict Resolution Rules

Policy Setting	Resolution
Hide Agent Control Panel	The agent uses true (Y).
Core: Download file via HTTP	The agent uses true (Y).
Maximum Log File Size	The agent uses the largest log file size value.
Logging Level	The agent uses the most comprehensive logging level value (Trace [4] > Diagnostic [3] > Normal [2] > Error [1] > Critical [0]).
Agent uninstall protection	The agent uses On.
Show alerts on endpoints	The agent uses false (N).
Reboot behavior	The agent uses a combination of the most secure value, while still giving the user the best chance to save their work. The items are listed in the following order: • Notify user, user response required before reboot = 0 • Don't notify user, wait for next user-initiated reboot = 2 • Notify user, automatically reboot with 5 minute timer = 1
Core: Heartbeat Interval	The agent uses the largest heartbeat interval frequency value.
Core: Receive Interval	The agent uses the largest receive interval frequency value.
Core: Timeout Interval	The agent uses the largest timeout interval frequency value.
Core: Send Interval	The agent uses the largest send interval frequency value.

Policy Setting	Resolution
HEAT PatchLink DataCenter	
Maximum Transfer Rate	The agent uses the smallest maximum transfer rate value.
Minimum File Size	The agent uses the smallest minimum file size value.
Agent Scan Mode	The agent uses the fastest agent scan mode value (Fast Scan [2] > Initial Scan [1] > Normal Scan [0]).
Scheduling Frequency	The agent uses the shortest scheduling frequency interval value.
HPL Deployment: User May Cancel	The agent uses true (Y).
HPL Deployment: Always On Top	The agent uses true (Y).
HPL Deployment: Deploy within	The agent uses the smallest deploy within value.
HPL Deployment: User May Snooze	The agent uses false (N).
Resume Interrupted Downloads	The agent uses false (N).
Patch: FastPath Interval	The agent uses the shortest FastPath interval.
Patch: FastPath Servers	The agent uses all of the defined FastPath servers.
Patch: Download packages via HTTP	The agent uses true (Y).
Agent Listener Port	The agent listens on the highest defined port.
HPL Reboot: User May Cancel	The agent uses false (N).
HPL Reboot: Always On Top	The agent uses true (Y).
HPL Reboot: Reboot within	The agent uses the smallest reboot within value.
HPL Reboot: User May Snooze	The agent uses false (N).
Patch: Agent to Server Communication	The agent uses true (https://).
Patch: Communication Interval	The agent uses the shortest communication interval value.

HEAT software

Policy Setting	Resolution
Hours of Operation: Monday	The agent uses `Always On`.
Hours of Operation: Tuesday	The agent uses `Always On`.
Hours of Operation: Wednesday	The agent uses `Always On`.
Hours of Operation: Thursday	The agent uses `Always On`.
Hours of Operation: Friday	The agent uses `Always On`.
Hours of Operation: Saturday	The agent uses `Always On`.
Hours of Operation: Sunday	The agent uses `Always On`.
InventoryCollectionOption: BIOS	The agent `ON`.
InventoryCollectionOption: CPU	The agent `ON`.
InventoryCollectionOption: CUSTOM	The agent `ON`.
InventoryCollectionOption: DISK_DRIVE	The agent `ON`.
InventoryCollectionOption: ENABLE_WMI	The agent `ON`.
InventoryCollectionOption: HW_DEV_OTHER	The agent `ON`.
InventoryCollectionOption: HW_IDE_CONTROL	The agent `ON`.
InventoryCollectionOption: HW_NETWORK_ADAPT	The agent `ON`.
InventoryCollectionOption: HW_NON_PNP	The agent `ON`.
InventoryCollectionOption: HW_SND_GAME	The agent `ON`.

Policy Setting	Resolution
InventoryCollectionOption: HW_SYS_DEV	The agent ON.
InventoryCollectionOption: HW_USB	The agent ON.
InventoryCollectionOption: HW_USB_CONTROL	The agent ON.
InventoryCollectionOption: HW_USB_STORAGE	The agent ON.
InventoryCollectionOption: LAST_REBOOT	The agent ON.
InventoryCollectionOption: LAST_USER	The agent ON.
InventoryCollectionOption: MANUF_MODEL	The agent ON.
InventoryCollectionOption: None	The agent OFF.
InventoryCollectionOption: OS_SERIAL	The agent ON.
InventoryCollectionOption: PC_ASSET_TAG	The agent ON.
InventoryCollectionOption: PC_SERIAL	The agent ON.
InventoryCollectionOption: RAM	The agent ON.
InventoryCollectionOption: SERVICES	The agent ON.
InventoryCollectionOption: SOFTWARE	The agent ON.
InventoryCollectionOption: VIRTUAL	The agent ON.

HEAT® software

The Agent Policy Sets Page Toolbar

This toolbar contains buttons that allow you to create and edit Agent Policy Sets.

The following table describes each toolbar button.

Table 103: Agent Policy Sets Page Toolbar

Button	Function
Delete	Deletes the selected Agent Policy Set(s). For additional information, refer to Deleting an Agent Policy Set on page 242.
Create...	Creates a new Agent Policy Set. For additional information, refer to Creating an Agent Policy Set on page 230.
Export	Exports the page data to a comma-separated value (.csv) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Agent Policy Sets Page List

For each agent policy set that you create, an item for that set appears in the **Agent Policy Sets** page list. This list names each existing agent policy set and provides access to editing functionality.

Table 104: Agent Policy Sets Page List

Column	Description
Action	Contains **Edit** and **Delete** icons. Use these icons to edit and delete the associated agent policy set. For additional information, refer to the following topics: • Editing an Agent Policy Set on page 236 • Deleting an Agent Policy Set on page 242
	Note: The **Global System Policy** cannot be deleted.
Name	The name of the agent policy set.

Each item listed on the **Agent Policy Sets** page can be expanded to list its individual policy settings. To view agent policy set details from the page list, click the **Rotating Chevron (>)** for the agent policy set, which opens a table containing additional details.

Table 105: Agent Policy Set Details Table

Name	Description
Policy Name	Indicates the unique name of the agent policy set.
Type	Indicates the type of agent policy set (`System` or `User Defined`).
Description	Indicates the description of the agent policy set.
Created By	Indicates the name of the user that created the agent policy set.
Created Date	Indicates the date and time that the agent policy set was created.
Modified By	Indicates the name of the user that last modified the agent policy set.
Modified Date	Indicates the date and time that the agent policy set was last modified.
Agent uninstall protection	Indicates whether agent uninstall protection is on.
Hide agent control panel	Indicates whether the Agent Control Panel is hidden from an endpoint user when they log on to their system. Any dialog or notification launched by the HEAT PatchLink DataCenter agent will also be hidden until the **Agent Control Panel** is started manually using **Windows Control Panel**.
Reboot behavior	Indicates the reboot behavior. The following values indicate each reboot behavior setting: • Notify user, user response required before reboot = `0` • Notify user, automatically reboot with 5 minute timer = `1` • Don't notify user, wait for next user-initiated reboot = `2`
Download files via HTTP	Indicates whether the HEAT PatchLink DataCenter Agent downloads files via HTTP rather than HTTPS. All other communication occurs over HTTPS.
Maximum Log File Size	Specifies the maximum size of the HEAT PatchLink DataCenter agent log before it is deleted.
Logging Level	Indicates the level of detail recorded in the HEAT PatchLink DataCenter Agent. The following values indicate each logging level: Critical = `0`, Error = `1`, Normal = `2`, Diagnostic = `3`, Trace = `4`.

HEAT®software

Name	Description
Show alerts on endpoints	Indicates whether alerts and notifications are shown to endpoint users.
Core: Heartbeat Interval	Indicates the interval at which the Endpoint Service sends a heartbeat to the server (in minutes).
Core: Receive Interval	Indicates the interval at which the Endpoint Service communication receive delay intervals (in seconds).
Core: Timeout Interval	Indicates the interval at which the Endpoint Service communication receive time intervals (in seconds)
Core: Send Interval	Indicates the interval at which the Endpoint Service communication send delay intervals.
Patch: Download packages via HTTP	Indicates if the agent downloads packages using HTTP, regardless of whether HTTPS is used for agent to server communication.
Patch: Maximum Transfer Rate	Indicates the maximum bandwidth used when an agent downloads packages. A setting of *0* disables bandwidth throttling.
Patch: Minimum File Size	Indicates the smallest file size that will be impacted by bandwidth throttling.
Patch: Agent Scan Mode	Indicates the agent detection scan mode (0 = Slow, 1 = Fast the first time, 2 = Fast).
Patch DAU: Scheduling Frequency	Indicates the number of hours between regularly scheduled detection scans.
Patch Deployment: User May Cancel	Indicates whether the user can cancel a deployment (Y, N).
Patch Deployment: Always on Top	Indicates whether the notification will be the topmost window (Y, N).
Patch Deployment: Deploy Within	Indicates the defined time frame (in minutes) during which the user may snooze or cancel a reboot.
Patch Deployment: User May Snooze	Indicates whether the user can snooze a deployment.
Patch: Resume Interrupted Downloads	Indicates whether resumable downloads are enabled (0 = No, 1 = Yes).

Name	Description
Patch: Fast Path Interval	Indicates the interval (configurable in minutes, hours, and days) between each check by FastPath to determine the fastest communication path back to the HEAT PatchLink DataCenter server.
Patch: Fast Path Servers	Indicates the available Fast Path routes.
Patch Agent Listener Port	Indicates the agent listener port. When the agent is contacted on this port, it responds with its version number and initiates communication with the HEAT PatchLink DataCenter server. A value of 0 turns the agent listener off.
Patch Reboot: User May Cancel	Indicates whether the user can cancel a reboot (`Y`, `N`).
Patch Reboot: Always on Top	Indicates whether the notification will be the topmost window (`Y`, `N`).
Patch Reboot: Reboot Within	Indicates the defined time window (in minutes) during which the user may snooze or cancel a reboot.
Patch Reboot: User May Snooze	Indicates whether the user can snooze a reboot (`Y`, `N`).
Patch: Agent to Server Communication Protocol	Defines how the agent will communicate with the server (`http://` or `https://`).
Patch: Communication Interval	Indicates the time period between agent communication attempts.
Patch: Hours of Operation Monday	Defines the agent Hours of Operation (HOP) for Monday.
Patch: Hours of Operation Tuesday	Defines the agent HOP for Tuesday.
Patch: Hours of Operation Wednesday	Defines the agent HOP for Wednesday.
Patch: Hours of Operation Thursday	Defines the agent HOP for Thursday.
Patch: Hours of Operation Friday	Defines the agent HOP for Friday.
Patch: Hours of Operation Saturday	Defines the agent HOP for Saturday.
Patch: Hours of Operation Sunday	Defines the agent HOP for Sunday.

HEAT®software

Name	Description
Patch: InventoryCollectionOptions: BIOS	Indicates whether BIOS data will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: CPU	Indicates whether CPU data will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: CUSTOM	Indicates whether custom inventory data will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: DISK_DRIVES	Indicates whether data regarding the disk drives will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: ENABLE_WMI	Indicates whether WMI data will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_DEV_OTHER	Indicates whether the Windows registry will be scanned for additional hardware information during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_IDE_CONTROL	Indicates whether data regarding IDE ATA/ATAPI controllers will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_NETWORK_ADAPT	Indicates whether data regarding network adapters will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_NON_PNP	Indicates whether data regarding non-Plug and Play drivers will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_SND_GAME	Indicates whether data regarding sound, video, and game controllers will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_SYS_DEV	Indicates whether system device data will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_USB	Indicates whether data regarding USB endpoint's inventory (from \ENUM\USB) will be gathered during agent inventory collection (OFF or ON).

Name	Description
Patch: InventoryCollectionOptions: HW_USB_CONTROL	Indicates whether data regarding USB controllers will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_USB_STORAGE	Indicates whether data regarding USB device inventory (from \ENUM\USBSTOR) will be gathered during agent inventory collection (OFF or ON).
InventoryCollectionOptions: LAST_REBOOT	Requires ENABLE_WMI = ON: Indicates whether the last boot time will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: LAST_USER	Indicates whether last logged in user and time will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: MANUF_MODEL	Requires ENABLE_WMI = ON: Indicates whether the computer manufacturer and model will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: OS_SERIAL	Requires ENABLE_WMI = ON: Indicates whether the OS serial number will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: PC_ASSET_TAG	Requires ENABLE_WMI = ON: Indicates whether the endpoint's asset tag will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: PC_SERIAL	Requires ENABLE_WMI = ON: Indicates whether the endpoint's serial number will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: RAM	Indicates whether the endpoint's total physical RAM will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: SERVICES	Indicates whether a listing of Windows services (not applicable for Windows 9x or ME) will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: SOFTWARE	Indicates whether a listing of installed software will be gathered during agent inventory collection (OFF or ON).

HEATsoftware

Name	Description
Patch: InventoryCollectionOptions: VIRTUAL	Indicates whether the endpoint's virtualization status will be gathered during agent inventory collection (OFF or ON).

> **Note:** This reference table does not list the **Value** contained in the agent policy set details. This column (which appears in the user interface) contains values that agent policies are set to.

Working with Agent Policy Sets

There are many tasks that you can perform from the *Agent Policy Sets* page related to agent policy sets. Some tasks are performed by clicking toolbar buttons, while others are performed by interacting with list items.

- Creating an Agent Policy Set on page 230
- Editing an Agent Policy Set on page 236
- Deleting an Agent Policy Set on page 242
- Changing the Global Uninstall Password on page 242
- Defining Agent Policy Logging Levels on page 244
- Defining Agent Hours of Operation on page 248
- The Edit FastPath Servers Dialog on page 250
- Exporting Data for Agent Policy Sets on page 254

Creating an Agent Policy Set

You can create an unlimited number of Agent Policy Sets to define how endpoints behave. Following creation, associate an Agent Policy Set with a group or endpoint to apply policy settings. After installing new modules, additional options are available when creating an Agent Policy Set.

Create an Agent Policy Sets from the **Create Agent Policy Set** dialog.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Agent Policy Sets**.

2. Click **Create**.

   Step Result: The **Create Agent Policy Set** dialog opens.

3. Type the applicable information in the **Policy Set Details** fields.

Field Name	Type
Policy Set Name	The name of the Agent Policy Set.
Policy Set Description	A description of the Agent Policy Set (optional).

4. Define the **Agent Hardening** option.

   These options define the steps required to delete an agent. For additional information, refer to About Agent Hardening on page 218.

Option	Description
Agent uninstall protection (list)	Select from the list to define whether the agent requires a password to be uninstalled. The default value is **On**.

5. Define the **Agent Logging** options.

   The following table describes each option.

Option	Step
Logging level (button)	Click to open the ***Logging Level*** dialog. Use this dialog to select the agent logging level. For additional information, refer to Defining Agent Policy Logging Levels on page 244.
Maximum log file size (field)	Type the amount of disk space that triggers the agent to delete its log (1-500 MB). A value of *10* is the default setting.

6. Define the **Bandwidth Throttling** options.

Option	Step
Maximum Transfer Rate (field)	Type the maximum amount of network bandwidth (in Kbps), per endpoint that can be used by the agent for content download (0-1024). The default value of *0* disables bandwidth throttling.
Minimum File Size (field)	Type the threshold (in KB) at which a file will be managed by bandwidth throttling (0-1024). Files smaller than the defined value will not be managed by bandwidth throttling. The default value is *100*.

7. Define the **HEAT PatchLink DataCenter Agent for Linux/UNIX Communication** options.

   The following table describes each option.

Options	Step
Use HTTP for file download (list)	Select whether packages are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and HEAT PatchLink DataCenter (*True* or *False*). The default value is *True*.

HEAT software

Options	Step
Send interval **(list)**	Select the amount of time that the agent should wait before sending an event to the HEAT PatchLink DataCenter server (0-5 seconds). A value of *2 seconds* is the default setting.
Receive interval **(field and list)**	Type and select the amount of time that the agent should delay before reattaching events from the HEAT PatchLink DataCenter Server. This value cannot exceed seven days. A value of *0 seconds* is the default setting.
Timeout interval **(field and list)**	Type and select the amount of time the agent should stay attached to the HEAT PatchLink DataCenter server before disconnecting (1 minute-7 days). A value of *12 hours* is the default setting.
Heartbeat interval **(field and list)**	Type and select the amount of time between agent check-ins with the HEAT PatchLink DataCenter server (1 minute-1 day). A value of *15 minutes* is the default setting.

8. Define the **HEAT PatchLink DataCenter Agent for Linux/UNIX Notification Defaults** options. The following table describes each option.

Option	Description
Hide Agent Control Panel	This option controls whether the *Agent Control Panel* (and all associated dialogs and notifications) are hidden or accessible to an endpoint user after logging on (**True** or **False**). **Note:** • This policy will not take effect until the agent is restarted. • This policy can hide only the HEAT PatchLink DataCenter Agent for Windows. Agents installed on Linux, Unix, or Mac endpoints cannot be hidden. • When set to **True**, endpoint users can still open the *Agent Control Panel* using **Windows Control Panel**. • This policy cannot hide the Patch Agent or the LES Agent.
Show Alerts on Endpoint	This option control whether the associated dialogs and notifications for the *Agent Control Panel* are hidden or accessible to an endpoint user after logging on (**True** or **False**).

9. Define the **Reboot Behavior Defaults** option.

   An endpoint module installation or feature may require an endpoint to restart (such as the Device Control module). This option defines how the reboot is performed.

   a) From the **Reboot behavior** list, select a behavior.

Notify user, user response required before reboot	All logged-on endpoint users must agree unanimously to a restart. After the final user agrees to the reboot it will start immediately.
Notify user, automatically reboot within 5 minute timer	All users logged on to the endpoint are notified by a dialog that a restart will take place in five minutes.
Don't notify user, wait for next user-initiated reboot	No dialog notifies users that a reboot is required, and the policy does not take effect until the next time the endpoint is rebooted.

10. Define the **Patch Agent Communication** options.

    The following table describes each option.

Option	Step
Use SSL for agent to server communication **(list)**	Select whether the Patch Agent uses HTTPS when communicating with the HEAT PatchLink DataCenter server.
Use HTTP for package download **(list)**	Select whether files are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and HEAT PatchLink DataCenter (*True* or *False*). The default value is *False*.
Agent Listener Port **(field)**	Select the agent listener port number. When the agent is contacted using this port, it responds with the agent version number and initiates communication with HEAT PatchLink DataCenter. The default value of *0* disables the agent listener.

/HEAT®software

Option	Step
Agent Scan Mode (list)	Select the mode that the Discover Applicable Updates (DAU) task runs in. These modes include:

	Normal	Performs the DAU task normally, which uses the least amount of resources.
	Initial Only	Performs the first DAU task in fast mode, but subsequent DAU tasks in normal mode.
	Fast Scan	Performs the DAU task faster, but uses more resources.

The default value is *Normal*.

Option	Step
Communication Interval (field and list)	Type and select the interval (in minutes, hours, or days) between agent and HEAT PatchLink DataCenter communication (1 minute-1 day). The default value is *15 minutes*.
Inventory Collection Options (button)	Click to open the **Select Inventory Collection** dialog. Use this dialog to select the inventory values for recording during agent scanning. For additional information, refer to Defining Inventory Collection Options on page 246.
Resume Interrupted Downloads (list)	Select whether the agent resumes interrupted downloads at the point of interruption (*True* or *False*). The default value is *True*.
Hours of Operation (button)	Click to open the **Edit Agent Hours of Operation** dialog. Hours of operation are based on agent local time, allowing for further definition of the agent start and end times. For additional information, refer to Defining Agent Hours of Operation on page 248.

11. Define the **HEAT PatchLink DataCenter Deployment Notification Defaults** options.

Option	Step
User May Cancel (list)	Select whether the deployment recipient can cancel the deployment (**True** or **False**). The default value is **False**.
User May Snooze (list)	Select whether the deployment recipient can snooze the deployment (**True** or **False**). The default value is **True**.

Option	Step
Deploy Within (field)	Select the default time (in minutes) between the creation of the deployment and the deployment deadline (1-1440). The default value is **5 minutes**.
Always On Top (list)	Select whether deployment notifications display as the topmost window (**True** or **False**). The default value is **True**. For additional information about the **Always on Top** policy, refer to About the Show on Top Option on page 329.

12. Define the **HEAT PatchLink DataCenter Reboot Notification Defaults**.

Option	Step
User May Cancel (list)	Select whether the deployment recipient can cancel the reboot (**True** or **False**). The default value is *True*.
User May Snooze (list)	Select whether the deployment recipient can snooze the reboot (**True** or **False**). The default value is *True*.
Reboot Within (field)	Type the default time (in minutes) between the creation of the deployment and the reboot deadline (1-1440). The default value is **5 minutes**.
Always on Top (list)	Select whether reboot notifications display as the topmost window (**True** or **False**). The default value is **True**. For additional information about the **Always on Top** policy, refer to About the Show on Top Option on page 329.

13. Define the **Discover Applicable Updates (DAU)** option.

Option	Step
Scheduling Frequency (field)	Type the frequency (in hours) of the DAU task (1-8760). The default value is *26 hours*.

14. Define the **FastPath Servers** options.

For additional information, refer to About FastPath on page 251.

Option	Step
Interval (field and list)	Type the time interval (in minutes, hours, or days) between FastPath server validations (0 minutes-7 days). The default value of *0* disables the option.

HEAT®software

Option	Step
Servers **(button)**	Click **Define** to open the *Edit FastPath Servers* dialog. Use this dialog to add FastPath servers. For additional information, refer to Adding/Editing FastPath Servers on page 251.

15. Click **Save**.

Result: Your Agent Policy Set is saved. You can now assign the Agent Policy Set to endpoint groups or edit the set.

After Completing This Task:

To assign an Agent Policy Set to a group, complete Assigning an Agent Policy Set to a Group on page 197.

Editing an Agent Policy Set

Following the creation of an Agent Policy Set, you can modify it to accommodate network environment changes.

The *Edit A Policy Set* dialog allows you to modify an agent policy set.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Agent Policy Sets**.

2. Click the **Edit** icon associated with the policy set you want to edit.

   Step Result: The *Edit a Policy Set* dialog opens.

3. [Optional] Edit the **Policy Set Details** fields.

Field Name	Type
Policy Set Name	The name of the Agent Policy Set.
Policy Set Description	A description of the Agent Policy Set (optional).

4. [Optional] Edit the **Agent Hardening** options.

   These options define the steps required to delete an agent. For additional information, refer to About Agent Hardening on page 218.

Option	Step
Agent uninstall protection **(list)**	Select from the list to define whether the agent requires a password to be uninstalled. The default value is **On**.

Option	Step
Global Uninstall Password (button)	Click **Modify** to open the ***Global Uninstall Password*** dialog. Use this dialog to define a password for manually uninstalling the agent. For additional information, refer to Changing the Global Uninstall Password on page 242.
	Note: This option only available when editing the Global System Policy agent policy set. Only users assigned to the built-in Administrator role may view or modify the global uninstall password.

5. [Optional] Edit the **Agent Logging** options.

Option	Step
Logging level (button)	Click to open the ***Logging Level*** dialog. Use this dialog to select the agent logging level. For additional information, refer to Defining Agent Policy Logging Levels on page 244.
Maximum log file size (field)	Type the amount of disk space that triggers the agent to delete its log (1-500 MB). A value of *10* is the default setting.

6. [Optional] Edit the **HEAT PatchLink DataCenter Agent for Linux/UNIX Communication** options.

Options	Step
Use HTTP for file download (list)	Select whether packages are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and HEAT PatchLink DataCenter (*True* or *False*). The default value is *True*.
Send interval (list)	Select the amount of time that the agent should wait before sending an event to the HEAT PatchLink DataCenter server (0-5 seconds). A value of *2 seconds* is the default setting.
Receive interval (field and list)	Type and select the amount of time that the agent should delay before reattaching events from the HEAT PatchLink DataCenter Server. This value cannot exceed seven days. A value of *0 seconds* is the default setting.
Timeout interval (field and list)	Type and select the amount of time the agent should stay attached to the HEAT PatchLink DataCenter server before disconnecting (1 minute-7 days). A value of *12 hours* is the default setting.

HEAT software

Options	Step
Heartbeat interval **(field and list)**	Type and select the amount of time between agent check-ins with the HEAT PatchLink DataCenter server (1 minute-1 day). A value of *15 minutes* is the default setting.

7. [Optional] Define the **HEAT PatchLink DataCenter Agent for Linux/UNIX Notification Defaults** options.

The following table describes each option.

Option	Description
Hide Agent Control Panel	This option controls whether the *Agent Control Panel* (and all associated dialogs and notifications) are hidden or accessible to an endpoint user after logging on (**True** or **False**).
	Note: • This policy will not take effect until the agent is restarted. • This policy can hide only the HEAT PatchLink DataCenter Agent for Windows. Agents installed on Linux, Unix, or Mac endpoints cannot be hidden. • When set to **True**, endpoint users can still open the *Agent Control Panel* using *Windows Control Panel*. • This policy cannot hide the Patch Agent or the LES Agent.
Show Alerts on Endpoint	This option control whether the associated dialogs and notifications for the *Agent Control Panel* are hidden or accessible to an endpoint user after logging on (**True** or **False**).

8. [Optional] Edit the **Reboot Behavior Defaults**.

An endpoint module installation or feature may require an endpoint to restart (such as the Device Control module). This option defines how the reboot is performed.

a) From the **Reboot behavior** list, select a behavior.

Notify user, user response required before reboot	All logged-on endpoint users must agree unanimously to a restart. After the final user agrees to the reboot it will start immediately.
Notify user, automatically reboot within 5 minute timer	All users logged on to the endpoint are notified by a dialog that a restart will take place in five minutes.
Don't notify user, wait for next user-initiated reboot	No dialog notifies users that a reboot is required, and the policy does not take effect until the next time the endpoint is rebooted.

9. [Optional] Edit the **Patch Agent Communication** options.

Option	Step
Use SSL for agent to server communication (list)	Select whether the Patch Agent uses HTTPS when communicating with the HEAT PatchLink DataCenter server.
Use HTTP for package download (list)	Select whether files are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and HEAT PatchLink DataCenter (*True* or *False*). The default value is *False*.
Agent Listener Port (field)	Select the agent listener port number. When the agent is contacted using this port, it responds with the agent version number and initiates communication with HEAT PatchLink DataCenter. The default value of *0* disables the agent listener.
Agent Scan Mode (list)	Select the mode that the Discover Applicable Updates (DAU) task runs in. These modes include: <table><tr><td>**Normal**</td><td>Performs the DAU task normally, which uses the least amount of resources.</td></tr><tr><td>**Initial Only**</td><td>Performs the first DAU task in fast mode, but subsequent DAU tasks in normal mode.</td></tr><tr><td>**Fast Scan**</td><td>Performs the DAU task faster, but uses more resources.</td></tr></table> The default value is *Normal*.
Communication Interval (field and list)	Type and select the interval (in minutes, hours, or days) between agent and HEAT PatchLink DataCenter communication (1 minute-1 day). The default value is *15 minutes*.
Inventory Collection Options (button)	Click to open the **Select Inventory Collection** dialog. Use this dialog to select the inventory values for recording during agent scanning. For additional information, refer to Defining Inventory Collection Options on page 246.
Resume Interrupted Downloads (list)	Select whether the agent resumes interrupted downloads at the point of interruption (*True* or *False*). The default value is *True*.

HEAT software

Option	Step
Hours of Operation (button)	Click to open the ***Edit Agent Hours of Operation*** dialog. Hours of operation are based on agent local time, allowing for further definition of the agent start and end times. For additional information, refer to Defining Agent Hours of Operation on page 248.

10. [Optional] Edit the **HEAT PatchLink DataCenter Server for Microsoft System Center Deployment Notification Defaults** options.

Option	Step
User May Cancel (list)	Select whether the deployment recipient can cancel the deployment (**True** or **False**). The default value is **False**.
User May Snooze (list)	Select whether the deployment recipient can snooze the deployment (**True** or **False**). The default value is **True**.
Deploy Within (field)	Select the default time (in minutes) between the creation of the deployment and the deployment deadline (1-1440). The default value is **5 minutes**.
Always On Top (list)	Select whether deployment notifications display as the topmost window (**True** or **False**). The default value is **True**. For additional information about the **Always on Top** policy, refer to About the Show on Top Option on page 329.

11. [Optional] Edit the **HEAT PatchLink DataCenter Server for Microsoft System Center Reboot Notification Defaults**.

Option	Step
User May Cancel (list)	Select whether the deployment recipient can cancel the reboot (**True** or **False**). The default value is *True*.
User May Snooze (list)	Select whether the deployment recipient can snooze the reboot (**True** or **False**). The default value is *True*.
Reboot Within (field)	Type the default time (in minutes) between the creation of the deployment and the reboot deadline (1-1440). The default value is **5 minutes**.

Option	Step
Always on Top **(list)**	Select whether reboot notifications display as the topmost window (**True** or **False**). The default value is **True**. For additional information about the **Always on Top** policy, refer to About the Show on Top Option on page 329.

12. [Optional] Edit the **Discover Applicable Updates (DAU)** option.

Option	Step
Scheduling Frequency **(field)**	Type the frequency (in hours) of the DAU task (1-8760). The default value is *26 hours*.

13. [Optional] Edit the **FastPath Servers** options.

Option	Step
Interval **(field and list)**	Type the time interval (in minutes, hours, or days) between FastPath server validations (0 minutes-7 days). The default value of *0* disables the option.
Servers **(button)**	Click **Define** to open the ***Edit FastPath Servers*** dialog. Use this dialog to add FastPath servers. For additional information, refer to Adding/Editing FastPath Servers on page 251.

14. [Optional] Edit the **Bandwidth Throttling** options.

Option	Step
Maximum Transfer Rate **(field)**	Type the maximum amount of network bandwidth (in Kbps), per endpoint that can be used by the agent for content download (0-1024). The default value of *0* disables bandwidth throttling.
Minimum File Size **(field)**	Type the threshold (in KB) at which a file will be managed by bandwidth throttling (0-1024). Files smaller than the defined value will not be managed by bandwidth throttling. The default value is *100*.

15. Click **Save**.

Result: Your edits are saved. The new policy values take effect the next time the applicable agents communicate with the HEAT PatchLink DataCenter server.

HEAT software

Deleting an Agent Policy Set

As your network environment changes, Agent Policy Sets may no longer be applicable. When this event occurs, you may delete the unnecessary Agent Policy Set.

You can delete Agent Policy Sets at any time from the *Agent Policy Sets* page.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Agent Policy Sets**.

2. Delete one or more Agent Policy Sets.

   Use one of the following methods.

Method	Steps
To delete one Agent Policy Set:	Click the **Delete** icon associated with an Agent Policy Set.
To delete multiple Agent Policy Sets:	1. Select the check boxes associated with the Agent Policy Sets you want to delete. 2. From the toolbar, click the **Delete** button.

Note: Assigned agent policy sets and the **Global System Policy** cannot be deleted.

Step Result: A dialog displays, asking you to acknowledge the deletion.

3. Acknowledge the deletion by clicking **OK**.

Result: The Agent Policy Set(s) is deleted.

Changing the Global Uninstall Password

Change the Global Uninstall Password associated with the **Global System Policy** set. to uninstall any agent in your network.

Note: To uninstall an agent from its host endpoint, you must enter one of two passwords: *Endpoint Uninstall Password* or the *Global Uninstall Password*. The Global Uninstall Password feature ensures that endpoint users cannot uninstall the agent without the knowledge and permission of the administrator.

Define the Global Uninstall Password when editing the **Global System Policy**.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Agent Policy Sets**.

2. Click the edit icon ( ) for the **Global System Policy** set.

   Step Result: The *Edit a Policy Set* dialog opens.

3. Under the **Agent Hardening** section, click the **Modify** button adjacent to the **Global uninstall password** field.

    Step Result: The **Global Uninstall Password** dialog opens.

Figure 43: Global Uninstall Password Dialog

4. Type the desired password in the **New password** field.

    Tip: The password must be at least `8` characters in length.

5. Retype the password in the **Confirm new password** field.

6. Click **Save**.

    Note: Password edits are not saved until the agent policy set itself is saved.

7. Finish any desired edits to the **Global System Policy** set and click **Save**.

    Note: Password edits are not saved until the **Global System Policy** set is saved.

Result: The **Global Uninstall Password** dialog closes. Your edits take effect the next time HEAT PatchLink DataCenter for Microsoft System Center and the applicable agents communicate.

HEAT software

Defining Agent Policy Logging Levels

All HEAT PatchLink DataCenter for Microsoft System Center Agents record a log of events that transpire on the endpoint. An Agent Policy Set logging level setting controls how much memory an agent's host endpoint allocates for event logs.

Note: A defined logging level can help troubleshoot agent policy behavior. Define logging levels carefully: a low logging level may not record enough information to be useful; however, a high logging level may record verbose information at the cost of higher disk space.

Define logging levels when creating or editing an Agent Policy Set.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Agent Policy Sets**.

2. Perform one of the following procedures based on your context.

Context	Procedure
If you are creating an agent policy set:	Click **Create**.
If you are editing an agent policy set:	Click the edit icon associated with the policy set containing the logging level setting you want to edit.

   Step Result: Either the **Create an Agent Policy Set** or the **Edit a Policy Set** dialog opens.

3. Under the **Agent Logging** section perform one of the following procedures based on your context.

Context	Procedure
If you are defining the logging level for the first time:	Click the **Define** button adjacent to the **Logging level** field.

Context	Procedure
If you are modifying the logging level:	Click the **Modify** button adjacent to the **Logging level** field.

Step Result: The *Logging Level* dialog opens.
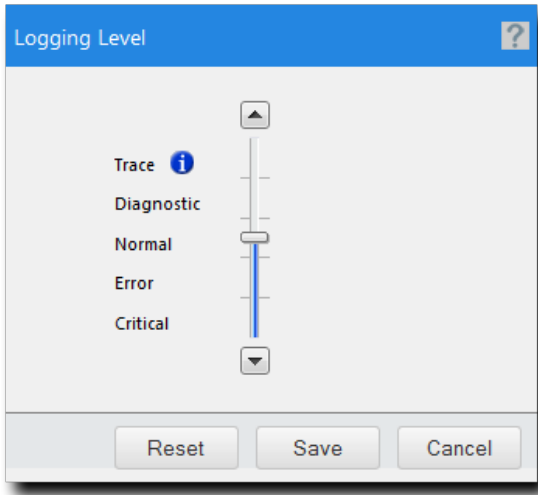
Figure 44: Logging Level Dialog

4. Move the slider to the desired logging level.

The following table describes each logging level.

Logging Level	Description
Trace	Logs all errors and system actions.
	Note: This highest level logging level should be used only when necessary, as it will consume a large amount of resources on the endpoint.
Diagnostic	Logs all errors and major system actions.
Normal	Logs all errors and basic system action and usage information.
Error	Logs only errors.
Critical	Logs only critical events.

5. Click **Save**.

HEAT®software

6. Finish any additional edits to the Agent Policy Set and click **Save**.

Note: Logging level edits are not saved until the Agent Policy Set is saved.

Result: The *Logging Level* dialog closes. Your edits take effect the next time the HEAT PatchLink DataCenter for Microsoft System Center server and the applicable agents communicate.

Defining Inventory Collection Options

Each HEAT PatchLink DataCenter for Microsoft System Center agent compiles a list of hardware and software present on its host endpoint. However, you can control how detailed this inventory is; you can configure what hardware and software items the agent should scan for. Selecting fewer items from the list requires fewer system resources, but the resulting inventory is not as robust.

Perform this task from *Select Inventory Collection* dialog when editing or creating an agent policy set.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Agent Policy Sets**.

2. Perform one of the following procedures based on your context.

Context	Procedure
If you are creating an agent policy set:	Click **Create**.
If you are editing an agent policy set:	Click the edit icon associated with the policy set containing the logging level setting you want to edit.

Step Result: Either the *Create Agent Policy Set* or the *Edit a Policy Set* dialog opens.

3. Under the *Patch Agent Communication* section perform one of the following procedure based on your context.

Context	Procedure
If you defining inventory collection options for the first time:	Click the **Define** button adjacent to the **Inventory Collection Options** field.
If you modifying inventory collection options:	Click the **Modify** button adjacent to the **Inventory Collection Options** field.

Step Result: The *Select Inventory Collection* dialog opens.

4. Select or clear the check boxes associated with the desired inventory collection options. The following table describes each option.

Tip: Selecting an option with child options automatically selects the child options as well.

Option	Description
Allow use of WMI during inventory collection	Required if Windows Management Instrument (WMI) data will be gathered.
Hardware	Selects or clears all options grouped under **Hardware**.
USB controllers	Scans for data regarding USB device inventory (from `HKEY_LOCAL_MACHINE\Enum\USB`).
IDE ATA/ATAPI controllers	Scans for data regarding IDE ATA/ATAPI controllers.
Other hardware devices	Scans for system device data.
Processors	Scans for processor data.
USB Storage Devices	Scans for data regarding USB device inventory (from `HKEY_LOCAL_MACHINE\Enum\USBSTOR`).
Network adapters and MAC address (may use WMI)	Scans for data regarding network adapters.
Physical RAM - amount	Scans for the endpoint's total physical RAM.
System devices	Scans the Windows registry for additional hardware information.
Non-Plug and Play drivers	Scans for data regarding non plug-and-play drivers.
Locally attached drives, total, and free space	Scans for data regarding the disk drives.
USB devices	Scans for data regarding USB controllers.
BIOS information	Scans for BIOS data.
Sound, video, and game controllers	Scans for data regarding sound, video, and game controllers.
Services	Scans for a listing of Windows services (not applicable for Windows 9x or ME).
Software	Scans for a listing of installed software.
Other	Selects or clears all child options grouped under **Other**.
OS serial number (requires WMI)	Scans for the OS serial number (requires WMI).
Virtual Machines	Scans to determine if the endpoint is a virtual machine.

HEAT software

Option	Description
Endpoint serial number (requires WMI)	Scans for the endpoint's serial number (requires WMI).
Endpoint manufacturer and model (may use WMI)	Scans for the computer manufacturer and model.
Endpoint asset tag (requires WMI)	Scans for the endpoint's asset tag (requires WMI).
User - last logged on	Scans for last logged in user and time.
System uptime (may use WMI)	Scans for and returns the time since last reboot (system uptime).
Custom import from file (may use WMI)	Scans for files containing custom inventory data.

5. Click **OK**.

6. Finish any desired edits in the agent policy set dialog and click **Save**.

> **Note:** Edits to the **Inventory Collection Options** are not saved until you click **Save** in the agent policy set dialog.

Result: Your edits are saved. These edits take effect the next time HEAT PatchLink DataCenter for Microsoft System Center and the applicable agents communicate.

Defining Agent Hours of Operation

Agent hours of operations determine when a patch agent is active on its host endpoint. In other words, this setting restricts agent operations to a specific time range. By applying a specific hours of operation setting, you can configure the agents to operate at optimal hours. For example, setting your agents to only work during the weekend will ensure bandwidth remains open during operation hours, helping to maintain worker efficiency. Optimal agent hours of operation vary by network.

Edit agent hours of operation when creating or editing an agent policy set.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Agent Policy Sets**.

2. Perform one of the following procedures based on your context.

Context	Procedure
If you are creating an agent policy set:	Click **Create**.

Context	Procedure
If you are editing an agent policy set:	Click the edit icon associated with the policy set containing the logging level setting you want to edit.

Step Result: Either the *Create Agent Policy Set* or the *Edit a Policy Set* dialog opens.

3. Under *Patch Agent Communication* perform one of the following procedure based on your context.

Context	Procedure
If you are creating an agent policy set:	Click the **Define** button adjacent to the **Hours of Operation** field.
If you are editing an agent policy set:	Click the **Modify** button adjacent to the **Hours of Operation** field.

Step Result: The *Edit Agent Hours of Operation* dialog opens.
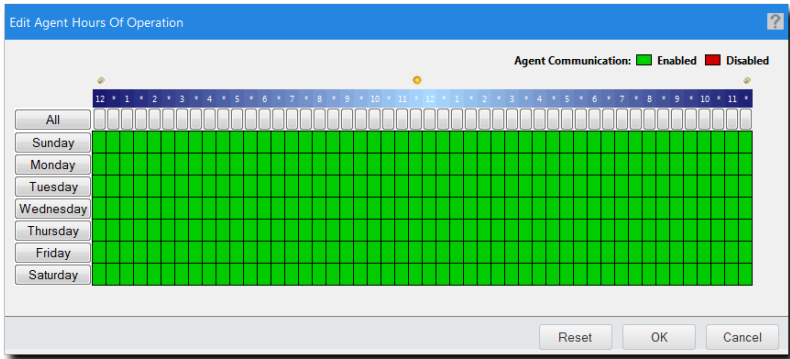
Figure 45: Edit Agent Hours of Operation Dialog

4. Click time units to define agent hours of operation.

Green units indicate days and times of enablement, while red units indicate days and times of disablement.

- Click **All** to toggle all *Time* units on or off.
- Click *Day* to toggle time units for a day on or off.
- Click *Time* units to toggle individual units on or off.

5. Click **OK**.

HEAT®software

6. Finish any desired edits in the dialog and click **Save**.

> **Note:** Changes made to the **Hours of Operation** schedule will not be saved until you have clicked **Save** in the **agent policy set dialog**.

Result: Your edits are saved. These edits take effect the next time HEAT PatchLink DataCenter for Microsoft System Center and the applicable agents communicate.

The Edit FastPath Servers Dialog

Use this dialog to leverage caching proxies in your network, also known as *FastPath Servers*, to store content and reroute your server and agent communications.
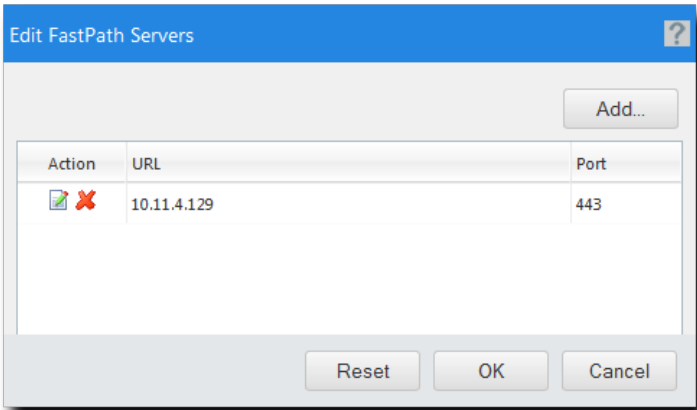
Figure 46: Edit FastPath Servers Dialog

To access this dialog, click the **Define/Modify** next to **Servers** field within the ***Create/Edit A Policy Set*** dialog.

Table 106: Edit FastPath Servers Dialog Columns

Column	Description
Action	Contains action icons (✎ and ✖). Use these to edit and delete FastPath servers.
URL	The URL of the FastPath server.
Port	The port number the FastPath server uses to route communication between the server and agents.

The following table describes the buttons specific to the *Create/Edit FastPath Servers* dialog.

Table 107: Edit FastPath Servers Dialog Buttons

Button	Description
Add	Opens the *Add/Modify FastPath Server* dialog. For additional information, refer to Adding/Editing FastPath Servers on page 251.

About FastPath
In large networks, you can configuring caching proxies, or FastPath servers, to increase deployment speed and reroute server and agent communications.

This practice provides several benefits:

- Endpoints download deployment content from FastPath servers instead of your HEAT PatchLink DataCenter for Microsoft System Center server. This action reduces bandwidth consumed during large deployments.
- You can assign FastPath servers to endpoints by applying policies to groups, rather than assigning them directly to the endpoint.
- You can assign fallback FastPath servers, in case the primary FastPath server fails.

Periodically, agents validate the FastPath servers you have assigned to a group. During this process, agents determine the FastPath server used by contacting each one. The FastPath server with the shortest path to the agent is used for deployments and communications.

Add FastPath servers and a FastPath communication interval to a policy by defining the **FastPath Server** policies.

Adding/Editing FastPath Servers
Use of FastPath servers, or caching proxies, optimizes communication routes between your server and agents.

You can add or edit FastPath servers from the *Add/Modify FastPath Server* dialog when creating or editing agent policy sets.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Agent Policy Sets**.

2. Perform one of the following procedures based on your context.

Context	Procedure
To create an agent policy set:	Click **Create**.
To edit an agent policy set:	Click ✎ for the policy you want to edit.

Step Result: A dialog for creating or editing an agent policy set opens.

HEAT software

3. Under *FastPath Servers* perform one of the following procedures based on context.

Context	Procedure
If adding FastPath servers for the first time:	Click **Define** next to the **Servers** field.
If modifying FastPath servers that have already been defined:	Click **Modify** next to the **Servers** field.

Step Result: The *Edit FastPath Servers* dialog opens.

4. Click **Add**.

Tip: If you want to edit existing FastPath server settings, click 📝 for the server.

Step Result: The *Add/Modify Server* dialog opens.

5. Define the FastPath server information.

Type the FastPath server information in the following fields.

Field	Description
URL	The FastPath server URL in the following format: `http://<FastPathURL>`.
Port	The FastPath server port number used to route server and agent communication.

6. If using a FastPath server that requires authentication, select the **Authenticated** check box and type the applicable information in the following fields.

HPL validates the credentials that you enter.

Field	Description
User Name	A local or domain user account that authenticates with the FastPath server.
Password	The password for the user name.
Confirm Password	The password retyped.

7. Click **OK**.

Step Result: The *Add/Modify Fastpath Server* dialog closes.

8. [Optional] Repeat the previous step to add another FastPath server.

> **Tip:**
>
> HEAT recommends the following practices when assigning FastPath servers:
>
> - Add the HEAT PatchLink DataCenter server itself as a FastPath server. This practice ensures that if all other FastPath servers cannot be validated, the agent can still communicate with the server.
> - Because FastPath servers do not share cache directories with each other, do not add more than three servers per policy. Adding more servers negates bandwidth conservation.
> - Assign FastPath servers to groups based on geographical location.

9. Click **OK** to close the ***Edit FastPath Servers*** dialog.

10. Finish any desired edits in the agent policy set dialog and click **Save**.

> **Note:** Added FastPath servers are not saved until its parent agent policy set is saved.

Result: Your edits are saved. Your FastPath servers are validated immediately.

Deleting FastPath Servers
When you no longer want to use a FastPath server, delete its entry from the ***Edit FastPath Servers*** dialog.

Delete FastPath Servers from the ***Edit FastPath Servers*** dialog. You can delete FastPath servers when creating or editing an agent policy set.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Agent Policy Sets**.

2. Click the **Edit** icon associated with the agent policy set that contains the FastPath server you want to delete.

   Step Result: The ***Edit a Policy Set*** dialog opens.

3. Under ***Fastpath Servers*** click the **Modify** button adjacent to the **Servers** field.

   Step Result: The ***Edit FastPath Servers*** dialog opens.

4. Click the **Delete** icon associated with the FastPath server you want to delete.

   Step Result: A dialog opens asking you to acknowledge the deletion.

5. Acknowledge the deletion by clicking **OK**.

Result: The FastPath server is deleted.

HEAT®software

Exporting Data for Agent Policy Sets

Click the toolbar **Export** button to export the list of Agent Policy Sets listed on the ***Agent Policy Sets*** page to a comma-separated value (`.csv`) file. Exporting data lets you work with data in other programs for reporting and analytical purposes.

Data for policy values are also exported. For additional information, refer to Exporting Data on page 37.

Assigning an Agent Policy Set to a Group

Assigning an Agent Policy Set to a group defines functional rules for the group.

Prerequisites:

Create an Agent Policy Set. Refer to Creating an Agent Policy Set (Groups Page) on page 199 for details.

Assign Agent Policy Sets to groups from the ***Agent Policy Sets*** view.

Note: Groups that do not have an associated Agent Policy Set assigned, use the **Global System Policy**. Refer to About Agent Policies and Agent Policy Sets on page 217 for additional information.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Agent Policy Sets**.

3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Click **Assign**.

   Step Result: The **Select a Policy Set** list becomes active.

5. Select an agent policy set from the **Select a Policy Set** list.

6. Click the **Save** icon (🖫) to save your changes.

   Step Result: The **Select a Policy Set** list closes and your policy is assigned.

   Note: The **Cancel** icon (🖫) cancels your changes and any edits are not saved.

Result: The policy set is saved and associated with the group.

Unassigning an Agent Policy Set from a Group

When desired, you can unassign an Agent Policy Set from a group.

Prerequisites:

An Agent Policy Set is assigned. Refer to Assigning an Agent Policy Set to a Group on page 197 for details.

Unassign the Agent Policy Sets to groups from the ***Agent Policy Sets*** view.

Note: Groups that do not have an associated Agent Policy Set assigned, use the **Global System Policy**. Refer to About Agent Policies and Agent Policy Sets on page 217 for additional information.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. From the **View** list, select **Agent Policy Sets**.

3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Remove the desired policy sets.

   Use one of the following methods.

Method	Steps
To remove one Agent Policy Set:	Click the **Unassign** icon (⟳) associated with the Agent Policy Set you want to remove.
To remove multiple Agent Policy Sets:	1. Select the check boxes associated with the Agent Policy Sets you want to remove. 2. From the toolbar, click the **Unassign** button.

   Note: An **Unassign Disabled** icon indicates you cannot remove an inherited Agent Policy Set. Instead, you must change the group policy inheritance setting or remove the inherited policy set from the parent group. Refer to *Policy Inheritance* in Editing Group Settings on page 212 for additional information.

   Step Result: A dialog appears, prompting you to acknowledge the removal.

5. Click **OK**.

   Step Result: The selected policy set(s) are removed and the dialog closes.

Result: The Agent Policy Set(s) are no longer associated with the group.

HEAT software

Chapter

10

Managing HPL Users and Roles

In this chapter:

- The Users and Roles Page
- The Users Tab
- Working with Users
- The Roles Tab
- Working with Roles

User and role management features let you add, edit, and delete HEAT PatchLink DataCenter for Microsoft® System Center users, and also assign users access rights.

Create, configure, and manage users and roles from the *Users and Roles* page.

The Users and Roles Page

This page lets you view and manage *Users* and *Roles*. Users are a name or title used to log in to the HEAT PatchLink DataCenter for Microsoft System Center Web console. Roles defines the functions and pages that are available to a user and includes access rights to groups and endpoints.

Existing users and user roles are listed on the *Users* and *Roles* tab:

Tools > Users and Roles						▲ Hide Filters
Username:		**Role:**				
		--- All --- ▾	Update View			

Users	Roles

	⊘ Remove	✕ Delete	Create...	Change Password...	Validate Users	▦ Export		Options ▾

☐	Action	Name ▲	Full Name	Role	First Login	Last Login
☐	🖉	AUTO1\TestRunner		Administrator	7/14/2015 4:10:46 PM (Local)	7/24/2015 11:22:37 AM (Local)
☐	🖉🔄	Test Walker		Operator		

Rows per page: 100 ▾	0 of 2 selected	Page 1 of 1 |◀ 1 ▶|
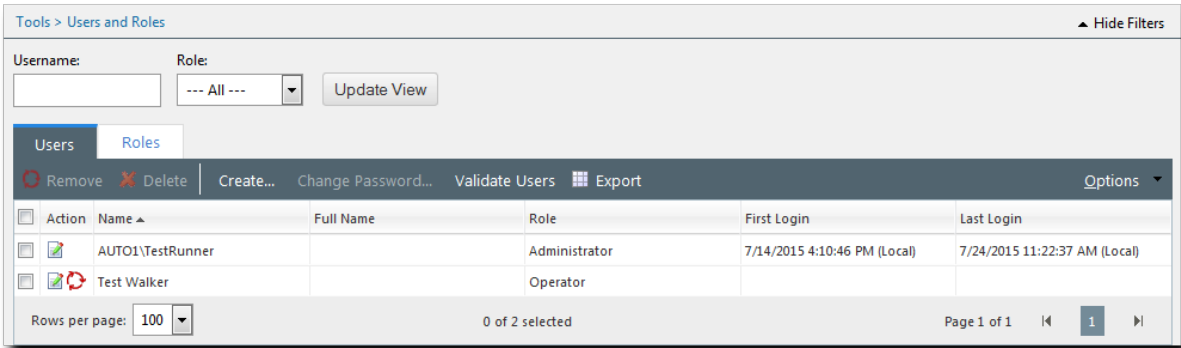
Figure 47: Users and Roles Tabs

Viewing the Users and Roles Page

Navigate to this page to create and manage users and user roles.

You can access this page using the navigation menu.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Security** > **Users and Roles**.

2. Select a tab based on the task you want to accomplish:

    - To work with users, select the **Users** tab.
    - To work with roles, select the **Roles** tab.

3. [Optional] Complete a task.

    - To complete a user task, refer to Working with Users on page 262.
    - To complete a roles task, refer to Working with Roles on page 283.

User Access

HEAT PatchLink DataCenter for Microsoft System Center supports the establishment of security policies that conform to your network needs. Two mechanisms determine security access: Windows-based authentication and HEAT PatchLink DataCenter for Microsoft System Center access rights.

Windows Authentication

Access to HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) is controlled by the Windows operating system authentication of local groups.

Note: Users who have access to HEAT PatchLink DataCenter are members of the local Windows group, `PLUS Admins`. Members of this group have specific registry and file permissions to use the HEAT PatchLink DataCenter application.

HEAT PatchLink DataCenter Access Rights

After a user logs in to HEAT PatchLink DataCenter, the system authenticates the user based on their assigned role. If a user does not have access to a given HEAT PatchLink DataCenter page or function, an access denied message displays, or the feature is simply unavailable.

On the **Users and Roles** page, the **Users** tab is where you create and manage users, and the **Roles** tab is where you create and manage HEAT PatchLink DataCenter roles.

The Users Tab

This tab lets you create and manage HEAT PatchLink DataCenter for Microsoft System Center users.

The tab displays user details and allows you remove, delete, create, and modify a user. This includes changing an assigned user role.
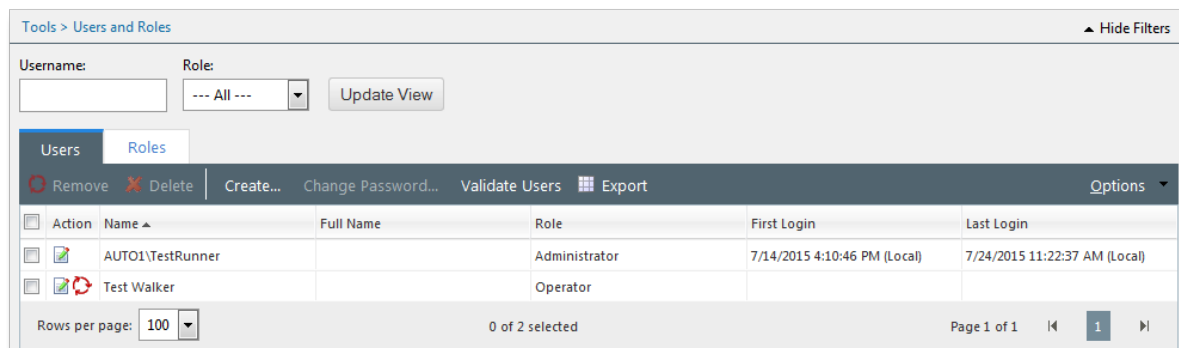
Figure 48: Users Tab

About Users

Users are names or titles that are used to log in to the HEAT PatchLink DataCenter for Microsoft System Center Web console. Users can be defined as individuals (John Smith) or conceptual users (Quality Assurance Manager).

A user profile includes access credentials (user name and password) and the role assigned to the user. A user can be assigned only one role at a time, but multiple users can share a user role which defines the functions and pages that are available to them.

There are two methods of introducing users to the system: creating users and adding users.

Creating New Users	When a user is created, that user is added to both HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) database and Windows. Additionally, new users assigned the **Manage Users** access right are added to the Windows Administrators group; without addition to this group, the user would be unable to modify other users.

HEAT software

Adding Existing Windows Users	You can grant existing Windows users (both local users and domain users) access to HEAT PatchLink DataCenter. Using this method, you can search Windows for existing users and add them to HEAT PatchLink DataCenter. Additionally, added users assigned the **Manage Users** access right are added to the Windows Administrators group; without addition to this group, the user would be unable to modify other users.

Note: Microsoft IIS Web server software, used by HEAT PatchLink DataCenter, does not support user names or passwords in languages that require unicode characters (such as Korean or Kanji).

The Users Tab Toolbar

This toolbar contains buttons that let you create and manage users.

The following table describes the function of each toolbar button.

Table 108: Users Tab Toolbar

Button	Function
Remove	Removes the selected user. Removing a user removes it from HEAT PatchLink DataCenter for Microsoft System Centerwithout deleting that user account within Windows. For additional information, refer to Removing Users on page 267.
Delete	Deletes the selected user. Deleting a user removes it from HEAT PatchLink DataCenter for Microsoft System Center and Windows. For additional information, refer to Deleting Users on page 269.
Create...	Creates a new user. For additional information, refer to Creating New Users on page 262.
Change Password...	Changes the password for the selected user. For additional information, refer to Changing a User Password on page 270.
Validate Users	Removes HPL users that cannot be found in: • Your domain (if the HEAT Patch Manager DataCenter Server can contact it). • The HEAT Patch Manager DataCenter Server local **PLUS Admins** user group. For additional information, refer to Validating Users on page 271.

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Users Tab List

This list displays each user role within the system. Use the list icons to edit or remove users. Additionally, you can also filter the lists to display only specified roles.

The following table describes the **Users** tab list columns.

Table 109: Users Tab List

Column	Description
Action	Contains **Edit** and **Remove** icons. Use these icons to edit or remove the associated user. For additional information, refer to one of the following topics: • Editing Users on page 265 • Removing Users on page 267
Name	The name of user.
Full Name	The full name of the user.
Role	The role assigned to the user.
First Login	The date and time in which the user first logged in.
Last Login	The date and time in which the user last logged in.

HEAT®software

Working with Users

To perform tasks associated with users, click a toolbar button or list icon. To perform some tasks, selecting one or multiple users from the list may be necessary.

Creating New Users

You can create a new user when you need to allow a person within your organization access to HEAT PatchLink DataCenter for Microsoft System Center Web console.

Create new users from the **Users** tab.

> **Note:** New users are added to both HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) and Windows. Refer to User Access on page 258 for additional information.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Security** > **Users and Roles**.

2. Ensure the **Users** tab is selected.

3. Click **Create**.

   Step Result: The **Create User Wizard** opens.

4. Ensure the **Creating a new local user** option is selected.

5. Click **Next**.

   Step Result: The **New user information** dialog opens.

6. Define the user credentials.

> **Tip:** The * indicates a required field.

Type the applicable information in the following fields.

Field Name	Description
User name	The desired user name.
	Note: The user name must be a unique name. It must be between 1-20 characters in length and cannot include any of the following characters:
	• ' \ " @ ^ % & { } ( ) [ ] ; < > ! # : ? / = |
Password	The desired password.
	Note: The **Password Strength** indicator factors password effectiveness based on password length, complexity, character variety, and common word resemblance. Strong passwords contain eight characters or greater and combine symbols, numbers, uppercase letters, and lowercase letters. Also, they do not resemble common words or names, including words with numbers in place of letters.
Confirm Password	The password retyped.

7. From the **Select a Role** list, select the desired role.

Select from the following roles:

- **Administrator**
- **Manager**
- **Operator**
- **Guest**
- *Custom Role(s)*

> **Note:** *Custom Role(s)* are only available if a custom role has been created. Refer to Custom Roles on page 274 for additional information.

8. [Optional] Define the user information.

Type applicable information in the following fields.

Field Name	Description
Description	The description of the user.
Full name	The full name of the user.

HEAT®software

Field Name	Description
Office phone	The office phone number of the user.
Cell phone	The cell phone number of the user.
Pager	The pager number of the user.
E-mail	The email address of the user.

9. Click **Finish**.

Step Result: The *Creation Summary* dialog opens indicating you have successfully created a user.

> **Note:** In the event that user creation requirements are not met, you receive a notification message or in the event of password failure the *Creation Summary* dialog opens to display the error. You must resolve these errors to successfully create a user.

10. Click **Close**.

Step Result: The *Creation Summary* dialog closes.

Result: The new user is created and is displayed on the *User Tab* list. The new user can now access all authorized features of HEAT PatchLink DataCenter.

You may edit the user from the *Users* tab. Refer to Editing Users on page 265.

Adding Existing Windows Users

You can create a user by adding a pre-existing Windows domain or local user. Add this type of user when they need to access to HEAT PatchLink DataCenter for Microsoft System Center Web console.

Add existing Windows users from the *Users* tab.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Security** > **Users and Roles**.

2. Click **Create**.

Step Result: The *Create User Wizard* opens.

3. Select the **Adding existing local or domain users** option.

4. Click **Next**.

Step Result: The *Existing user* dialog opens.

5. In the **Search for the following users** field, type a user name, or the beginning characters of one or more user names.

   Use semicolons to separate user names. To search for users within a specific domain, prefix the user name with the domain. Example, (*DOMAINNAME\UserName*).

   Note: There must be a secure connection between the domain and the HEAT PatchLink DataCenter's domain, or the user will be unable to access HEAT PatchLink DataCenter.

6. Click **Next.**

   Step Result: The *User Roles* dialog opens.

7. From the **Select a Role** list, select the desired role.

   Select from the following roles:

   - **Administrator**
   - **Manager**
   - **Operator**
   - **Guest**
   - *Custom Role(s)*

   Note: *Custom Role(s)* are only available if a custom role has been created. Refer to Custom Roles on page 274 for additional information.

8. Click **Finish**.

   Step Result: The *Creation Summary* dialog opens indicating you have successfully created a user.

   > **Note:** In the event that user creation requirements are not met, you receive a notification message or in the event of password failure the *Creation Summary* dialog opens to display the error. You must resolve these errors to successfully create a user.

9. Click **Close**.

   Step Result: The *Creation Summary* dialog closes.

Result: The new user is created and is displayed on the *User Tab* list. The new user can now access all authorized features of HEAT PatchLink DataCenter.

You may edit the user from the *Users* tab. Refer to Editing Users on page 265.

Editing Users

Edit existing HEAT PatchLink DataCenter for Microsoft System Center users to change their assigned role or contact information.

Edit users from the *Users* tab.

HEAT software

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Security** > **Users and Roles**.

2. Ensure the *Users* tab is selected.

3. Find the desired user(s).

   Use one of the following methods.

Method	Steps
To search for user(s) by name:	1. Type an applicable name in the **Username** field. 2. Click **Update View**.
To search for user(s) by role:	1. Select the applicable role from the **Role** drop-down list. 2. Click **Update View**.

   Step Result: The user list updates based on your search.

4. Click the **Edit** icon associated with the user you want to edit.

   Step Result: The *Edit User* dialog opens.

Figure 49: Edit User Dialog

5. [Optional] Edit the **Full name** field.

6. [Optional] Select a new role from the **Role** list.

   Select one of the following roles:

   - **Administrator**
   - **Manager**
   - **Operator**
   - **Guest**
   - *Custom Role(s)*

   Note: *Custom Role(s)* are only available if a custom role has been created.

7. [Optional] Edit the following fields.

Field Name	Description
Office phone	The user's office phone number.
Cell phone	The user's cell phone number.
Pager	The user's pager number.
E-mail	The user's email address.
Description	The user's description.

8. Click **Next**.

   Step Result: The *Edit Confirmation* dialog opens.

9. Click **Finish**.

   Step Result: The *Edit Summary* dialog opens.

10. Click **Close**.

   Step Result: The *Edit Summary* dialog closes.

Result: The user is updated according to your changes.

Removing Users

Removing a user account removes it from HEAT PatchLink DataCenter for Microsoft System Center without deleting that user account within Windows or in Active Directory.

Remove users when you want to prevent a user from logging in to HEAT PatchLink DataCenter for Microsoft System Center, (HEAT PatchLink DataCenter) but want the user to still to have a Windows

HEAT software

(local) account. Once removed, the user is removed from the HEAT PatchLink DataCenter endpoint groups and the user list on the ***Users and Roles*** page.

> **Note:** For additional information on deleting users (deleting removes them from both HEAT PatchLink DataCenter and Windows), refer to Deleting Users on page 269.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Security** > **Users and Roles**.

2. Ensure the ***Users*** tab is selected.

3. Find the desired user(s).

    Use one of the following methods.

Method	Steps
To search for user(s) by name:	1. Type an applicable name in the **Username** field. 2. Click **Update View**.
To search for user(s) by role:	1. Select the applicable role from the **Role** drop-down list. 2. Click **Update View**.

   Step Result: The user list updates based on your search.

4. Remove the desired user(s).

> **Important:** You cannot remove users assigned the **Administrator** role. You must first edit the user, change the role, then remove the user.

    Use one of the following methods.

Method	Steps
To remove a single user:	Click the **Remove** icon associated with the user you want to remove.
To remove multiple users:	1. Select the check boxes associated with the users you want to remove. 2. From the toolbar, click the **Remove** button.

   Step Result: A dialog displays, asking you to acknowledge the removal.

5. Acknowledge the removal by clicking **OK**.

Result: The user is removed from HEAT PatchLink DataCenter for Microsoft System Center. You can re-add the removed user at any time if the user's Windows account still exists.

Deleting Users

Delete a user when you want to remove it from both HEAT PatchLink DataCenter for Microsoft System Center and Windows.

Deleting users removes them from both HEAT PatchLink DataCenter and Windows (locally), whereas removing users only removes them from HEAT PatchLink DataCenter.

Note: Refer to Removing Users on page 267 for additional information on how to remove a user.

Delete users from the *Users and Roles* page *Users* tab.

Important: You cannot delete users assigned the **Administrator** role. You must first change the role type by editing the user, then you may remove the user.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Security** > **Users and Roles**.

2. Ensure the **Users** tab is selected.

3. Find the desired user(s).

   Use one of the following methods.

Method	Steps
To search for user(s) by name:	1. Type an applicable name in the **Username** field. 2. Click **Update View**.
To search for user(s) by role:	1. Select the applicable role from the **Role** drop-down list. 2. Click **Update View**.

   Step Result: The user list updates based on your search.

4. Select the user(s) you want to delete.

5. Click **Delete**.

   Caution: Deleting a user deletes them from both HEAT PatchLink DataCenter and Windows (locally).

   Step Result: A dialog displays, asking you to acknowledge the deletion.

6. Acknowledge the deletion by clicking **OK**.

Result: The user is deleted from both HEAT PatchLink DataCenter and Windows (locally).

Note: Deleting a HEAT PatchLink DataCenter user that was added from your Active Directory will not delete the Windows user account within Active Directory. The account will only be removed from HEAT PatchLink DataCenter.

HEAT®software

Changing a User Password

Change a password for security reasons or if a user has forgotten theirs.

Prerequisites:

You have the **Change Password** access right. Refer to Defining Access Rights on page 69 for additional information on this access right that allows you edit other user's passwords.

Change user passwords from the *Users* tab.

Note: Changing a user's password in HEAT PatchLink DataCenter for Microsoft System Center also changes the user's Windows password on the HEAT PatchLink DataCenter for Microsoft System Center server or in Active Directory.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Security** > **Users and Roles**.

2. Ensure the *Users* tab is selected.

3. Find the desired user(s).

   Use one of the following methods.

Method	Steps
To search for user(s) by name:	1. Type an applicable name in the **Username** field. 2. Click **Update View**.
To search for user(s) by role:	1. Select the applicable role from the **Role** drop-down list. 2. Click **Update View**.

   Step Result: The user list updates based on your search.

4. Select the user whose password you want to change.

   Tip: You may only select a single user at a time to change passwords.

5. Click **Change Password**.

   Step Result: The *Change password for* dialog opens.

6. Type a new password in the **New Password** field.

   The **Password Strength** indicator factors your password security based on length, complexity, character variety, and common word resemblance.

Strong passwords contain eight characters or greater and combine symbols, numbers, and letters (both upper and lowercase). Also, they do not resemble common words or names, including words with numbers in place of letters.

Attention: Passwords must adhere to Windows local and/or domain password policies.
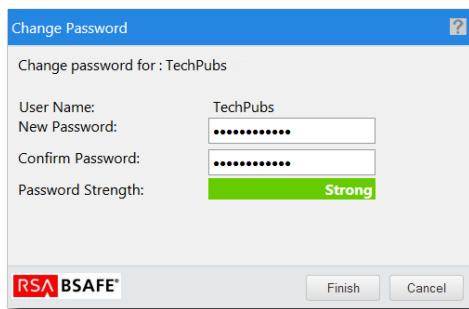
Figure 50: Change My Password Dialog

7. Retype the password in the **Confirm Password** field.

8. Click **Finish**.

Result: The password for the user is changed.

Validating Users

Over time, staff who use HPL move on from your enterprise. This attrition can create orphaned user accounts in the HPL system. Instead of manually managing user and roles, you can use the **Validate Users** button to revoke access rights for orphaned accounts.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.

2. From the toolbar, click **Validate Users**. Click **OK** to continue.

Note: If HPL can't contact the domain, domain users won't be validated. Retry validation when HPL has domain connectivity.

Result: • User validation synchronization begins. Depending on the number of users in your domain, this process may take up to two minutes.
• Users in HPL that are deleted from either your domain or your HEAT Patch Manager DataCenter Server PLUS Admin local user group are removed from the console.

Note: Only user accounts that are deleted from the domain (or server) have their access rights revoked. Users accounts that are merely disabled remain in the HPL system.

Exporting User Data

You can export the data displayed on the *Users* tab list so that it can be used in other applications. This data is exported to a comma separated value (`.csv`) file.

To export data, click the **Export** button. For additional information, refer to

The Roles Tab

This tab lets you create new roles and manage existing roles. It also lists information about each existing role.

Additionally, you can use this tab to edit roles or remove roles.
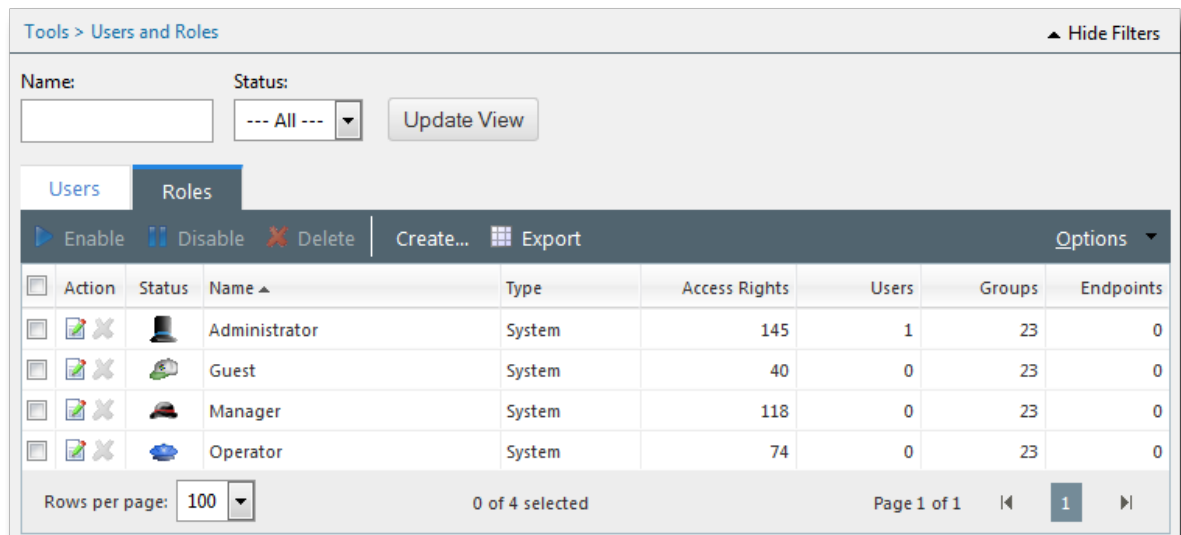
Figure 51: Roles Tab

About Roles

Roles define the functions and pages that are available to a user and include general access rights, group access rights, and endpoint access rights within the HEAT PatchLink DataCenter for Microsoft System Center. Roles can be customized and assigned to users.

The HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) contains two types of roles:

System Roles	These roles are included with the default HEAT PatchLink DataCenter installation. These roles are predefined with access rights appropriate for various user types. System roles cannot be edited or disabled, and by default can access all system groups and endpoints.

| ***Custom Roles*** | These roles are created after HEAT PatchLink DataCenter installation by users with the **Manage Users** access right. Custom roles let you grant users unique sets of access rights. Additionally, these roles let you define specific endpoints and groups that can be accessed and managed. |

The following table describes role attributes.

Table 110: Role Attribute Descriptions

Role Attribute	Description
Access Rights	Define the pages and functions available to the user.
Accessible Groups	Define the specific endpoint groups accessible to the user.
Accessible Endpoints	Define the specific endpoints accessible to the user.

Predefined System Roles

Predefined system roles are the default roles offered by HEAT PatchLink DataCenter for Microsoft System Center. The commonly used access rights selected for these roles are usually adequate for most networks and their users. Additionally, these roles can access and manage all groups and endpoints.

Predefined system roles have the following benefits:

- These roles types and their commonly used access rights are usually adequate for most networks and their users.
- A user assigned a predefined system role has access to all endpoints and groups.
- Users with the **Manage Users** access rights can assign predefined system roles to users.
- A predefined system role can be used as a template for creating a custom role.

The following table describes each predefined system role.

Table 111: Predefined System Role Descriptions

Role	Icon	Description
Administrator		Users with this role have full access to all HEAT PatchLink DataCenter for Microsoft System Center pages and functions. The Administrators role allows you to assign endpoints to other roles. **Important:** At least one user must be assigned the administrator role at all times.
Guest		Users can access pages, but cannot use their functions; this role allows read-only access.
Manager		Users can access pages and functions.

HEAT®software

Role	Icon	Description
Operator	☁	Users can perform all routine functions (detect, export, and so on). Operators usually perform typical daily functions.

Note: A user assigned a system role has access to all endpoints and groups.

Custom Roles

Custom roles are created after HEAT PatchLink DataCenter for Microsoft System Center installation. Custom roles let you grant users unique sets of access rights. Additionally, this role lets you define specific endpoints and groups that can be accessed and managed.

Custom roles have the following benefits:

- You can configure a custom role to restrict access to endpoints and groups.
- You can configure a custom role to restrict access to HEAT PatchLink DataCenter for Microsoft System Center pages and functions.
- Unlike system roles (which cannot be disabled or deleted), you can disable or delete a custom role at any time.
- When creating new custom roles you may use preexisting roles as templates to aid you.
- Custom roles are denoted by the **Wool Hat** icon.

Note: Custom roles are created by users with the **Manage Users** access right.

Defining Access Rights

Access rights are individual privileges that define whether a user can access a system feature. These rights control availability for every HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) page, feature, function, and action. The pages and features available to users are based on the access rights associated with the role assigned to them. The system roles are assigned a default set of access rights. Users inherit the access rights of the role they are assigned.

Access rights begin with read-only access to system pages and permission to export data. At the administrative level, users can be assigned rights to fully manage the various system pages and functions.

Note: New access rights are added when you install new modules.

Access Right	Description	Access
All		👤
Dashboard		
View Dashboard	Access to view the home page dashboard.	👤🎩☁🎩
View Current Status	Access to view the status of the server.	👤🎩☁🎩

Access Right	Description	Access
View HPL Widgets	Access to select and view the HEAT PatchLink DataCenter Dashboard widgets.	👤 🎩 ☁ 💾
Jobs		
View Discovery Scan Jobs	Access to view discovery scan jobs.	👤 🎩
Create Discovery Scan Jobs	Access to create and copy discovery scan jobs	👤 🎩
View Agent Management Jobs	Access to view agent management jobs.	👤 🎩
Create Agent Management Jobs	Access to create and copy agent management jobs.	👤 🎩
Manage Modules via Jobs	Access to install or uninstall agent modules using agent management jobs.	👤 🎩
Manage Jobs	Cancel, pause, resume, delete or merge all jobs the user has access to.	👤 🎩
Export Jobs	Export the jobs list.	👤 🎩
Vulnerabilities/Patch Content		
View Content	Access to vulnerability and other content data.	👤 🎩 ☁ 💾
Manage Content	Enable and disable vulnerabilities and other content.	👤 🎩
Export Content	Export vulnerability and other content data list.	👤 🎩 ☁
View Content Details	Access the detailed information for vulnerabilities and other content data.	👤 🎩 ☁
View My Custom Patch Lists	Access to view custom patch lists that this user has created.	👤 🎩 ☁
View All Custom Patch Lists	Access to view custom patch lists that all users have created.	👤
Manage Custom Patch Lists	Edit, delete or copy custom patch lists that this user has access to.	👤 🎩 ☁
Endpoints		
View Endpoints	Access the manage endpoints all tab.	👤 🎩 ☁ 💾

HEAT software

Access Right	Description	Access
Manage All Tab	Enable and disable agents, delete endpoints, manage agent modules, and wake endpoints.	
Export All Tab	Export the all tab endpoints list.	
Manage Remotely	Access the remote management options available.	
View HPL Tab	Access the HEAT PatchLink DataCenter tab.	
Manage HPL Tab	Install, uninstall, enable and disable the HEAT PatchLink DataCenter module.	
Export HPL Tab	Export the HEAT PatchLink DataCenter tab endpoints list.	
Download Agent Installers	Access to the Download Agent Installers page.	
Manage Agent Version	Access to the Manage Agent Version dialog.	
Scan Now Discover Applicable Updates	Scan endpoints using the DAU Scan Now Dropdown/button.	
Reboot Endpoints	Reboot endpoints using the Reboot Now button.	
Inventory		
View Inventory	View the endpoint inventory.	
Export Inventory	Export the endpoint inventory list.	
Groups		
View Groups	Access the groups.	
Manage Groups	Add, edit, enable, disable, and delete groups.	
Export Groups	Export the groups list.	
Users		
View Users	Access the user groups.	
Manage Users	Add or remove users from individual user policies.	
Export Users	Export the user groups list.	
Deployments and Tasks		

Access Right	Description	Access
Create Deployments	Ability to create new deployments.	🖥️🎩☁️
View My Deployments and Tasks	Access the deployments and tasks that this user has created.	🖥️🎩☁️💾
View All Deployments	Access the deployments that all users have created.	🖥️🎩☁️
Manage Deployments and Tasks	Deploy, enable, disable, abort, and delete deployments and tasks that this user has access to.	🖥️🎩☁️
Export Deployments and Tasks	Export the deployments and tasks in the list that this user has access to.	🖥️🎩☁️
Packages		
View Packages	Access the package data.	🖥️🎩☁️💾
Manage Packages	Create, edit, and delete packages.	🖥️🎩
Export Packages	Export the package data list.	🖥️🎩☁️
Cache Packages	Ability to download packages from the GSS onto the local machine.	🖥️🎩
Agent Policy Sets		
View All Agent Policy Sets	Access the agent policy sets.	🖥️🎩☁️💾
Manage All Agent Policy Sets	Create, edit and delete agent policy sets.	🖥️
Export All Agent Policy Sets	Export the agent policy sets list.	🖥️🎩
Security Configuration Management		
View SCM Data	Acess to view SCM data on the endpoint detail and groups views.	🖥️
Reports		
Reports Administer	Generate reports regardless of access rights for groups and endpoints.	🖥️
View My Core Reports	Generate core reports only for those items this user has access to.	🖥️🎩☁️💾

HEAT software

Access Right	Description	Access
View My HPL Reports	Generate HEAT PatchLink DataCenter reports only for those items this user has access to.	
Export Reports	Export the generated reports.	
Configure Enterprise Reporting (ER)	Configure settings to manage Configure Enterprise Reporting (ER)	
Users/Roles		
View Users	Access the users and roles list view.	
Manage Users	Create, delete, enable, and disable users and roles.	
Export Users	Export the users and roles list.	
Change Password	Ability to change the password for users other than themselves.	
Manage Server Modules		
Installation Manager	Access the Installation Manager to install, update and uninstall server modules.	
Subscriptions		
View Subscription	Access the subscription service information.	
Manage Subscription	Edit or update subscription service updates.	
Export Subscription	Export the subscription service information.	
Directory/Computer Synchronization		
View Directory Sync Schedule	Access to view the active directory sync schedule page.	
Manage Directory Sync Schedule	Create, edit, delete, enable, disable directory syncs.	
Export Directory Sync Schedule	Export the directory sync schedule lists.	
Email notifications		
View Email Notifications	Access the email notifications page.	

Access Right	Description	Access
Manage Email Notifications	Create and edit email notifications and settings for core feature. Note: All types of notifications may be deleted with this right.	🖳
Manage HPL Email Notifications	Create and edit HEAT PatchLink DataCenter email notifications and settings. Note: All types of notifications may be deleted with this right.	🖳
Export Email Notifications	Export the emails notifications list.	🖳 ⛟
Options		
View Options	Access to general, agent and deployment default server options.	🖳 ⛟ ☁ 🖥
Manage Options	Set and edit general, agent and deployment default server options.	🖳
Export Options	Export the options list.	🖳 ⛟
Technical Support		
View Technical Support	Access the technical product support information.	🖳 ⛟ ☁ 🖥
Export Technical Support	Export the technical product support information.	🖳 ⛟ ☁
Licenses		
View Licenses	Access the product licenses.	🖳 ⛟ ☁ 🖥
Manage Licenses	Update product licenses.	🖳
Export Licenses	Export the product license information.	🖳 ⛟

Defining Accessible Groups

Accessible groups are specific groups of endpoints that a particular role can access and manage. Use this feature for granularity when assigning roles to users.

Accessible groups are only applicable to custom user roles.

Note: The **Accessible Groups** feature is disabled when working with a predefined system role. System roles can access all groups and endpoints within the system.

This feature allows you to restrict a user to specified groups. For example, a user assigned the access right to manage deployments can be limited to managing deployments for select groups.

HEAT software

The **Accessible Groups** feature is defined on the *Groups* tab in both the *Create Role* dialog and the *Edit Role* dialog.
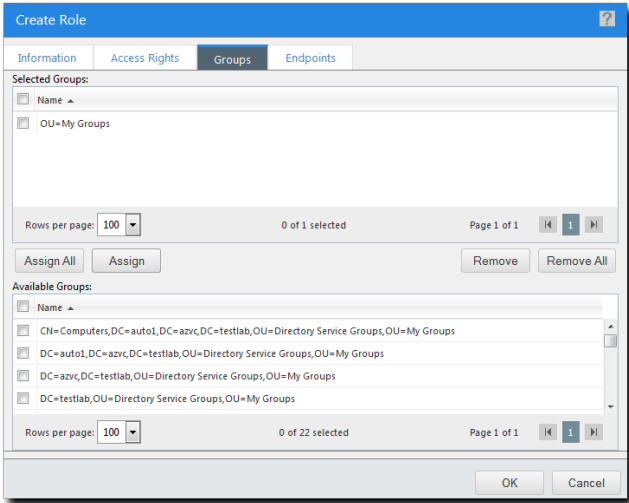
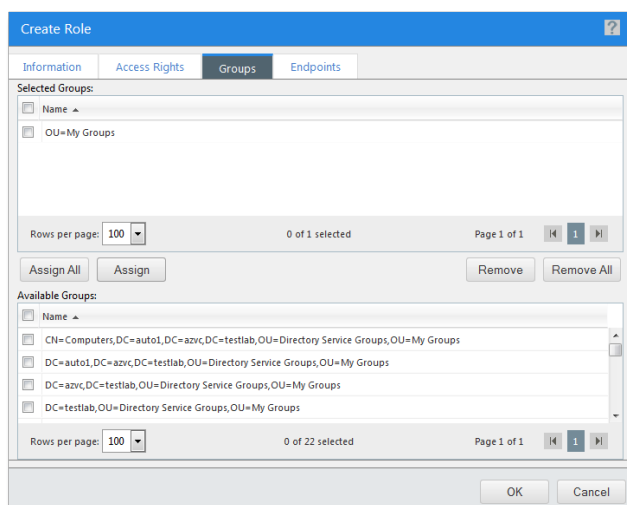Figure 52: Roles Dialog Group Tab

The *Groups* tab contains the following lists, which are used to control what groups are associated with a particular role:

Table 112: Groups Tab List Descriptions

List	Description
Selected Groups	Lists the groups assigned to the role.
Available Groups	Lists the available groups that can be assigned to the role.

Defining Accessible Endpoints

Accessible Endpoints are specific endpoints that a particular role can access and manage. This feature is similar to the **Accessible Groups** feature; it allows for granularity when assigning roles to system users.

Accessible endpoints are only applicable to custom user roles.

Note: The **Accessible Endpoints** feature is disabled when working with predefined system roles. System roles can access all groups and endpoints within the system.

As mentioned, this feature lets you define specific endpoints that users associated with the role can access and manage. For example, you can limit a user assigned the **Manage Endpoints** access right to management of a single endpoint.

This feature is are defined on the **Endpoints** tab in both the **Create Role** dialog and the **Edit Role** dialog.

Figure 53: Roles Dialog Endpoints Tab

The **Endpoints** tab contains the following lists, which are used to control which endpoints are associated with a role:

Table 113: Endpoint Tab List Descriptions

List	Description
Selected Endpoints	Lists the endpoints assigned to the role.
Available Endpoints	Lists the available endpoints that can be assigned to the role.

The Roles Tab Toolbar

This toolbar contains buttons that let you create and manage user roles.

The following table describes the function of each **Roles** tab toolbar button.

Table 114: Roles Tab Toolbar

Button Name	Function
Enable	Enables the selected disabled custom role. For additional information, refer to Enabling User Roles on page 287.
Disable	Disables the selected custom role. For additional information, refer to Disabling User Roles on page 286.
Delete	Deletes the selected custom role. For additional information, refer to Deleting User Roles on page 287.

HEAT®software

Button Name	Function
Create...	Creates a new user role. For additional information, refer to Creating User Roles on page 283.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Roles Tab List

This list displays all user roles that exist within HEAT PatchLink DataCenter for Microsoft System Center. Use the action icons to manage roles. Additionally, this list can be filtered to display only specified roles.

The following table describes each *Roles* tab list column.

Table 115: Roles Tab List

Column	Description
Action	Contains **Edit** and **Delete** icons. Use these icons to edit or delete the associated role. For addition information, refer to one of the following topics: • Editing User Roles on page 284 • Deleting User Roles on page 287
Status	Contains an icon that indicates the type of role. For additional information, refer to one of the following topics: • Predefined System Roles on page 273 • Custom Roles on page 274
Name	The name of the user role.
Type	The type of user role (`System` or `Custom`).
Access Rights	The number of access rights assigned to the role.
Users	The number of users assigned to the role.
Groups	The number of accessible groups assigned to the role.
Endpoints	The number of accessible endpoints assigned to the role.

Working with Roles

To perform tasks associated with roles, click a toolbar button or a list icon. To perform some tasks, selecting one or multiple roles from the list may be necessary.

- Creating User Roles on page 283
- Editing User Roles on page 284
- Disabling User Roles on page 286
- Enabling User Roles on page 287
- Deleting User Roles on page 287
- Exporting User Role Data on page 288

Creating User Roles

Custom roles let you select individual access rights, accessible groups, and accessible endpoints for that role. Create a custom role when predefined system roles do not contain the access rights needed for a particular user. Creating a custom role is also useful when you require a role that can only access specific groups or endpoints.

Create custom roles from the **Roles** tab.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Security** > **Users and Roles**.

2. Select the **Roles** tab.

3. Click **Create**.

   Step Result: The **Create Role** dialog opens to the **Information** tab.

4. Type a name in the **Name** field.

5. Type a description in the **Description** field.

6. Select a role template from the **Role Template** list.

   Any existing role can be used as a template. The selected role determines initial access rights. You can later change which access rights are assigned to the role.

7. Select the **Access Rights** tab.

8. Select or clear the desired access rights.

   For additional information, refer to Predefined System Roles on page 273.

   Tip: Select or clear the **All** check box to globally select or clear all access rights. Additionally, child access rights are unavailable until their parent access rights are selected.

9. Select the **Groups** tab.

HEAT software

10. Assign the desired accessible endpoint groups to the role.

Use one of the following methods to assign groups.

Method	Steps
To assign individual groups:	1. From the **Available Groups** table, select the check box(es) associated with the group(s) you want to assign. 2. Click **Assign**.
To assign all groups:	Click **Assign All**.

Tip: Remove groups using **Remove** and **Remove All**.

11. Select the *Endpoints* tab.

12. Assign the desired accessible endpoints to the role.

Use one of the following methods to assign endpoints.

Method	Steps
To assign individual endpoints:	1. From the **Available Endpoints** table, select the check box(es) associated with the endpoint(s) you want to assign. 2. Click **Assign**.
To assign all endpoints:	Click **Assign All**.

Tip: Remove endpoints using **Remove** and **Remove All**.

13. Click **OK**.

Result: Your new role is saved. It can now be assigned to users. Additionally, it can be edited from the *Users and Roles* page **Roles** tab.

Editing User Roles

Edit a custom user role as the needs of users associated with the role change. You can only edit custom roles (predefined system roles cannot be edited).

Edit roles from the *Roles* tab.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Security** > **Users and Roles**.

2. Select the *Roles* tab.

3. Click the **Edit** icon associated with the role you want to edit.

Step Result: The *Edit Role* dialog opens to the *Information* tab.

4. Define the *Information* tab content.

   a) The **Name field** is a read-only and cannot be edited.

   b) [Optional] Edit the **Description** field.

> **Tip:** The optional description can be simple or detailed and may include information concerning the access right you are editing for the specific role.

   c) [Optional] Select a role template from the **Role Template** drop-down list.

> **Tip:** Any existing role can be used as a template. The selected role determines initial access rights. You can later change which access rights are assigned to the role.

5. Select the *Access Rights* tab.

6. [Optional] Selecting or clear the desired access rights.

> **Tip:** Select or clear the **All** check box to globally select or clear all access rights. Additionally, child access rights are unavailable until their parent access rights are selected.

7. Select the *Groups* tab.

8. [Optional] Assign accessible endpoint groups to the role.

   Use one of the following methods to assign groups.

Method	Steps
To assign individual groups:	1. From the **Available Groups** table, select the check box(es) associated with the group(s) you want to assign. 2. Click **Assign**.
To assign all groups:	Click **Assign All**.

9. [Optional] Remove accessible endpoint groups from the role.

   Use one of the following methods to remove groups.

Method	Steps
To remove individual groups:	1. From the **Selected Groups** table, select the check box(es) associated with the group(s) you want to remove. 2. Click **Remove**.
To remove all groups:	Click **Remove All**.

10. Select the *Endpoints* tab.

HEAT®software

11. [Optional] Assign accessible endpoints to the role.

Use one of the following methods to assign endpoints.

Method	Steps
To assign individual endpoints:	1. From the **Available Endpoints** table, select the check box(es) associated with the endpoint(s) you want to assign. 2. Click **Assign**.
To assign all endpoints:	Click **Assign All**.

12. [Optional] Remove accessible endpoints from the role.

Use one of the following methods to remove endpoints.

Method	Steps
To remove individual endpoints:	1. From the **Selected Endpoints** table, select the check box(es) associated with the endpoint(s) you want to remove. 2. Click **Remove**.
To remove all endpoints:	Click **Remove All**.

13. Click **OK**.

Result: Your edits are saved. The edited role is applied to all associated users.

Editing User Roles
Within HEAT PatchLink DataCenter for Microsoft System Center, you can edit custom user roles, which can be assigned to users with unique access requirements.

Complete the dialog by defining the setting on each tab.

Disabling User Roles

You can disable any custom role, allowing you to maintain the role within HEAT PatchLink DataCenter for Microsoft System Center without assigning it to users. You can enable, edit, and delete disabled roles. Disabled roles appear unavailable.

Disable roles from the *Roles* tab.

Note: You cannot disable system roles: **Administrator**, **Manager**, **Operator**, **Guest**.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Security** > **Users and Roles**.

2. Select the *Roles* tab.

3. Select the check box(es) associated with the enabled custom role(s) you want to disable.

4. Click **Disable**.

Result: The selected role(s) is disabled.

> **Caution:** If you disable a role currently assigned to a user, they can still log in to HEAT PatchLink DataCenter for Microsoft System Center, but their access rights are heavily restricted.

Enabling User Roles

Enable roles when you want to reactive them.

Prerequisites:

The role is a custom role and is disabled.

> **Note:** You cannot disable system roles: **Administrator**, **Manager**, **Operator**, **Guest**.

Enable roles from the *Roles* tab.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Security** > **Users and Roles**.

2. Select the *Roles* tab.

3. Find the desired role(s).

    a) Select `Disabled` from the **Status** drop-down list.

> **Note:** Custom role(s) must have a status of `Disabled` to be enabled.

    b) Click **Update View**.

    Step Result: The role list updates based on your search.

4. Select the check box associated with the disabled role(s) you want to enable.

5. Click **Enable**.

Step Result: The role is disabled and the denoted **Wool Hat** (🎩) icon is active again.

Result: The selected role(s) is enabled. You can now assign it to users.

> **Note:** Users already assigned the previously disabled role will again be able to access HEAT PatchLink DataCenter for Microsoft System Center with their full access rights.

Deleting User Roles

Delete custom user roles when they are no longer needed. You can delete roles regardless of whether they are enabled or disabled.

Delete custom roles from the *Roles* tab.

> **Note:** You cannot delete system roles: **Administrator**, **Manager**, **Operator**, **Guest**.

HEAT software

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Security** > **Users and Roles**.

2. Select the **Roles** tab.

3. Find the desired user(s).

   Use one of the following methods.

Method	Steps
To search for roles(s) by name:	1. Type an applicable name in the **Name** field. 2. Click **Update View**.
To search for user(s) by role:	1. Select the applicable role from the **Status** drop-down list. 2. Click **Update View**.

   Step Result: The role list updates based on your search.

4. Delete the desired roles.

   Use one of the following methods.

Method	Steps
To delete a single user role:	1. Click the **Delete** icon associated with the role you want to delete. 2. Click **OK** to acknowledge the deletion.
To delete multiple user roles:	1. Select the check boxes associated with the user roles that you want to delete. 2. From the toolbar, click the **Delete** button. 3. Click **OK** to acknowledge the deletion.

Note: You cannot delete system roles: **Administrator**, **Manager**, **Operator**, **Guest**.

Result: The role is deleted.

> **Caution:** If you delete a role currently assigned to a user, they can still log in to HEAT PatchLink DataCenter for Microsoft System Center, but their access rights are heavily restricted.

Exporting User Role Data

You can export the data displayed on the **Roles** tab list so that it can be used in other applications. This data is exported to a comma-separated value (.csv) file.

To export data, click the **Export** button. For additional information, refer to Exporting Data on page 37.

Chapter

11

Managing Deployments and Tasks

In this chapter:

- About Deployments
- The Deployments and Tasks Page
- Working With Deployments and Tasks
- Using the Deployment Wizard
- The Deployment Details Page
- Deployment Details for Package

Within HEAT PatchLink DataCenter for Microsoft® System Center, a *deployment* initiates the download of security content by the agent to an endpoint for installation. It is the instruction set for a package, supplying an agent with the rules and conditions for deployment.

A deployment comprises all the information needed to perform the task(s) associated with the content. This includes required files and scripts for installing content, stopping a service, validating a system condition, or changing a database entry. The deployment is the mechanism that carries and supports a package.

A *task* is a deployment that initiates a system task. It contains no software or patches. Use tasks to reboot network endpoints or initiate DAU tasks.

About Deployments

The term *deployment* refers to the process of sending content items to managed endpoints.

Several key concepts and status indicators are associated with a deployment. These concepts are used to define deployment behavior.

The following topics include some of the key concepts and indicators that give definition to a deployment.

Topic	Description
Explaining Deployment Distribution Order on page 290	The order that the deployment is submitted to target endpoints.
Deployment Types on page 290	Deployments can be based on content, packages, or a Mandatory Baseline.
Standard and Chained Deployments on page 291	Deployments are processed as either standard or chained.

◢HEAT®software

Explaining Deployment Distribution Order

When deploying more than one package to an individual endpoint or group of endpoints, the deployments can be scheduled to process at different times. Order is also influenced by deployment type, status, and reboot requirements.

Important: You must install an agent on an endpoint in order to deploy content to the endpoint. A deployment is assigned to the agent installed on an endpoint.

Deployments proceed in the following order prior to regularly scheduled system tasks and agent processes:

1. Chained deployments
2. Standard deployments
3. System Task: Reboot
4. Task – Reboot System
5. Discover Applicable Updates (DAU)

Although no deployment occurs before its scheduled time, a chained deployment whose scheduled time has elapsed will always precede a standard deployment whose scheduled time has also elapsed.

If multiple chained deployments are scheduled and some endpoints have the final reboot suppressed, the determination of a reboot override is based on the last scheduled deployment.

Deployment Types

Deployments are based on the content-type being deployed and how the content is being deployed. Deployment types include System Tasks, Package Deployments, and Mandatory Baseline Deployments.

System Task	System tasks are HPL deployments where no actual patch content is deployed. Rather, they are instructions for the HEAT PatchLink DataCenter Agent for Linux/UNIX to execute to determine if an endpoint is in need of patch content, and then further instructions to complete deployment of patch content. There are two types of System tasks:
	• Discover Applicable Updates: this task, also called a DAU, is a HEAT PatchLink DataCenter Agent for Linux/UNIX scan that determines whether endpoints have applicable patch content available on the Global Subscription Service installed. By default HPL schedules a global DAU for all endpoints every twenty six hours following replication, but you can modify DAU schedules using Agent Policy Sets. Additionally, DAUs run five minutes after the HEAT PatchLink DataCenter Agent for Linux/UNIX installs a patch, immediately following an endpoint reboot, or immediately when you use the **Scan Now** feature.
	• Reboot: this task is usually executed following installation of a patch. You can also manually schedule a reboot as well.

Package Deployment	These deployments are a user-scheduled deployment of patch content. They include all patch content you select when completing the ***Deployment Wizard***. When the package deployment begins at the time you schedule, the HEAT PatchLink DataCenter Agent for Linux/UNIX runs scripts on the endpoint you targeted for deployment. These scripts identify whether the patch content included in the deployment applies to the endpoint. If the patch content applies, the content is installed.
Mandatory Baseline Deployment	Unlike package deployments, which are scheduled by the user, Mandatory Baseline deployments are deployments that HPL automatically initiates. Here's how it works: You can form a group of endpoints, and then select the patch content that group members must have installed at all times—a mandatory baseline. Every DAU will check to make sure that patch content included in the mandatory baseline is installed. If patch content from the mandatory baseline is missing, HPL deploys the patch content to incompliant endpoint immediately. For additional information, refer to About Mandatory Baselines on page 164.

Standard and Chained Deployments

Deployments come in two varieties: standard deployments and chained deployments.

Standard Deployment	A standard deployment is a deployment that has not been chained with another deployment. While not all standard deployments require a reboot, if the included package does require one and the reboot is suppressed, the endpoint will not accept additional deployments until it is rebooted.
Chained Deployment	A chained deployment is a deployment grouped with other deployments so the endpoint will not reboot after each one. Following the first chained deployment, the endpoint will accept only chained deployments until rebooted.

Reboot and Chained State

The reboot and chained states are the result of an endpoint not performing the required reboot following a deployment.

Table 116: Reboot and Chained State

State	Description
Reboot State	Indicates that the endpoint received a standard deployment requiring a reboot, but the reboot was suppressed. While in the reboot state, the agent only accepts deployments. A reboot deployment or a manual reboot clears this state.

HEAT software

State	Description
Chained State	Indicates that the agent received a chained deployment in which the reboot was suppressed. While in the chained state, the agent only accepts another chained deployment or a reboot deployment.

The following deployments always perform a reboot.

Table 117: Reboot Deployments

Deployment	Description
Reboot System Package	A system task that is automatically added to the end of chained deployments where the final reboot is not suppressed. This is also sent to agents when you click the **Reboot Now** button on the **Endpoints** page.
Task - System Reboot	A task that permits the user to schedule a reboot using the scheduling features of the **Schedule Deployment Wizard**.

Standard packages reboot for one of the following reasons:

- The deployed package required and forced the reboot (unless suppressed), during the installation.
- The package installer determined that it required a reboot.
- The reboot flag was sent to the agent. It is not necessary that the agent receive the Reboot System Package or Task. The agent performs the reboot on its own.

The Deployments and Tasks Page

Deployments and system tasks are reviewed on the **Deployments and Tasks** page. The page list displays each deployment job and the individual deployments or scans assigned to it.
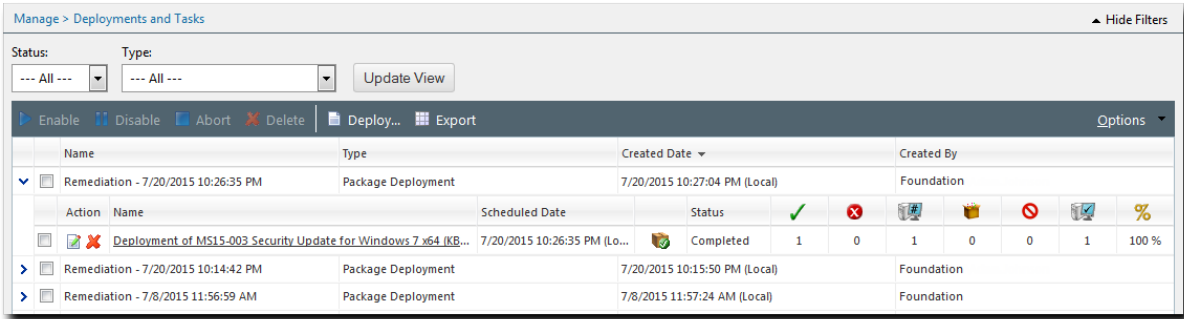
Figure 54: Deployments and Tasks Page

- For additional information about deployments, refer to About Deployments on page 289.

Viewing Deployments and Tasks

There are several pages within the HEAT PatchLink DataCenter for Microsoft System Center from which you can view deployments and system tasks. Based on the page from which you are viewing deployments, deployments may be organized by content type, endpoints, groups, or deployments themselves.

Viewing All Deployments and Tasks

You can view all deployments and system (either executed or scheduled) within HEAT PatchLink DataCenter for Microsoft System Center from the **Deployment and Tasks** page. This page displays all system deployments, regardless of the page used to schedule the deployment.

View all system deployments and tasks from the **Deployments and Tasks** page.

Note: Recurring Virus and Malware Scans do not appear on this page.

1. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **Deployments and Tasks**.

2. [Optional] Select the desired filter criteria and click **Update View**.

3. [Optional] To view the details for a deployment or task, expand a list item by clicking a rotating chevron (**>**).

Viewing Deployments and Tasks within Endpoints

You can view the deployments and tasks assigned to a specific endpoint from its **Endpoint Details** page. This page shows only the deployments for the selected endpoint, not the entire system.

View the deployments and tasks for an endpoint from the **Endpoint Details** page **Deployments and Tasks** tab.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Endpoints**.

2. Select your filter options and click **Update View**.

   Step Result: The applicable endpoints display in the **Endpoints** page.

3. Click the link for an endpoint with at least one deployment or task to view its details.

   Step Result: The **Endpoint Details** page opens.

4. Select the **Deployments and Tasks** tab.

   Step Result: The **Deployments and Tasks** tab opens.

5. [Optional] To view details for a deployment or task, expand it by clicking the applicable rotating chevron (**>**).

Result: The deployment details display.

HEAT®software

Viewing Deployments and Tasks within Groups

You can view deployments and tasks for specific endpoint groups from the **Groups** page. When viewing group deployments, you can only view deployments for the selected group; other system deployments are not listed.

View group deployments and tasks from the **Groups** page **Deployments and Tasks** view.

1. From the **Assets and Compliance** workspace, select **HEAT PatchLink DataCenter** > **Groups**.

2. In the **Groups** page, select **Deployments and Tasks** from the **View** drop-down list.

   Step Result: The **Deployments and Tasks** view displays next to the **Browser**.

3. Select a group from the browser.

Result: The selected group is highlighted and displays the assigned deployments and tasks.

The Deployments and Tasks Page Toolbar

This toolbar contains buttons that let you create new deployments, control existing deployments, and export deployment data.

The following table describes each toolbar button

Table 118: Deployments and Tasks Page Toolbar Functions

Menu Item	Function
Enable	Enables the selected disabled deployment or task. For additional information, refer to Enabling Deployments on page 298.
Disable	Disables the selected enabled deployment or task. For additional information, refer to Disabling Deployments on page 298.
Abort	Cancels the deployment or task for any endpoints which have not already received the deployment package. For additional information, refer to Aborting Deployments and Tasks on page 297.
Delete	Removes the deployment or task from your HEAT PatchLink DataCenter for Microsoft System Center. For additional information, refer to Deleting Deployments on page 302.
Deploy...	Deploys the selected packages or tasks. For additional information, refer to Deploying Content (Deployments and Tasks Page) on page 303.

Menu Item	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Deployments and Tasks Page List

A record of each default deployment and each deployment that you have created resides in the *Deployments and Tasks* page list.

The following table describes the columns that appear in the *Deployments and Tasks* page list. Expand the deployment list item to view all the available column headers for the item.

Table 119: Deployments and Tasks Page List Column Descriptions

Column	Description
Name	The name of the deployment.
Type	The deployment type. For more information, see Deployment Types on page 290.
Created Date	The date and time a user created the deployment.
Created By	The user that created the deployment.

You can expand deployments to view the packages that are included in them. Expand deployments clicking the **Arrow** icon (**>**). The following table describes each column for an expanded deployment.

Table 120: Expanded Deployment Columns

Column	Icon	Description
Action	N/A	Contains **Edit** and **Delete** icons you can use to control packages in a deployment. For additional information see: • Editing Package Deployment Options on page 298 • Deleting Deployments on page 302

HEAT software

Column	Icon	Description
Name	N/A	The name of the package or task in the deployment. Click the name to display its **Deployment Details** page. For additional information, see The Deployment Details Page on page 335.
Scheduled Date	N/A	The date and time a user scheduled the package or task to deploy.
Status Icon	N/A	An icon that indicates the status of the package deployment.
Status	N/A	The status of the package deployment.
Number of endpoints/ groups which were successful	✓	The total number of endpoints and groups that finished the deployment successfully.
Number of endpoints/ groups which failed	⊗	The total number of endpoints and groups that finished the deployment unsuccessfully.
Number of endpoints/ groups assigned to the deployment	🗔	The total number of endpoints and groups that are assigned to the deployment.
Number of endpoints/ groups which are in progress	📦	The total number of endpoints and groups that are receiving the deployment. **Note:** If you deploy to a group using Agent Local Time, the deployment remains in progress until all time zones have passed. This behavior ensures any endpoints added to the group following deployment start also receive content. This behavior does not occur when using Agent UTC Time.
Number of endpoints/ groups which were not deployed	⊘	The total number of endpoints and groups that were excluded from the deployment (because the package was already applied, not applicable, or marked *Do Not Patch*).
Number of endpoints/ groups which have completed the deployment	🗹	The total number of endpoints and groups that finished the deployment.

Column	Icon	Description
Percentage Complete	**%**	The percentage of endpoints and groups that finished the deployment. Percentage = [Total Finished endpoints / Total Assigned endpoints]

Working With Deployments and Tasks

There are several procedures associated with deployments and tasks that manage and deploy content. The controls to begin these procedures are available on the **Deployments and Tasks** page toolbar.

You can perform the following tasks from the **Deployments and Tasks** page:

Aborting Deployments and Tasks

Aborting deployments cancels deployments for endpoints that have not already received the deployment. Abort deployments when you do not want endpoints to receive their packages.

Abort deployments from the **Deployments and Tasks** page.

> **Note:**
> - Aborted deployments only affect endpoints that have no yet received the deployment. Endpoints that have already received the deployment are not effected.
> - System tasks, completed deployments, or previously aborted deployment cannot be aborted.

1. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **Deployments and Tasks**.

2. Select the deployments you wish to abort.

3. Click **Abort**.

   Step Result: A confirmation message displays, asking you to confirm that you want to abort the deployment.

4. Click **OK** to confirm that you want to abort the deployment.

Result: The selected deployment is canceled.

> **Note:** You cannot abort system tasks or Mandatory Baseline deployments.

HEAT software

Disabling Deployments

Disabling deployments pauses them, thus temporarily stopping the distribution of the package(s) to endpoints that have not already received a deployment. Disable deployments when you temporarily want to prevent them from installing on endpoints.

Disable deployments from the *Deployments and Tasks* page.

Note: You cannot disable deployments of system task packages.

1. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **Deployments and Tasks**.
2. Select the deployments you want to disable.
3. Click **Disable**.

Result: The selected deployments are disabled.

Enabling Deployments

After you have disabled a deployment, reenable it to resume sending content to the deployment's assigned endpoints.

Reenable deployments from the *Deployments and Tasks* page.

1. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **Deployments and Tasks**.
2. Select the disabled deployments you want to enable.
3. Click **Enable**.

Result: The selected deployments are enabled.

Editing Package Deployment Options

After scheduling a deployment, you can edit the package deployment options for each package assigned to the deployment. Editing a packages deployment options changes the deployment's behavior. This function is useful when you want each package in a deployment to deploy using different behavior options.

Edit package deployment behavior from the *Deployments and Tasks* page.

Note: System task packages are automatically assigned to endpoints, so removing an endpoint from a deployment of a system task package will have no effect (the endpoint will be re-assigned to the deployment by the HEAT PatchLink DataCenter for Microsoft System Center).

1. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **Deployments and Tasks**.
2. Expand the deployment that you want to modify.

3. Select the individual deployment package that you need to modify.

Note: If the deployment you are editing contains only one package, this list is unavailable.

4. Click the **Edit** icon.

Step Result: The *Package Deployment Options* dialog opens.

Figure 55: Package Deployment Options

5. From the **Package Name** list, ensure the desired package is selected.

6. Define **Distribution Options.**

Choose from the following options.

Option	Steps
To deploy concurrently:	1. Select the **Concurrent** option. 2. Type the desired number of endpoints you want to deploy to at a time in the field.

HEAT software

Option	Steps
To deploy consecutively:	Select the **Consecutive** option.

7. If available, select the desired **Deployment Flags**.

   For additional information, refer to Behavior Icon Definitions on page 323.

8. If needed, type additional deployment flags in the **Optional Flags** field.

   For additional information, refer to Package Flag Descriptions on page 325.

9. Define the **Deployment Options**.

   Table 121: Deployment Options

Option	Description
Do not notify users of this deployment	Deploys the Mandatory Baseline package without notifying the recipients.
	Note: Selection of this option makes the remaining **Deployment Options** unavailable.
Notify users of this deployment	Deploys the Mandatory Baseline package and notifies the recipients.
	Note: Selection of this option makes the remaining **Deployment Options** available.
Message (field)	Displays a message notifying recipients of the deployment.
Use Policies (check box)	Uses the group's assigned agent policy set to define the remaining **Deployment Options**.
	Note: Selection of this option makes the remaining **Deployment Options** unavailable.
Allow user to cancel (check box and list)	Permits the recipient of the deployment to cancel. Either select the **Use Agent Policy** check box or define the **Setting** list.
Allow user to snooze (check box and list)	Permits the recipient of the deployment to delay the deployment. Either select the **Use Agent Policy** check box or define the **Setting** list.
Notification on top (check box and list)	Displays the *Agent Deployment* dialog when notifying a deployment recipient. Either select the **Use Agent Policy** check box or define the **Setting** list.

Option	Description
Deploy within (check box, field, and list)	Defines the time between the deployment creation and the deployment deadline. If **Allow user to snooze** is enabled, this value is also the maximum deployment snooze duration. Either select the **Use Agent Policy** check box or define the **Setting** field and list.

10. Define the **Reboot Options**.

Table 122: Reboot Options

Option	Description
Do not notify users of this reboot	Reboots following installation of the Mandatory Baseline package without notifying recipients.
	Note: Selection of this option makes the remaining **Reboot Options** unavailable.
Notify users of this reboot	Reboots following installation of the Mandatory Baseline package and notifies the recipients.
	Note: Selection of this option makes the remaining **Reboot Options** available.
Message (field)	Displays a message notifying recipients of the reboot.
Use Policies (check box)	Uses the applicable agent policy set to define the remaining **Deployment** options.
	Note: Selection of this option makes the remaining **Reboot Options** unavailable.
Allow user to cancel (check box and list)	Permits the recipient of the deployment to cancel the reboot. Either select the **Use Agent Policy** check box or define the **Setting** list.
Allow user to snooze (check box and list)	Permits the recipient of the deployment to delay the reboot. Either select the **Use Agent Policy** check box or define the **Setting** list.
Reboot within (check box and list)	Defines the time between the deployment creation and the reboot deadline. If **Allow user to snooze** is enabled, this value is also the maximum reboot snooze duration. Either select the **Use Agent Policy** check box or define the **Setting** field and list.

HEAT software

11. Click **OK**.

Result: The *Package Deployment Options* dialog closes and the deployment is modified.

Deleting Deployments

Deleting deployments removes the deployments from the HEAT PatchLink DataCenter for Microsoft System Center. You can delete entire deployments or individual packages within a deployment.

Delete completed deployments, aborted deployments, or deployment packages from the *Deployments and Tasks* page.

Note:

- Deleting deployments has no effect on endpoints that have already received the deployments.
- You cannot delete system tasks.
- Scheduled deployments cannot be deleted until they are aborted.

---

1. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **Deployments and Tasks**.
2. Delete deployments. You can either delete an entire deployments, or you can delete individual packages included in a deployment.
   Complete one of the following substep sets based on whether you want to partially or fully delete a deployment.

Option	Steps
To delete entire deployment(s):	1. Select the completed or aborted deployments you want to delete. 2. From the toolbar, click **Delete**.
To delete individual packages in a deployment (partial deletion):	1. Expand the deployment containing packages you want to delete by clicking the rotating chevron (**>**). 2. Click the **Delete** icon (✖) for the package you want to delete. **Tip:** Repeat this process for each package you want to delete.

3. Click **OK** to delete the deployment(s) or package.

Deploying Content (Deployments and Tasks Page)

Within HEAT PatchLink DataCenter for Microsoft System Center, content can be deployed from a number of pages, including the **Deployments and Tasks** page. Deploying content remotely installs different types of software on your network endpoints.

You can deploy content from the **Deployments and Tasks** page. For additional information about deployments, refer to About Deployments on page 289.

1. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **Deployments and Tasks**.

2. Click **Deploy**.

Result: The **Deployment Wizard** opens.

After Completing This Task:
Review Using the Deployment Wizard on page 303 and complete subsequent tasks.

Explaining Deployment Deadlines

Deadlines determine when a deployment or reboot should occur. A deadline can be calculated based upon the agent's group policy or defined by you as a specific date and time.

When using deadlines, define the deadline using the following parameters:

*   Date and time.
*   Starting date and time.
*   Ability to snooze the deployment or reboot, as many times as desired, up to the defined deadline.

Using the Deployment Wizard

The **Deployment Wizard** is the dialog used to create or edit deployment schedules for multiple endpoints and multiple packages. The wizard assists in selecting endpoints, scheduling the deployment, and if needed, setting recurring deployments.

The following table describes the scenarios for a deployment. These options are selected prior to starting the **Deployment Wizard**.

Table 123: Deployment Actions

Deployment Selection	Result
Endpoint	The **Deployment Wizard** deploys only to the selected endpoint.
Content	The **Deployment Wizard** automatically selects all the endpoints and packages required for the content.
Package	The **Deployment Wizard** deploys the selected package to the selected groups or endpoints selected within the wizard.

HEAT®software

Deployment Selection	Result
Group	The *Deployment Wizard* deploys the applicable packages to the selected group members.

For additional information on configuring a deployment, refer to

Introduction Page

The *Introduction* page of the *Deployment Wizard* explains the purpose and capabilities of the wizard.

This page can be hidden during future deployments by selecting the **Do not display this page in the future** checkbox.

If this page displays, click **Next** to continue to the

Available Endpoints/Groups Page

When scheduling a deployment, you must choose endpoints and groups for patching.
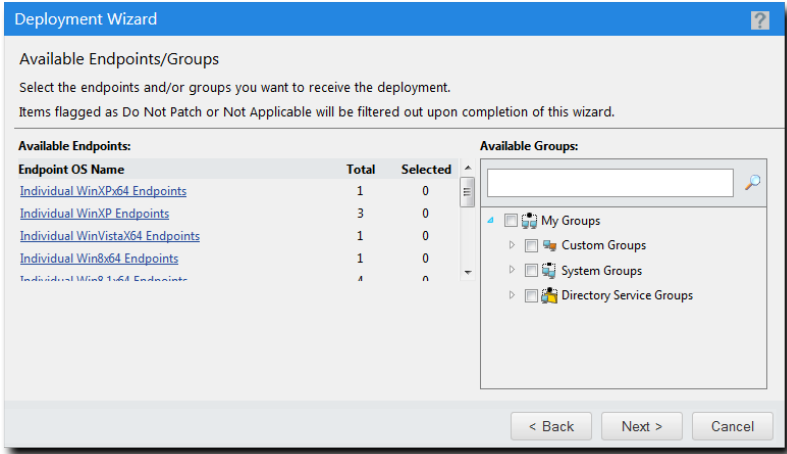
Figure 56: Available Endpoints/Groups Page

Endpoint Notes

• You can select endpoints, groups, or a combination of the two.

> **Note:** If you select endpoints or groups before initiating a deployment with the toolbar, those endpoints are preselected when you get to the *Available Endpoints/Groups* page.

• Endpoints are categorized by operating system. Click a link to display all the endpoints using that operating system.

• Groups are organized into a tree of custom groups, system groups, and directory service groups.

  • Use the search field to find specific groups quickly.
  • Wildcard searches are not supported.

Patch Notes

If you selected patches for deployment before opening the **_Deployment Wizard_**, there are a few things you should know:

- The **_Deployment Wizard_** only lists endpoints that the patches apply to.
- The **_Deployment Wizard_** only lists groups that the patches apply to.

  - If the group contains one or more endpoint that the patch applies to, it's listed.

- If you are deploying a _single_ patch that is marked _Do Not Patch_:

  - **Available Endpoints** does not list endpoints that are _Do Not Patch_.

- If you are deploying multiple patches, and one or more of those patches are marked _Do Not Patch_:

  - **Available Endpoints** or **Available Groups** marked _Do Not Patch_ are automatically selected because the other patches selected for deployment still apply. However, the patch marked _Do Not Patch_ does not deploy to the marked endpoints and groups.

After choosing endpoints and groups, click **Next** to proceed to the

Creating an Endpoint Deployment
When creating deployments, you can define deployment recipients by selecting individual endpoints, regardless of group membership.

Select endpoints as deployment recipients from the **_Available Endpoints/Groups_** page.

1. From the **Available Endpoint** list, select the **Endpoint OS Name** required.

   Step Result: The list of endpoints within that operating system display.

2. Select an endpoint (or endpoints) from the list.

   Step Result: The endpoint(s) are highlighted.

Result: Endpoints are targeted as deployment recipients.

Creating a Group Deployment
You can select single groups, multiple groups, and group hierarchies as deployment recipients using the **Available Groups** directory tree. This method of selecting recipients lets you select multiple groups for a deployment without having to create deployments for each individual group.

Select endpoints as deployment recipients from the **_Available Endpoints/Groups_** page.

Note: If endpoints are added to a group after a deployment is created but before the time the deployment occurs, the newly-added endpoints will receive the deployment.

HEAT®software

From the **Available Groups** directory tree, select the group or groups requiring the deployment.

Selecting a parent group also selects its child hierarchy. If you do not want to deploy to a parent's child group hierarchy, cancel the deployment for the desired groups by clearing the applicable check boxes.

Result: Groups are targeted as deployment recipients.

Available Packages Page

While completing the **Deployment Wizard**, packages must be selected for installation on target endpoints. These packages are selected from the **Available Packages** page.

When selecting packages for deployment, remember the following helpful information:

- Only vendors and packages applicable to the selected endpoint(s) display. Inapplicable content is hidden.
- If you opened the **Deployment Wizard** from one of the **Content** pages after selecting content items from the page list, those items are preselected in the wizard. Finding the packages you want to deploy is unnecessary (although you can select more packages if desired).

Note: If you pre-selected vulnerabilities for deployment, the **Available Packages** page may display more packages selected for deployment that the number of vulnerabilities you selected. This discrepancy is because a vulnerability may contain more than one package.

- An icon in the listed packages indicates if the package your want to deploy is already cached. If you already have the package cached, you can deploy it more quickly. HEAT recommends caching packages before deployment.

After defining the **Available Packages** page, click **Next** to proceed to the

For additional information of selecting packages, refer to

Selecting Deployment Packages
Selecting packages to deploy to selected endpoint remediates endpoint vulnerabilities.

Select packages for deployment from the **Available Packages** page.

1. Select the **Vendor** link containing the package(s) you want to deploy.

    Step Result: A list of the vendor's packages for the selected deployment recipients opens.

2. Select the package(s) needed.

    Step Result: The packages are selected.

3. [Optional] Repeat the selection process for additional vendors.

4. [Optional] Click a **Package Name** link to open the **Associated Vulnerability Analysis** page. For additional information, refer to

5. Click **Next** to proceed to the *Licenses* page.

When using the *Deployment Wizard*, the wizard will not necessarily install service packs first. Verify that all relevant service packs have deployed successfully before creating deployments using the *Deployment Wizard*.

Associated Vulnerability Analysis Page
This page lists the package status for each endpoint that it applies to (not just the endpoints included in the deployment). Viewing this page is useful to estimate how many of your selected endpoints will not receive the deployment package due to patch status (for example, the patch does not apply to the endpoint).
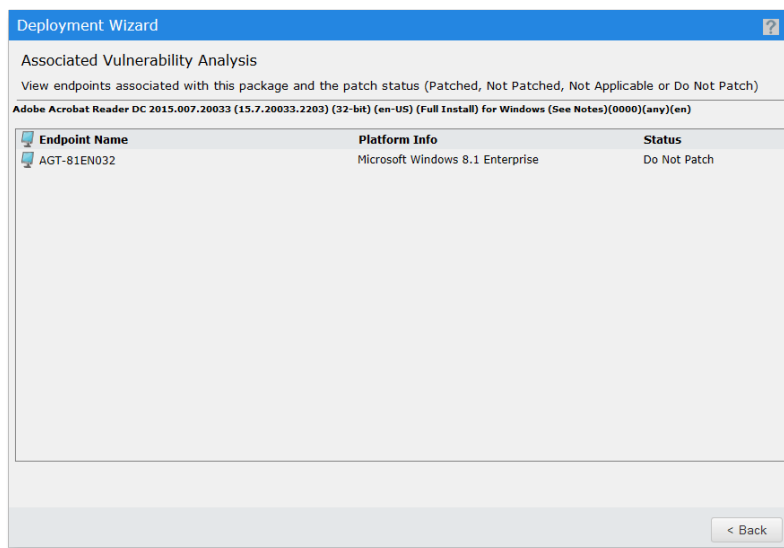
Figure 57: Associated Vulnerability Analysis Page

The following table describes the page columns.

Table 124: Associated Vulnerability Analysis Columns

Name	Description
Endpoint Name	The endpoint that the package applies to.
Platform Info	The operating system that the endpoint is using.
Status	The patch status of the package for the endpoint. Values include: • Patched • Not Patched • Not Applicable • Do Not Patch

HEAT software

When finished viewing the page, click **Back** to return to the Available Packages Page on page 306.

Licenses Page

To continue configuration of your deployment, you must first accept the vendor license agreement(s).

The number of different license agreements that appear depend upon how many packages you selected to install. For example, you selected four different packages for installation and these packages were created by three different vendors, you would have to agree to three different license agreements.

For additional information on accepting license agreements, refer to Accepting License Agreements on page 308.

After accepting licenses, click **Next** to proceed to the Deployment Information Page on page 309.

Accepting License Agreements

To continue configuration of your deployment, you must first accept the vendor license agreement(s).

Accept licenses from the *Licenses Page*.
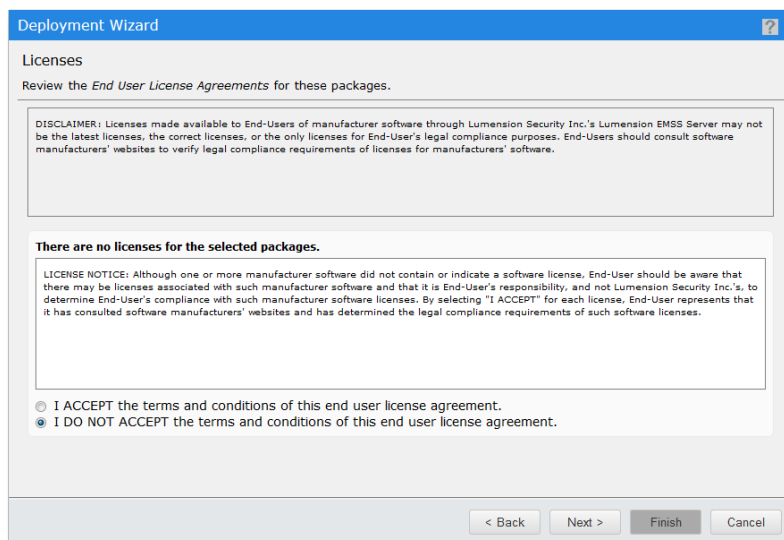
Figure 58: Licenses Page

1. Review the agreement.
2. If you accept the agreement, select the **I ACCEPT the terms and conditions of this end user license agreement** option.
3. If there are multiple agreements, repeat the previous steps.

   All agreements must be accepted before continuing.
4. [Optional] Click **Next** to proceed to the *Deployment Information* page.

Deployment Information Page

You can control the user notification options associated with a deployment using the ***Deployment Information*** page. You can set the deployment job name, start time, manner, and add notes.

The following information may be useful when completing this page:

- Job and task names will later be used to identify deployment results.
- Deploying using Agent Local Time is useful in geographically dispersed networks. This deployment method helps ensure deployments complete off peak business hours.
- Deploying using UTC time is useful when you want to deploy content at one specific time.
- Concurrent deployments ensure endpoint receive packages near simultaneously, but may consume excessive network bandwidth.
- Consecutive deployments reduces network bandwidth consumption, but endpoints may receive deployment at different times.

After defining deployment information, click **Next** to proceed to the Package Deployment Order and Behavior Page on page 320.

For additional information of defining deployment information, refer to Configuring Deployment Information on page 309.

Configuring Deployment Information

The deployment information contains controls for naming and configuring your deployment. You can use this page to choose a start time and the manner in which it deploys.

Configure deployment information from the ***Deployment Information*** page.

1. [Optional] Edit the **Job name** and **Task name** fields.

Field	Description
Job name	The name of the job. By default, jobs are named `Remediation`, followed by the date and time at the time of deployment creation.
Task name	The task name for the job. Use this name to describe the purpose of the deployment. By default, tasks are named `Deployment of {Package Name}`.

Tip: Upon completion of the ***Deployment Wizard***, use the **Job name** and **Task name** to identify your deployment. The **Job name** displays on the ***Deployment and Tasks*** page, and the **Task name** displays when you expand your deployment.

◢HEAT®software

Use the **Start time** options to configure the deployment start time and start date. You can also use these options to schedule a recurring deployment or select deployment time zone options.

2. [Optional] Schedule the deployment **Start Time**, which is the date and time that the deployment begins. Edit the **Start time** by clicking **Change**. By default, the **Start time** is set to the date and time the *Deployment Wizard* was opened.

   For additional information on start times and configuring recurring deployments, refer to Schedule Configuration Page on page 312.

3. Select the desired **Deployment time zone** option.

   Use this option to configure which time zone setting is used to trigger a deployment. The following table defines the options.

Option	Description
Agent Local Time	The deployment begins according to the local time zone on each endpoint.
Agent UTC Time	The deployment begins according to UTC (coordinated universal time) on each endpoint.

Note: If you deploy to a group using **Agent Local Time**, the deployment remains in progress until all time zones have passed. This behavior ensures any endpoints added to the group following deployment start also receive content. This behavior does not occur when using Agent UTC Time.

Use the **Manner** options to configure how endpoints receive the deployment in relation to one another. The **Manner** options also include:

- A feature to disable the entire deployment should deployment to an individual endpoint fail.
- A feature to redeploy packages to an endpoint, even if the package has been previously installed.

4. Select a **Manner** deployment option.

The following table describes each manner deployment option and how to use them.

Option	Description and Instructions
Concurrent	This option deploys the package(s) to a defined number of endpoints simultaneously. New deployments are distributed when agents report back after completing the previous deployment. If an endpoint takes longer than four hours to complete the deployment, it is no longer counted against the concurrent deployment limit. To deploy to endpoints concurrently, complete the following steps: 1. Select the **Concurrent** option. 2. Type a number in the **Deploy to *<x>* nodes at a time** field.
Consecutive	This option deploys the packages simultaneously to all endpoints. However, the global deployment limit will always take precedence over the defined distribution options defined. To deploy to endpoints consecutively, select the **Consecutive** option.

5. [Optional] Define the remaining **Manner** options. Enable or disabled the options by selecting or clear each option checkbox.

The following table describes the remaining **Manner** options.

Option	Description
Suspend the deployment of this package if it fails to deploy to one or more nodes.	This option suspends all subsequent deployments following any deployment failure.
Deploy package even if the computer has been previously patched.	This option deploys the package(s) to all selected endpoints regardless of patch status.

HEAT software

> Finally, the **Deployment Information** page features a **Notes** field to type text about the deployment. You can view this text after you complete the **Deployment Wizard** by viewing the deployment details on various HEAT PatchLink DataCenter pages.

6. [Optional] Type notes and comments in the **Notes** field.

> **Tip:** After completing the **Deployment Wizard**, you can view deployment notes by expanding the deployment from an **Endpoint Details** page **Deployment and Tasks** tab.

Result: Deployment information is defined. Click **Next** to continue to the **Package Deployment Order and Behavior** page.

Schedule Configuration Page

You can set the timing and frequency of a deployment using the **Schedule Configuration** page. Deployments can be defined as one-time or recurring. Additional schedule configuration options are also available.

> **Note:** If endpoints are added to a group after a deployment is created but before the deployment occurs, the newly-added endpoints will receive the deployment.
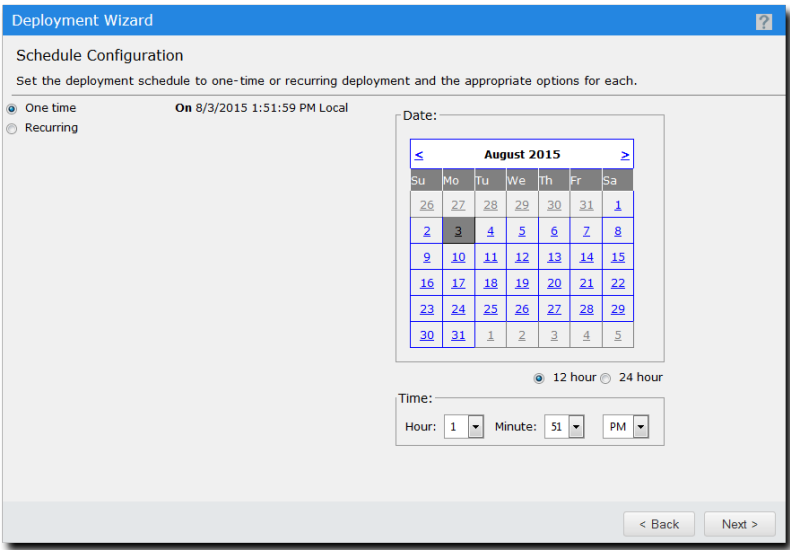
Figure 59: Schedule Configuration Page

Complete one of the following tasks based on how you want to schedule the deployment:

- If you want to run the deployment once, complete Scheduling a One Time Deployment on page 313.
- If you want to run the deployment on a recurring basis, complete Scheduling a Recurring Deployment on page 314.

Scheduling a One Time Deployment

A one time deployment starts on the selected day at the selected time.

Prerequisites:

- Begin Configuring Deployment Information on page 309.

1. From the ***Deployment Wizard Schedule Configuration*** page, click **Change** located in the **Start Time** option.

2. Ensure **One Time** is selected.

   Step Result: The deployment will start on the selected day at the defined time.

3. [Optional] Select a date from the calendar. This is the date that the deployment will begin.

4. Define a **Time**. This is the time that the deployment will begin.

   > **Tip:** Select from the **12 hour** and **24 hour** options to change time listing values. When the **24 hour** option is selected, the **AM/PM** list is unavailable.

   a) Select a value from the **Hour** list.
   b) Select a value from the **Minute** list.
   c) Select a value from the **AM/PM** list.

5. Click **Next**.

   Step Result: The deployment is configured to start on the selected date and time, and the ***Deployment Information*** page opens. If you scheduled the deployment for a lapsed date and time, the deployment will start the next time applicable agents contact the HEAT PatchLink DataCenter for Microsoft System Center server.

After Completing This Task:

Complete Configuring Deployment Information on page 309.

HEAT®software

Scheduling a Recurring Deployment
A recurring schedule starts deployments on the selected day at the selected time. The deployment repeats every day, week, or month and if defined, ends on a specific date.
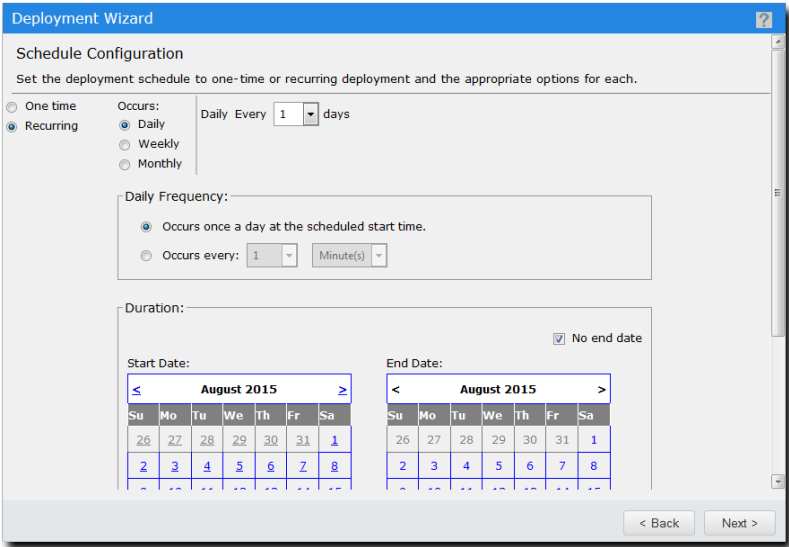
Figure 60: Schedule Configuration Page

To schedule a recurring deployment, complete one of the following tasks:

Configuring a Daily Recurring Deployment
You can configure a deployment to happen every day. Recurring deployments are useful to ensure selected content remains installed on endpoints.

Prerequisites:

Schedule deployments for daily recurrence from the **Schedule Configuration** page

1. From the **Deployment Information** page, click **Change**, located in the **Start Time** section of the page.

   Step Result: The **Schedule Configuration** page opens.

2. Select **Recurring**.

Begin configuring your daily recurring deployment by defining the occurrence options. Configure the deployment to run daily or, alternatively, configure it run it at intervals of a defined number of days.

3. Configure the **Occurs** options for a daily deployment.

    a) Select **Daily**.

    b) Select a value from the **Daily Every <x> days** list (1-366).

Next, select a **Daily Frequency** option. You can configure your recurring deployment to run at one time on its scheduled day, or several times on its scheduled day.

4. Select a **Daily Frequency** option.

    The following table describes each **Daily Frequency** option and lists instructions for using it.

Option	Description and Instructions
Occurs once a day at the scheduled start time	The deployment occurs as defined in the **Occurs** and **Duration** options once on the scheduled day(s). To use this option, select **Occurs once a day at the schedule start time**.
Occurs every <x> <time unit>	The deployment occurs as defined in the **Occurs** and **Durations** options at the selected interval. To use this option, complete the following steps: 1. Select the **Occurs every <x> <time unit>** option. 2. Select a value from the **<x>** list. The values available changes according to the value selected from the **<time unit>** list. 3. Select a value from the **<time unit>** list (**Minute[s]**, **Hour[s]**).

Finally, select the duration of your recurring deployment. All recurring deployments require a start date. However, you have the option of selecting an end date for your recurring deployment or letting it run indefinitely.

5. Define a deployment **Start Date**. This is the date and time the recurring deployment will start.

> **Tip:** Select from the **12 hour** and **24 hour** options to change time listing values for both the **Start Date** and **End Date** calendars. When the **24 hour** option is selected, the **AM/PM** list is unavailable.

    a) Select a date from the **Start Date** calendar.

    b) Select a value from the **Hour** list.

    c) Select a value from the **Minute** list.

    d) Select a value from the **AM/PM** list.

HEAT®software

6. Define a deployment **End Date**.

End Date Option	Instructions
To end the recurring deployment on a selected date:	**1.** Ensure the **No end date** checkbox is cleared. **2.** Select a date from the **End Date** calender. **3.** Select a value from the **Hour** list. **4.** Select a value from the **Minute** list. **5.** Select a value from the **AM/PM** list.
To run the recurring deployment indefinitely:	Ensure the **No end date** checkbox is selected.

7. Click **Next**.

After Completing This Task:
Complete Configuring Deployment Information on page 309.

Configuring a Weekly Recurring Deployment
You can configure a deployment that happens every week. Recurring deployments are useful to ensure selected content remains installed on endpoints.

Prerequisites:

Begin Configuring Deployment Information on page 309.

Schedule deployments for weekly recurrence from the *Schedule Configuration* page.

1. From the *Deployment Information* page, click **Change**.

   Step Result: The *Schedule Configuration* page opens.

2. Select **Recurring**.

Begin configuring your weekly recurring deployment by defining the occurrence options. You can configure deployments to run weekly, or you can configure it to run weekly with an interval of weeks between deployments. You can also configure the deployment to run on certain days of your weekly deployment.

3. Configure the **Occurs** options for a weekly deployment.

   a) Select the **Weekly** option.
   b) Select a value from the **Every <x> weeks on** list.
   c) Select the weekday checkboxes for the days of the week that you want the deployment to run (**Monday** through **Sunday**).

Next, select a **Daily Frequency** option. You can configure your recurring deployment to run at one time on its scheduled day, or several times on its scheduled day.

4. Select a **Daily Frequency** option.

   The following table describes each **Daily Frequency** option and lists instructions for using it.

Option	Description and Instructions
Occurs once a day at the scheduled start time	The deployment occurs as defined in the **Occurs** and **Duration** options once on the scheduled day(s). To use this option, select **Occurs once a day at the schedule start time**.
Occurs every <x> <time unit>	The deployment occurs as defined in the **Occurs** and **Durations** options at the selected interval. To use this option, complete the following steps: 1. Select the **Occurs every <x> <time unit>** option. 2. Select a value from the **<x>** list. The values available changes according to the value selected from the **<time unit>** list. 3. Select a value from the **<time unit>** list (**Minute[s]**, **Hour[s]**).

Finally, select the duration of your recurring deployment. All recurring deployments require a start date. However, you have the option of selecting an end date for your recurring deployment or letting it run indefinitely.

5. Define a deployment **Start Date**. This is the date and time the recurring deployment will start.

   Tip: Select from the **12 hour** and **24 hour** options to change time listing values for both the **Start Date** and **End Date** calendars. When the **24 hour** option is selected, the **AM/PM** list is unavailable.

   a) Select a date from the **Start Date** calendar.
   b) Select a value from the **Hour** list.
   c) Select a value from the **Minute** list.
   d) Select a value from the **AM/PM** list.

6. Define a deployment **End Date**.

End Date Option	Instructions
To end the recurring deployment on a selected date:	1. Ensure the **No end date** checkbox is cleared. 2. Select a date from the **End Date** calender. 3. Select a value from the **Hour** list. 4. Select a value from the **Minute** list. 5. Select a value from the **AM/PM** list.

HEAT®software

End Date Option	Instructions
To run the recurring deployment indefinitely:	Ensure the **No end date** checkbox is selected.

7. Click **Next**.

After Completing This Task:
Complete Configuring Deployment Information on page 309.

Configuring a Monthly Recurring Deployment
You can configure a deployment that happens every month. Recurring deployments are useful to ensure selected content remains installed on endpoints.

Prerequisites:

Begin Configuring Deployment Information on page 309.

Configure deployments for monthly recurrence from the ***Schedule Configuration*** page.

1. From the ***Deployment Information*** page, click **Change**, located in the **Start Time** section of the page.

2. Select **Recurring**.

Begin configuring your monthly recurring deployment by defining the occurrence options. You can configure the deployment to run monthly, or you can configure the deployment to run monthly with an interval of months between deployments. You can also schedule your monthly deployment to run on a specific date (July, 1) or a specific day (first Sunday on the month).

3. Configure the **Occurs** options for a monthly deployment.

    a) Select the **Monthly** option.
    b) Select one of the **Monthly** options that displays, and then select values from its drop-down lists.
       Select one of the following options and then define its lists.

- **Day *<x>* of every *<x>* months**
- **The *<x>* *<day>* of every *<x>* months**

Next, select a **Daily Frequency** option. You can configure your recurring deployment to run at one time on its scheduled day, or several times on its scheduled day.

4. Select a **Daily Frequency** option.

   The following table describes each **Daily Frequency** option and lists instructions for using it.

Option	Description and Instructions
Occurs once a day at the scheduled start time	The deployment occurs as defined in the **Occurs** and **Duration** options once on the scheduled day(s). To use this option, select **Occurs once a day at the schedule start time**.
Occurs every <x> <time unit>	The deployment occurs as defined in the **Occurs** and **Durations** options at the selected interval. To use this option, complete the following steps: 1. Select the **Occurs every <x> <time unit>** option. 2. Select a value from the **<x>** list. The values available changes according to the value selected from the **<time unit>** list. 3. Select a value from the **<time unit>** list (**Minute[s]**, **Hour[s]**).

Finally, select the duration of your recurring deployment. All recurring deployments require a start date. However, you have the option of selecting an end date for your recurring deployment or letting it run indefinitely.

5. Define a deployment **Start Date**. This is the date and time the recurring deployment will start.

   Tip: Select from the **12 hour** and **24 hour** options to change time listing values for both the **Start Date** and **End Date** calendars. When the **24 hour** option is selected, the **AM/PM** list is unavailable.

   a) Select a date from the **Start Date** calendar.
   b) Select a value from the **Hour** list.
   c) Select a value from the **Minute** list.
   d) Select a value from the **AM/PM** list.

6. Define a deployment **End Date**.

End Date Option	Instructions
To end the recurring deployment on a selected date:	1. Ensure the **No end date** checkbox is cleared. 2. Select a date from the **End Date** calender. 3. Select a value from the **Hour** list. 4. Select a value from the **Minute** list. 5. Select a value from the **AM/PM** list.

HEAT software

End Date Option	Instructions
To run the recurring deployment indefinitely:	Ensure the **No end date** checkbox is selected.

7. Click **Next**.

After Completing This Task:
Complete Configuring Deployment Information on page 309.

Package Deployment Order and Behavior Page

The packages selected for deployment can have their order and behavior edited. For instance, you may want a particular package deployed before another. Use the **Package Deployment Order and Behavior** page to edit order and behavior.
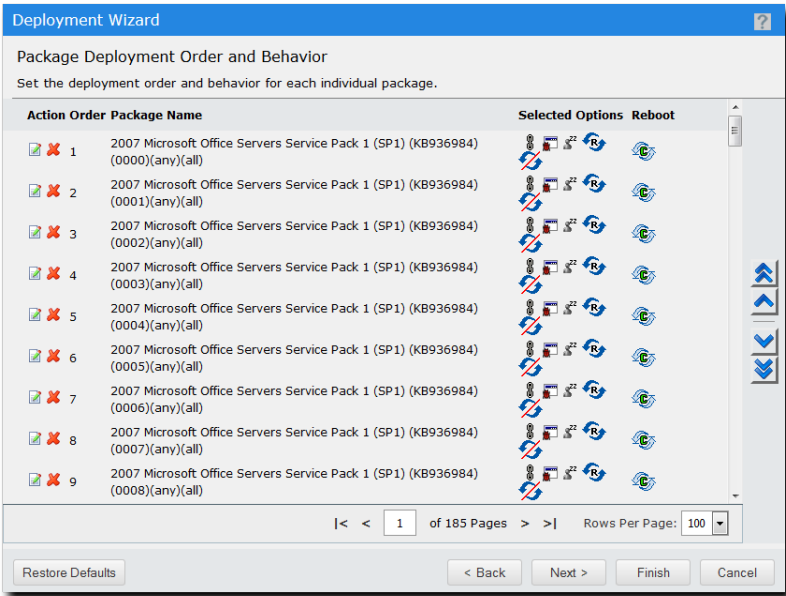
Figure 61: Package Deployment Order and Behavior Page

The following table describes each page column.

Table 125: Package Deployment Order and Behavior Columns

Column	Description
Action	Contains **Edit** and **Delete** icons. Click the **Edit** icon to open ***Package Deployment Behavior Options*** page, which you can use to change package behavior options. Click the **Delete** icon to remove the package from the deployment. For additional information on editing package behavior, refer to Selecting Deployment Behavior Options on page 322
Order	Indicates the order number of the package.
Package Name	Indicates the name of the package.
Selected Options	Displays icons that indicate behaviors selected for the package. Mouse over for a text description of the behavior. For additional information, refer to Behavior Icon Definitions on page 323.
Reboot	Displays icons that indicate whether a reboot follows the package deployment. For additional information, refer to Reboot Icon Definitions on page 324.

From this page, you can change the order that packages are deployed in using the page controls. For additional information on settings the package deployment order, refer to Selecting Deployment Behavior Options on page 322.

Note: Chained packages cannot be moved without first removing their chained status. When a package is chained, HEAT PatchLink DataCenter for Microsoft System Center determines the deployment order. However, when no longer chained, the package can be deployed at anytime following the chained deployments.

After defining deployment order and behavior, click **Next** to proceed to the Notification Options Page on page 327.

Setting Package Deployment Order
Set the deployment order to determine which packages are installed first.

Define the deployment order from the ***Package Deployment Order and Behavior*** page.

1. Select the package(s) you want to move within the queue.

Tip: You can remove a package from the deployment clicking its **Delete** icon (✖).

HEAT software

2. Move the selected packages within the queue.

Click the following icons to move packages to desired queue position.

Icon	Description
Double Up Arrow	Moves the selected package(s) to the top of the queue.
Up Arrow	Moves the selected package(s) up one queue position.
Double Down Arrow	Moves the selected package(s) to the bottom of the queue.
Down Arrow	Moves the selected package(s) down one queue position.

Tip: After editing package deployment order, you can restore the default order by clicking **Restore Defaults**.

3. [Optional] Edit deployment behavior options for packages by clicking the **Edit** icon (🖉).

For additional information, refer to Selecting Deployment Behavior Options on page 322.

Result: Package deployment order is defined. Click **Next** to proceed to the *Notification Options* page.

Selecting Deployment Behavior Options
Each package in a deployment can have its behavior changed by selecting behavior options.

Select deployment behavior options for a package from the *Package Deployment Behavior Options* page.

1. Select the check box for each behavior you want the package to use.

The behaviors available change for each package. For a complete list of behaviors and their descriptions, refer to Behavior Icon Definitions on page 323.

2. Define additional behaviors typing entries in the **Optional Flags** field.

For a complete listing of behavior flags, refer to Package Flag Descriptions on page 325.

3. Select a **Display** option.

This option defines the notification that deployment recipients receive when user notifications are enabled. Select one of the following options.

Option	Description
Behavior options settings	Displays the expected deployment behavior.

Option	Description
Package description	Displays the package description.

> **Note:** Modifying behavior options initiates a system reevaluation of the deployment, which may result in a change in the package order.

Result: The package enables the selected behaviors. Click **Next** to return to the ***Package Deployment Order and Behavior*** page.

Behavior Icon Definitions

Behavior icons appear on the ***Package Deployment Order and Behavior*** page and indicate the activities related to the deployment configuration.

The following table describes the deployment behavior icons and their descriptions. The icons representing the selected behaviors appear in the **Selected Options** column.

Table 126: Behavior Icon Definitions

Icon	Action	Use to
	Uninstall	Uninstall the packages.
	Force Shutdown	Force all applications to close if the package causes a reboot.
	Do Not Backup	Uninstall package without backing up files.
	Suppress Reboot	Prevent a reboot after installation.
	Quiet Mode	Suppress any user interfaces during the deployment.
	Unattended Setup	Set up packages in unattended mode.
	List Hot Fixes	Return a listing of hot fixes installed on the target devices.
	Force Reboot	Force a reboot regardless of package requirements.
	Reboot is Required	Indicate a reboot is required prior to completing the installation.
	Chain Packages	Set the package as chainable (package must support chaining).
	Suppress Chained Reboot	Suppress the reboot, so that other chained packages can be sent following this package. When creating multiple deployment jobs, this option is recommended.

◢ **HEAT**®software

Icon	Action	Use to
	Repair File Permissions	Repair file permissions following the package installation.
	Download Only	Distribute the package without running the package installation script.
	Suppress Notification	Suppress any user notifications during installation.
	Debug Mode	Run the package installation in debug mode.
	Do Not Repair Permissions	Suppress the repair of file name permissions after the reboot.
	May Reboot	Force a reboot, if required.
	Multi-User Mode	Perform the installation in multi-user mode.
	Single-User Mode	Perform the installation in single-user mode.
	Restart Service	Restart the service following the deployment.
	Do Not Restart Service	Suppress the restart of the service following the deployment.
	Reconfigure	Perform the system reconfigure task following deployment.
	Do Not Reconfigure	Suppress the system reconfigure task following deployment.

Note: When using a chained deployment, reboots are suppressed whenever possible. The final deployment is represented as `May Reboot` because HEAT PatchLink DataCenter for Microsoft System Center determines if the agent is in a *dirty state*. If so, a `System Task - Reboot` deployment is sent before deploying the remaining packages.

Reboot Icon Definitions
Reboot icons appear on the **Package Deployment Order and Behavior** page and determine the reboot conditions for a deployment.

The following table describes the reboot icons.

Table 127: Reboot Icon Definitions

Icon	Name	Reboot Status
	Reboot may occur	The device may be rebooted, dependent upon the package installer requirements (at the time of install).

Icon	Name	Reboot Status
	Reboot may occur chained	The device may be rebooted, dependent upon the package requirements. However if a reboot is required and the device is not rebooted, the device will enter a reboot state.
	Reboot required	No other (chainable or non-chainable) packages will be installed until the device reboots.
	Reboot required chained	Only chainable packages will continue to be installed until the device has been rebooted.
	Reboot will occur	The device will be rebooted following the package installation.

Click **Next** to proceed to the Notification Options Page on page 327 page.

Click **Finish** to create the deployments and proceed to the Deployment Confirmation Page on page 331.

Package Flag Descriptions
You can attach behavior to package deployments using package flags.

The following table defines flag behavior and their descriptions:

Table 128: Package Flag Descriptions

Description (flag behavior)	Display Flag	Select Flag
Perform an uninstall; can be used with -mu or -q.	-yd	-y
Force other applications to close at shutdown.	-fd	-f
Do not back up files for uninstall.	-nd	-n
Do not restart the computer when the installation is done.	-zd	-z
Use quiet mode, no user interaction is required.	-qd	-q
Use unattended setup mode.	-dmu	-mu
Install in multi-user mode[1]	N/A	-su
Restart service after installation[1]	N/A	-restart
Do not restart service after installation[1]	N/A	-norestart
Reconfigure after installation[1]	N/A	-reconfig
Do not reconfigure after installation[1]	N/A	-noreconfig

HEAT software

Description (flag behavior)	Display Flag	Select Flag
Download packages to `tmp` folder, but don't install[2]	N/A	-CACHEPACKAGES
Install packages cached in the `tmp` folder[2]	N/A	-INSTALLFROMCACHE

Tip: If you are patching Linux and Unix endpoints that receive content directly from vendor repositories, deployments may exceed your scheduled window because the patch content must first be downloaded, a process that may be excessively long. To reduce the likelihood of deployments that exceed maintenance schedules:

1. Cache the content to the endpoints by completing a deployment using the -CACHEPACKAGES flag. This deployment downloads the content, but doesn't install it.
2. Install the cached content by completing a second deployment using the -INSTALLFROMCACHE flag. The deployment skips the download of content, and installs the content already cached.

Description (flag behavior)	Display Flag	Select Flag
Ignores discrepancies between libraries available in different architectures[2]	N/A	-YUM_PROTECTED_MULTILIB
Skips packages with broken dependencies when updating the endpoint[2]	N/A	-YUM_SKIP_BROKEN
Performs a trial run of the deployment with no package changes made.[3]	N/A	-TRIAL_RUN
This package is chainable and will run Qchain.exe (Windows) or (UNIX/Linux).	-dc	-c
Suppress the final chained reboot.	-dc	-sc
Repair permissions.	-dr	-r
Deploy only.	-PLD1	-PLDO
No Pop-up	-PLN1	-PLNP
Debug	-PLDG	-PLDEBUG
Suppress Repair	-dsr	-sr
Force the script to reboot when the installation is done.	-1d	-1
Reboot is required.	N/A	-2
Reboot may occur.	N/A	-3
Reboot is required, and may occur.	N/A	-4

Description (flag behavior)	Display Flag	Select Flag
1. This flag applies to Linux and Unix operating systems only. 2. This flag applies to only Red Hat Enterprise Linux 7, Oracle Enterprise Linux 7, and CentOS Linux 7. 3. This flag applies to only Oracle Solaris 11.		

Notification Options Page

You can define whether users will receive notification of deployments and/or reboots, and if so, what the notification will contain using the **Notification Options** page of the **Deployment Wizard**.
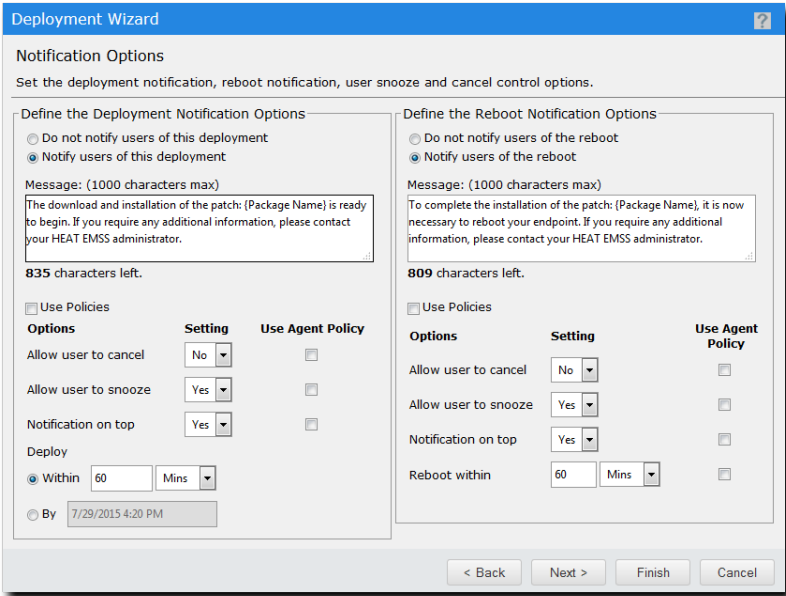
Figure 62: Notification Options Page

Note: When an agent is installed on a server where multiple users are logged in simultaneously, the deployment manager will provide each user with the ability to snooze or reject the deployment and/or reboot if snooze or reject is enabled.

For additional information on defining notification options, refer to Setting Notification Options on page 327.

After editing the **Notifications Options** page, click **Next** to view the Deployment Confirmation Page on page 331.

Setting Notification Options

During deployments, you can notify recipients that their endpoints are receiving deployment or require an endpoint. From the **Notification Options** page, you can define the message that recipients receive.

Define notification options from the **Notification Options** page.

1. Select a **Define the Deployment Notification Options** option.

   - **Do not notify users of this deployment**.
   - **Notify users of this deployment**.

2. If you selected the **Notify users of this deployment** option, complete the following substeps.

   a) [Optional] Type a notification in the **Message** field.
   b) Select whether you want to manually define remaining notification options or use the default settings defined in the Global Policy Set.

      - To manually define remaining notification options, ensure the **Use Policies** check box is cleared and continue to the next substep.
      - To use the default notification option settings defined in the agent policy set associated with the target endpoints, select the **Use Policies** check box and continue to the next step.

   c) Define the **Allow user to cancel** option.

      - To manually define this option, select *yes* or *no* from the **Setting** list.
      - To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

   d) Define the **Allow use to snooze** option.

      - To manually define this option, select *yes* or *no* from the **Setting** list.
      - To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

   e) Define the **Notification on top** option.

      - To manually define this option, select *yes* or *no* from the **Setting** list.
      - To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

      For additional information about this option, refer to

   f) Select and define a **Deploy** option.

      - To deploy the notification within a specific time frame, select the **Within** option and define the field and list (**Mins**, **Hours**, **Days**).
      - To deploy the notification by a specific deadline, select the **By** option and define a date and time.

        Use the calender controls that display to define the date and time, and then click **OK**.

3. Select a **Define the Reboot Notification Options** option.

   - **Do not notify users of this reboot**
   - **Notify users of this reboot**

4. If you selected the **Notify users of this reboot** option, complete the following substeps to define the remaining options.

    a) [Optional] Type a notification in the **Message** field.

    b) Select whether you want to manually define remaining notification options or use the default settings defined in the agent policy set associated with the target endpoints.

- To manually define remaining notification options, ensure the **Use Policies** check box is cleared and continue to the next substep.
- To use the default notification option setting defined in the agent policy set that applies to the target endpoints, select the **Use Policies** check box and continue to the next step.

    c) Define the **Allow user to cancel** option.

- To manually define this option, select *yes* or *no* from the *Setting* list.
- To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

    d) Define the **Allow use to snooze** option.

- To manually define this option, select *yes* or *no* from the *Setting* list.
- To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

    e) Define the **Notification on top** option.

- To manually define this option, select *yes* or *no* from the *Setting* list.
- To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

  For additional information about this option, refer to

    f) Define the **Reboot within** option.

- To manually define this option, enter a value in the field and select a value from the list (**Mins**, **Hours**, **Days**).
- To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

Result: Notification options are configured. Click **Next** to continue to the *Deployment Confirmation* page.

About the Show on Top Option

When creating a deployment or a Mandatory Baseline item, you can define the **Show on Top** options. Theses options determine whether notifications for deployments or reboots display on top or on bottom of all other open endpoint windows.

There are two different *Show on Top* options:

- A **Show on Top** option for **Deployment Notification Options**
- A **Show on Top** option for **Reboot Notification Options**

HEAT®software

The following table describes the notification dialog behaviors for each option setting (**Yes** or **No**).

Table 129: Always on Top Option Setting Description

Always on Top Option Setting	Notification Dialog Behaviour
Yes	The deployment or reboot notification displays as the topmost window. All other open windows display behind it.
No	The deployment or reboot notification displays as the bottommost window. All other open windows display in front of it.
	Note: When sending a deployment or reboot notification for the first time, the deployment or reboot notification displays as the topmost window (with the exception of some dialogs, such as **Windows Task Manager**). The notifications will display as the bottommost window in subsequent notifications.

Tip:

You can configure an agent policy to define the default **Show on Top** option setting for deployments and reboots when configuring a deployment or Mandatory Baseline. For additional information, refer to the following tasks:

- Creating an Agent Policy Set on page 230
- Editing an Agent Policy Set on page 236

Deployment Confirmation Page

This page displays the options that you've selected while completing the **Deployment Wizard**. Use this page to verify the options that you've chosen before finishing the wizard and beginning the deployment.

Deployment Confirmation Text

Figure 63: Deployment Confirmation Text

The upper portion of the page summarizes what options you selected while completing the **Deployment Wizard**.

Table 130: Deployment Confirmation Text

Text	Description
Job Name	The job name that you entered.
Schedule	The deployment schedule that you chose.
Manner	The manner that the patches are deployed.
Deployment notification	The option that you selected for notifying endpoint users of deployments.
Reboot notification	The option that you selected for notifying endpoint users of deployment reboots.

Text	Description
Total selected packages	The total number of packages included in the deployment.
	Note: Some patches include more than one package. If the number of packages in the deployment exceeds the number of patches you selected for deployment, one or more package likely includes multiple packages.
Total selected endpoints/groups	The total number of endpoints and groups included in the deployment. Both endpoints and groups add a value of 1. For example, if you select 5 endpoints and 1 group of 5 endpoints, the total is 6, not 10.
Notes	Any notes that you entered to describe the deployment and its purpose.

Note: When an agent is installed on a server where multiple users are logged in simultaneously, the deployment manager will provide each user with the ability to snooze or reject the deployment and/or reboot if snooze or reject is enabled.

Selected Packages
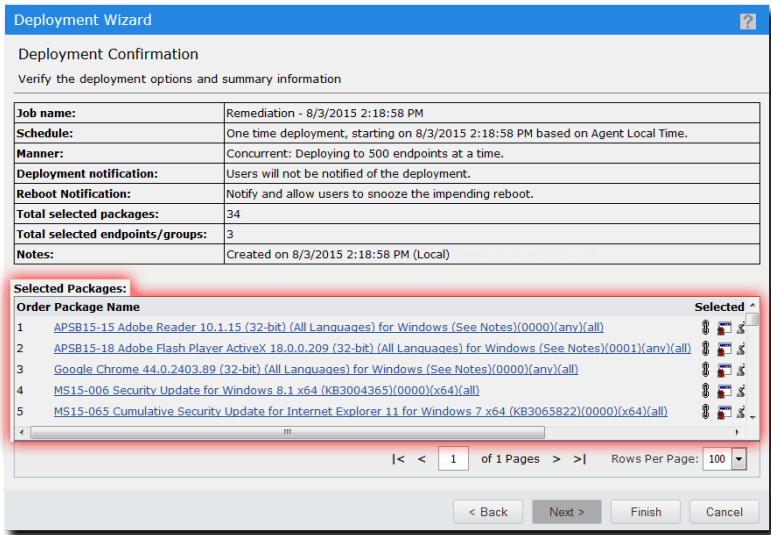
Figure 64: Selected Packages

The lower portion of the page lists the packages you chose for deployment.

Table 131: Selected Packages Column Descriptions

Column	Description
Order	The package's place in queue during the deployment. The order is optimized to minimize reboots.

Column	Description
Package Name	The name of the package being deployed.
Selected Options	The options and flags that you selected while configuring the deployment.
Reboot	Indicates if a reboot is required to complete installation of the package.
Endpoints/Groups	The number of endpoints and groups the package is deploying to.

After reviewing the ***Deployment Confirmation*** page, click **Finish** to proceed to the Deployment Summary Page on page 333.

Deployment Summary Page

This page lists all the options that you chose while completing the ***Deployment Wizard***. You can also use this page to cache packages before beginning the deployment.

All information displayed is identical to the info displayed on the Deployment Confirmation Page on page 331.

More importantly, you can use the page to *cache* packages before beginning the deployment.

What's *Caching*?

Caching is the process of commanding the HEAT Patch Manager DataCenter Server to download selected packages to its local hard drive.

Why Should I Cache Packages Before a Deployment?

- Caching ensures that packages are installed in an optimized, predictable order.
- Starting a deployment without caching the packages first may result in unpredictable endpoint behavior. Packages are deployed as they are downloaded. For example, if deployment includes multiple packages that require a reboot, endpoints may repeatedly enter a reboot state, or (even worse) endpoints force reboots multiple times, thus interrupting employee work.

HEAT®software

How do I Know When I Need to Cache Packages?

If you haven't already cached the packages you're deploying, the **Selected Pages** list includes red warning text and controls related to caching. We recommend waiting until caching completes before closing the **Deployment Wizard**. Read about caching information in the table that follows.
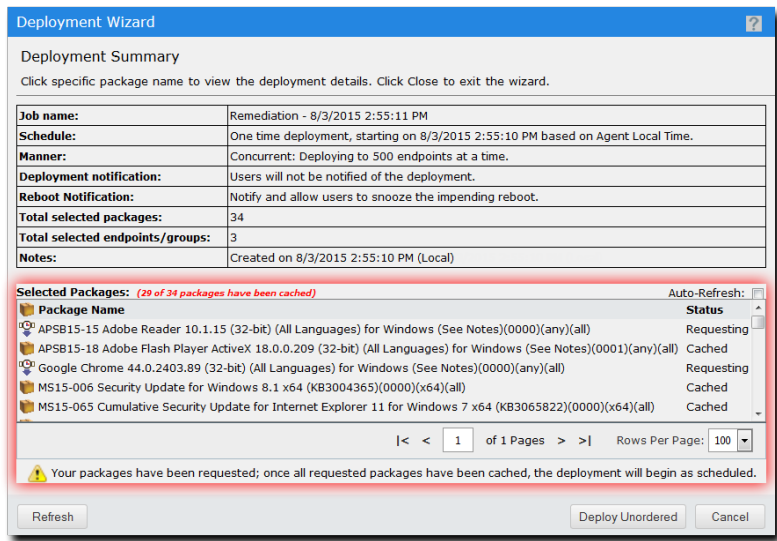
Figure 65: Deployment Summary Page - Packages Not Cached

Table 132: Selected Packages (Caching Packages)

Column	Description
Package Icon	Contains an icon that indicates if the package is cached or is being requested. Mouse over the icon for a description.
Package Name	The name of the package being deployed.
Status	Indicates the package cache status. • **Cached** • **Requesting**

If you don't see these controls, go ahead and close the wizard. You're all set because the packages are cached.
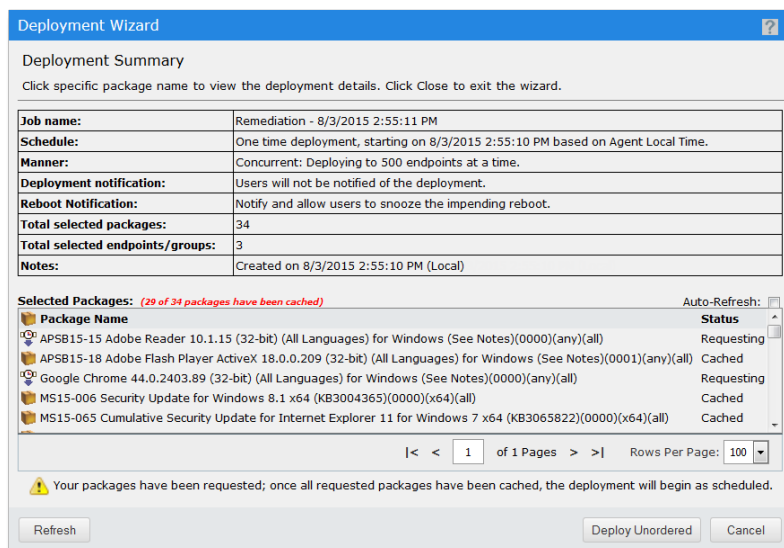
Figure 66: Deployment Summary Page - Packages Cached

After you finish reviewing the summary, click **Close** to dismiss the ***Deployment Wizard***.

The Deployment Details Page

The ***Deployment Details*** page shows targeted endpoint groups, targeted endpoints, deployment status, and deployment times for individual deployments.
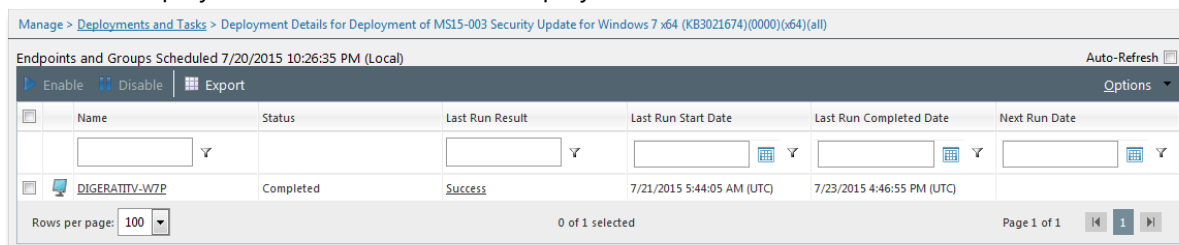
Figure 67: The Deployment Details Page

Viewing the Deployment Details

View the ***Deployment Details*** page for details about a specific deployment.

View the ***Deployment Details*** page by clicking a link from the ***Deployments and Tasks*** page.

1. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **Deployments and Tasks**.

HEAT software

2. Expand a deployment.

3. Click a package to view details about its deployment.

The Deployment Details Page Toolbar

The **Deployment Details** page toolbar contains functionality that you can use to enable and disable deployments and export deployment detail information.

The following table describes each toolbar button.

Table 133: Deployments Details Page Toolbar

Menu Item	Function
Enable	Enables the selected disabled deployment. For additional information, refer to Enabling Deployments on page 298.
Disable	Disables the selected enabled deployment. For additional information, refer to Disabling Deployments on page 298.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Deployment Details Page List

Details for individual deployments that you select from the **Deployments and Tasks** page reside in the **Deployment Details** page list.

Table 134: Deployment Details Column Definitions

Column	Description
Agent Status Icon	Indicates the status of the endpoint or endpoint group. For additional information, refer to Agent Module Status Icons on page 110.
Name	Indicates the name of the endpoint or endpoint group. The group name is a link; clicking the link displays the group membership and individual endpoint results.

Column	Description
Status	Indicates the current status of the deployment. Values include: • **Success** • **Not Patched** • **Not Deployed** • **Aborted** • **Failed** **Note:** A state of **Not Deployed** indicates that the patch either does not apply or has been marked *Do Not Patch*.
Last Run Result	Indicates the deployment's status when last ran. The status is a link; clicking the link displays the Package Deployment Results page.
Last Run Start Date	Indicates the date and time the deployment began.
Last Run Completed Date	Indicates the date and time the deployment completed.
Next Run Date	Indicates the next scheduled start date and time for this deployment.

Deployment Details for Package

You can view details for a package's deployment progress or outcome. This information may be helpful for troubleshooting purposes, such as if a package deployment fails.

Manage > Endpoints > Deployment Results for DIGERATITV-W7P

Deployment Information

Package Name: MS15-003 Security Update for Windows 7 x64 (KB3021674)(0000)(x64)(all)

Deployment Type: Endpoint Deployment

Associated Impact: Critical - 01

Deployment Result Detail: The deployment completed successfully.

Last Run Result: Success

Next Run Date:

Status: Success

Last Run Start Date: 7/20/2015 10:44:05 PM (UTC-07:00)

Last Run Completed Date: 7/23/2015 9:46:55 AM (UTC-07:00)

Figure 68: Deployment Results

The following table describes the text displayed in ***Deployment Information***.

Table 135: Deployment Information Fields

Field	Description
Package Name	Indicates the name of the package that was deployed.
Deployment Type	Indicates the deployment type.

⟋HEAT®software

Field	Description
Associated Impact	Indicates if the impact of the package.
Deployment Result Detail	Indicates the overall deployment status information.
Last Run Result	Indicates the result of the last time the endpoint performed the deployment.
Next Run Date	Indicates if the deployment is recurring and displays the date when the endpoint is to perform the deployment again.
Status	Indicates the result of the last time the endpoint performed the deployment. Values include: • **Success** • **Not Patched** • **Not Deployed** • **Aborted** • **Failed** **Note:** A state of **Not Deployed** indicates that the patch either does not apply or has been marked *Do Not Patch*.
Last Run Date	Indicates the status of the last time the endpoint performed the deployment.
Last Run Start Date	Indicates the date when the endpoint last started the deployment.
Last Run Completed Date	Indicates the date when the endpoint last finished the deployment.
Do Not Patch Reason	If a user has marked the package *Do Not Patch*, this text indicates the reason that the patch was marked for exclusion (if the user entered one).

Chapter

12

Using Patch Content

In this chapter:

- About Patch Content
- The Patch Content Page
- Working With Content
- The Patch Status Page
- Working with Content Items

The term *patch content* encompasses all updates across all endpoints registered to the HEAT PatchLink DataCenter Server for Microsoft® System Center Server.

Within HEAT PatchLink DataCenter Server for Microsoft System Center, content consists of:

- The content description.
- Signatures and fingerprints required to determine whether the content is patched or not patched.
- Associated package or packages for performing the patch.

Packages contain all vendor-supplied updates and executable code used to correct or patch security issues.

The following graphic illustrates the relationship between content and packages. Typically, a single content item is shared by multiple endpoints on multiple operating system platforms. There may be a series of separate patches to remediate the same content in different environments. The separate patches are grouped in packages identified by their respective product or OS. As a result, a series of packages may be included for one content item.

About Patch Content

The pages related to content display a list of patches, software updates, and other content. Once reported and analyzed, the content is distributed to your HEAT PatchLink DataCenter for Microsoft System Center server through the Global Subscription Service.

The agent installed on each endpoint checks for known content using the Discover Applicable Updates (DAU) task. The DAU scans the endpoint and sends the results back to the HEAT PatchLink DataCenter

HEAT®software

for Microsoft System Center server, which compares it with the list of known content. If the endpoint is missing a patch, a deployment can be set up to resolve the issues.
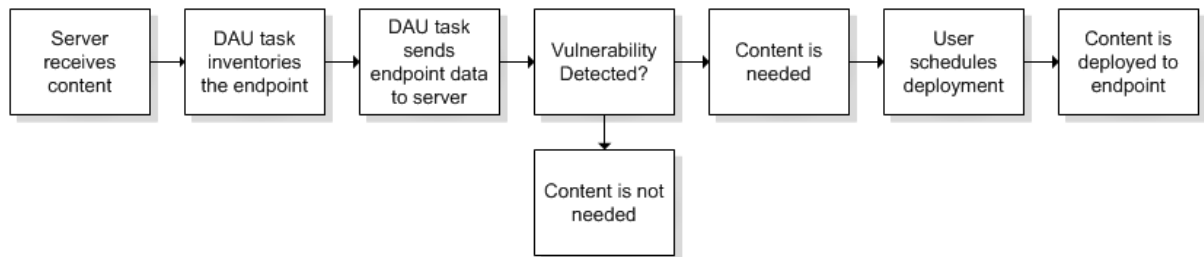
Figure 69: Discover Applicable Updates Task

Defining Content Structure

The structure of a content item allows the ability to create one patch applicable for many different operating systems and software versions. This allows for different packages and signatures capable of identifying the presence of patch files within an endpoint.

As depicted in the following diagram, for each content item you can have more than one signature. For each signature, you can have multiple fingerprints and pre-requisites. However, you can only have one package per signature.
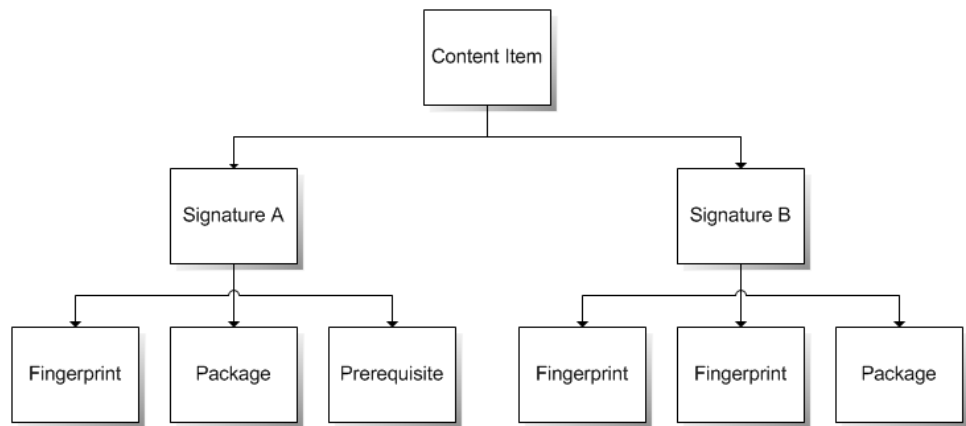
Figure 70: Patch Structure

Content Item

A content item is the container for the entire object. All properties set for the content item are viewed in content pages. Each security content item can have one or more signatures.

Signatures

Signatures recognize specific combinations of installed software in an operating system. Patches usually contain multiple signatures to compensate for differences within applications. A patch require different executables, libraries, and switches to run or detect the patch within different operating systems.

Fingerprints

A fingerprint can represent a unique file, folder, or other data value somewhere within a system. Each signature can contain one or more fingerprints detecting if a patch is present in the system.

Pre-requisites

A pre-requisite is a signature belonging to another patch with its own fingerprints.

Adding a pre-requisite to a signature requires the pre-requisite be met before analyzing the signature for the current patch. If that signature's pre-requisite is met, the agent will analyze the fingerprints of the current signature, otherwise they will be ignored and the patch will not be applied to the device.

Packages

The package contains the actual files used to update or install software on the system. Each package contains the script commands for installing the package files or running the executable that installs the patch.

Vulnerabilities

Vulnerabilities are patches that fix critical security issues. They are categorized by content type, which indicates the level of need for an endpoint to have the vulnerability deployed and installed.

Vulnerabilities are classified into the following content types:

All Critical	Displays all content that HEAT or the vendor recommends for immediate installation.
Critical (NEW)	Displays all English language content that HEAT or the vendor recommends for immediate installation that is less than thirty days old. By default, HPL automatically caches content in this category. After 30 days, critical patches are moved to **Critical > 30 Days**.
Critical > 30 Days	Displays all content that HEAT or the vendor recommends for immediate installation that is more than thirty days old. Most security patches are included in this category.
Critical International (NEW)	Displays all non-English language content that HEAT or the vendor recommends for immediate installation that is less than thirty days old. Most of the recent international security updates are included in this category. After 30 days, international patches are moved to **Critical > 30 Days**. This filter only returns results if you've used the *Subscription Service Configuration* dialog to select new content languages.
Critical and Not Superseded	Displays all content that HEAT or the vendor recommends for immediate installation. All patches in this category has not been supplanted by newer patches.

HEAT software

Critical but Superseded	Displays all content that HEAT or the vendor recommends for immediate installation. Content in this category has been supplanted by new content.

Software Content

Software content consists of content intended to keep software up to date.

You can review software content in the following categories:

Software All	Displays available software. This category combines the **Software**, **Recommended**, and **Informational** types.
Software Installers	Displays available software installers.
Software Updates (Not Critical)	Displays updates to existing software. These patches are not critical to the applicable software's operation.

In addition to the categories listed above, you can also view a list of all available software security content.

Other Content

Other content includes items that are not directly related to patching an endpoint or updating software. It is categorized by content type, which indicates the level of need for an endpoint to have the vulnerability deployed and installed.

Other content items are classified into the following content types:

Not Applicable	Displays content that doesn't apply to your endpoints.
Not Critical	Displays a list of content applicable to your endpoints, but is not critical for security or operations (content listed under **All Critical**, **Critical > 30 Days**, and **Critical and Not Superseded**).
Detection Only	Displays content that contains signatures common in vulnerabilities. This content contains no patches and are only used in the detection process.
Informational	Displays content that detects a condition that HEAT or the vendor has declared as informational. If the report has an associated package, you may want to install it as your discretion.
Policy	Displays content that impacts policy.
Recommended	Displays content that HEAT or the vendor recommends installing. The content is not critical or security related, but is useful and should be applied end user convenience.
Tasks	Displays tasks that administrators may use to run various virus detections across their network. Anti-Virus tools and updates are included in this category.

Virus Removal	Displays a list of content that removes viruses and other malware.
Critical & Not Superseded/Recommended	Displays all content classified as **All Critical** , **Critical and Not Superseded**, and **Recommended**.

The Patch Content Page

Within HEAT PatchLink DataCenter for Microsoft System Center, you can view all vulnerabilities and software available for deployment from the ***Patch Content*** page. This page contains a variety of filters that you can use to view content relevant in your enterprise.

Figure 71: The Patch Content Page

To Access the Content

Review content to see which content items are available and which items you may want to deploy to your managed endpoints.

1. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **My Default Patch View**.

2. Choose filter settings to display the content you're looking for.

Patch Content Filters

When using the *Patch Content* page, use the page filters to reduce the list to a manageable scope. This topic describes how each *Patch Content* page filter works.

Regardless of the navigation menu selection chosen to open the *Patch Content* page, the same filters are always available. You may need to toggle the **Show Filters / Hide Filters** button to display them. All filters can be used in combination with each other.

Filters

Name or CVE-ID	Use this field to filter the page by patch name or a patch's Common Vulnerability and Exposures ID.
Content type	Use this drop-down list to filter the page to a certain content type. See the **Content Types** list below for more info on what content is in each type.
Vendor	Use this drop-down list to filter the page to display content from only certain vendors. All vendors for content replicated from the Global Subscription Service or imported from HEAT Content Wizard are listed.
	Note: When viewing Custom Patch Lists, only applicable vendors are available for selection.
Vendor release date	Use this drop-down list and field to filter the page for content released after (or before) a date that you define. To define a date, either use the calendar icon to select one, or type the date in a mm/dd/yyyy format.
Applicability	Use this drop-down list to filter the page for content that applies (or doesn't apply) to your enterprise endpoints (or groups).
State	Use this drop-down list to filter the page for content that is in an enabled or disabled state.
Detection status	Use this drop-down list to filter the page for content that has been installed (or hasn't been installed) on endpoints.

Show results for	Use this drop-down list to filter the page for content that applies only to the selected group. Select the **Include sub-groups** to include the group's child groups in the filtering process.

Content Types

The **Content type** filters contains a list of selectable content categories. The list below describes what content is includes in each category.

All	Displays all content available from the Global Subscription Service.
All Critical	Displays all content that HEAT or the vendor recommends for immediate installation.
Critical (NEW)	Displays all English language content that HEAT or the vendor recommends for immediate installation that is less than thirty days old. By default, HPL automatically caches content in this category. After 30 days, critical patches are moved to **Critical > 30 Days**.
Critical > 30 Days	Displays all content that HEAT or the vendor recommends for immediate installation that is more than thirty days old. Most security patches are included in this category.
Critical International (NEW)	Displays all non-English language content that HEAT or the vendor recommends for immediate installation that is less than thirty days old. Most of the recent international security updates are included in this category. After 30 days, international patches are moved to **Critical > 30 Days**. This filter only returns results if you've used the *Subscription Service Configuration* dialog to select new content languages.
Critical and Not Superseded	Displays all content that HEAT or the vendor recommends for immediate installation. All patches in this category has not been supplanted by newer patches.
Critical but Superseded	Displays all content that HEAT or the vendor recommends for immediate installation. Content in this category has been supplanted by new content.
Software All	Displays available software. This category combines the **Software**, **Recommended**, and **Informational** types.
Software Installers	Displays available software installers.
Software Updates (Not Critical)	Displays updates to existing software. These patches are not critical to the applicable software's operation.
Not Applicable	Displays content that doesn't apply to your endpoints.

/HEAT®software

Not Critical	Displays a list of content applicable to your endpoints, but is not critical for security or operations (content listed under **All Critical**, **Critical > 30 Days**, and **Critical and Not Superseded**).
Detection Only	Displays content that contains signatures common in vulnerabilities. This content contains no patches and are only used in the detection process.
Informational	Displays content that detects a condition that HEAT or the vendor has declared as informational. If the report has an associated package, you may want to install it as your discretion.
Policy	Displays content that impacts policy.
Recommended	Displays content that HEAT or the vendor recommends installing. The content is not critical or security related, but is useful and should be applied end user convenience.
Tasks	Displays tasks that administrators may use to run various virus detections across their network. Anti-Virus tools and updates are included in this category.
Virus Removal	Displays a list of content that removes viruses and other malware.
Critical & Not Superseded/ Recommended	Displays all content classified as **All Critical** , **Critical and Not Superseded**, and **Recommended**.

The Patch Content Page Toolbar

Each page you can use to deploy content contains a toolbar of common functions.

The following table describes the toolbar functions used in each content page.

Table 136: Content Pages Toolbar Functions

Button	Function
Enable	Enables a selected disabled content item. For additional information, refer to Enabling Content Globally on page 354.
	Note: If no content items are disabled, **Enable** is unavailable.
Disable	Disables a selected enabled content item. For additional information, refer to Disabling Content Globally on page 353.
Do Not Patch...	Disables the selected patch for specific groups and endpoint that you select. For more information, see Disabling Content for Groups/ Endpoints on page 355.
Update Cache	Updates the package cache for the selected content item. For additional information, refer to Updating the Cache on page 359.

Button	Function
Deploy...	Opens the ***Deployment Wizard***. For additional information, refer to Using the Deployment Wizard on page 303.
Scan Now...	Prompts the Discover Applicable Updates task to launch immediately and scan all agent-managed endpoints within your network for vulnerabilities. For additional information, refer to Scanning Endpoints for Vulnerabilities on page 360.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Patch Content Page List

Use the page list to view information about each patch and the deployment information for it.

The following table describes the ***Patch Content*** page list.

Table 137: Column Definitions

Column	Icon	Definition
State	📄	The content item state, which indicates when the server downloaded the content item metadata. For additional information, refer to Content Status and Type on page 349.
Package Status	📦	The cache status for the content item, which indicates if the server downloaded the content item packages. For additional information, refer to Content Icons and Descriptions on page 350.
Name	N/A	The content item name, which links to the ***Patch Status*** of the item. For additional information, refer to The Patch Status Page on page 361.

HEAT software

Column	Icon	Definition
Content Type	N/A	Indicates the content item type. For more information, see one of the following topics: • Vulnerabilities on page 341 • Software Content on page 342 • Other Content on page 342
Vendor	N/A	The name of the vendor that created the software in the content item.
Vendor Release Date	N/A	The date and time that the vendor released the software in the content item.
Number of endpoints which came up Patched	✓	The number of endpoints patched with the content item.
Number of endpoints which came up Not Patched	❌	The number of endpoints not patched with the content item.
Total applicable	Σ	The number of endpoints that the content item applies to.
Number of endpoints which came up Do Not Patch	⊟	The number of endpoints that administrators have created a patch exception for.
Percent patched	%	The the percentage of applicable endpoints patched with the content item.

Additionally, you can expand each content item by clicking its arrow (**>**). The following table describes each field that displays when you expand a content item.

The following detail information appears on this page.

Table 138: Content Item Field Descriptions

Name	Description
Beta	Indicates if the content item is in beta.
Downloaded on (UTC)	The date and time on which the content was downloaded.
Associated packages	The number of packages associated with the content item.
Package status	The cache status for the content item packages.
HPL ID	The HPL identifier for the content item.
State	The enabled/disabled/completed status of the content item.

Name	Description
Enabled/Disabled by	The HPL user who last disabled or enabled the content.
Enabled/Disabled date (Server)	The date and time the content was disabled or enabled.
Enable/Disable reason	The reason the user provided for disabling or enabling the content. You can click the **Edit** link to change the reason.
Vendor product ID	The identifier given to the security content item by the vendor.
Vendor release date/time (UTC)	The date and time the vendor released the software in the content item.
Common Vulnerability Exploit (CVE) [1]	The CVE number for the content.
Vulnerability Code Description [1]	A description of the vulnerability associated with the content item.
Reference Text [1]	The reference text(s) associated with the content item vulnerability.
Description [1]	The narrative description of the distribution package. This section may include important notes about the content item and a link to more information.
[1]This meta data appears conditionally based on whether it was added for the content item. Additionally, there may be multiple instances of each meta data section.	

Content Status and Type

An icon in the **Status** column indicates the status of content items. The menu options and filter criteria that you select determines which content items are displayed. You can set the available filters to display content items of a certain status type.

Table 139: Status and Descriptions

Status	Description
New	Downloaded from the Global Subscription Service since the last session.
Current	Present content items residing on HEAT PatchLink DataCenter Server for Microsoft System Center.
Tasks	System task package.
Local	Locally created package.
Beta	Released to the HEAT BETA community.

HEAT software

The following table includes descriptions of the security content status icons.

Table 140: Security Content Status Icons and Descriptions

New	Current	Beta	Status Description
			Active content.
			The content has been disabled.

Content Cache Status and Type
A content item may have any number of packages associated with it. A package contains the patch to address the security issue. Each package may be cached (downloaded) from the Global Subscription Service.

The downloading of packages can occur automatically if the security content item impact is rated as critical or if a deployment has been created for a particular package or content item. Selecting the **Package Status** icon displays a list of the individual packages associated with the content item.

Content Icons and Descriptions
An icon in the **Package Status** column indicates the cache status of content items. The menu options and filter criteria that you select determines which content items are displayed. You can set the available filters to display content items of a certain status type.

The content status icons and their status are classified as follows:

Table 141: Security Content Status Icons and Descriptions

New	Current	Tasks	Local	Description
			N/A	The package is not cached.
			N/A	The package has been scheduled to be cached or is in the process of being cached.
			N/A	An error occurred while trying to cache the package.
				The package is cached and ready for deployment.
				The package is currently deploying (animated icon).

New	Current	Tasks	Local	Description
				The package is disabled.

Content Name

The names of content items typically include the vendor (manufacturer of the content item) and specific application and version information.

Working With Content

There are several tasks designed to assist with management and deployment of content items. These are available from buttons located within the toolbar on the **Review** pages for the individual content types.

These tasks include:

-
-
-
- Disabling Content on page 351
- Updating the Cache on page 359
- Disabling Content for Groups/Endpoints on page 355
- Enabling Patches for Groups/Endpoints on page 358
-
-
- Deploying from the Patch Content Page on page 359
- Scanning Endpoints for Vulnerabilities on page 360
- Exporting Content Data on page 361

Disabling Content

All content downloaded from the Global Subscription Service can be toggled between disabled and enabled states. You can disable content either globally or per endpoint.

Disabling Content Globally

Disable content globally when you don't want it to be installed on *any* endpoint in your network. Globally disabling content prevents it from being deployed mistakenly. Globally disabled content can be re-enabled at any time.

⚡HEAT®software

Disabling Content by Groups or Endpoints (also known as *Do Not Patch*)

Using the *Do Not Patch* feature, you can disable content for groups or endpoints that you choose. Use *Do Not Patch* when a particular patch is causing problems, or would cause known problems, for a group or endpoint. Content disabled by endpoint/group can also be re-enabled at any time.

You should know a few things about *Do Not Patch*:

- *Do Not Patch* is considered a special patch state.

  - The *Do Not Patch* state takes precedence over all other patch states, such as *patched*, *not patched*, and *not applicable*.
  - Content marked *Do Not Patch* is considered a special state different from *disabled* since it can still be deployed to most of your endpoints.

  > **Note:** If you need find content marked *Do Not Patch* when filtering list pages or reports, clear all page filters and sort by the **Do Not Patch** column (🔴).

  - Patches marked *Do Not Patch* exclude selected endpoints from its patch compliance score.

- If you mark content as *Do Not Patch* after it has already been installed on the endpoints you select:

  - The endpoints still enters a *Do Not Patch* state although the patch is installed.
  - You must uninstall the patch manually from those endpoints (because patches cannot be retroactively uninstalled). The *Do Not Patch* feature *does not* uninstall patches from endpoints.

- If you mark content as *Do Not Patch* for a group, that group's child hierarchy is also considered *Do Not Patch*.
- If you mark content included in a mandatory baseline as *Do Not Patch*, the endpoints or groups marked *Do Not Patch* are exempt from that patch.

***Do Not Patch* use example:**

Say your organization has mission-critical servers that require an older version of Java to operate. Although you should patch most of your endpoints with the latest version to secure them, these mission-critical servers need to remain on the older version to continue operations. In this case, mark the mission-critical servers as *Do Not Patch* to exempt them from a more recent version of Java.

Disabled/Enable Comments

When disabling/enabling content, you have the option of entering a reason for completing the action.

- A disable comment is useful for tracking why a content item is disabled. The default reasons include:
  - OS / System conflict
  - Application conflict
  - High incidence of installation failures
  - Not approved
- Typically, content is re-enabled when the reason for originally disabling it is resolved. Use re-enable comments to track why content has been reintroduced. The default enable reasons are:
  - Resolved OS / System conflict
  - Resolved application conflict
  - Resolved installation failures
  - Approved

Tip: Disable/enable comments also appear in related reports.

Disable/Enable Tips and Behaviors

- After a patch is disabled/re-enabled, you can edit the reason by expanding the patch's metadata from the **Patch Content** page list and clicking the Enable/Disable reason **Edit** link.
- If you disable a patch that's cached, it isn't updated if a new version of the patch is released.
- You can't retroactively remove a patch from a deployment that's scheduled or in-progress by disabling the patch. If you schedule a deployment but then globally disable a patch that's included, that patch is still deployed. If you need to stop the patch from being deployed, abort the deployment instead of disabling the patch.

Disabling Content Globally

Disabling a patch prevents it from being deployed.

1. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **My Default Patch View**.
2. Filter the page to show content that's enabled.
   a) If necessary, click **Show Filters** to toggle the page filters.
   b) Select page filters. Make sure the **State** filter has **Enabled** selected.
   c) Click **Update View**.
3. Find and select the content you want to disable.
4. Click **Disable**.

Note: If you disable a content item that's already been cached, the package will not be updated if a new version of the content item is released.

HEATsoftware

5. [Optional] Choose a reason for disabling the content.

- To enter a new reason, type it in the field.
- To choose a reason that's already been used, select it from the drop-down menu.

6. Click **Disable**.

> **Note:** You can't retroactively remove a patch from a deployment that's scheduled or in-progress by disabling the patch. If you schedule a deployment but then globally disable a patch that's included, that patch is still deployed. If you need to stop the patch from being deployed, abort the deployment instead of disabling the patch.

Result: The content is disabled. To confirm, filter the page to display disabled content and confirm it's listed.

Enabling Content Globally
Enabling a previously disabled content item allows you to deploy the content item to your endpoints.

1. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **My Default Patch View**.

2. Filter the page to show content that's disabled.

   a) If necessary, click **Show Filters** to toggle the page filters.
   b) Select page filters. Make sure the **State** filter has **Disabled** selected. Select the **Content type** filter **All** value to make sure all disabled content is displayed.
   c) Click **Update View**.

3. Find and select the content you want to enable.

4. Click **Enable**.

5. [Optional] Choose a reason for disabling the content.

- To enter a new reason, type it in the field.
- To choose a reason that's already been used, select it from the drop-down menu.

6. Click **Enable**.

Result: The content is re-enabled.

Disabling Content for Groups/Endpoints

You can disable patches for specific groups and endpoints, placing them in a *do not patch* state for that patch.

1. Open a page that list patches *Patch Content* page.
   - Select **Review** > **My Default Patch View**, or any other **Review** menu item to open the *Patch Content* page.
   - Select **Manage** > **Endpoints**, click an endpoint link, and then select the **Vulnerabilities/Patch Content** tab.
   - Select **Manage** > **Groups** and select the **Vulnerabilities/Patch Content** view.

2. [Optional] Use the *Patch Content* page filters and click **Update View** to find patches that you want to disable for a group/endpoint.

   > **Tip:** If the filters are not displayed, click **Show Filters**.

3. Select the patch you want to disable, and then click **Do Not Patch**.

4. Complete the *Do Not Patch Groups and Endpoints* wizard.

The Do Not Patch Groups and Endpoints Wizard

Use this wizard to mark the patch you've selected as "do not patch" for groups and endpoints that you choose. This wizard includes two to three pages, depending on the actions you choose while using it:

Select Groups and Endpoints to Mark as 'Do Not Patch' on page 355	Use this page to exclude specific groups and endpoints from receiving the patch.
Do Not Patch Reason on page 357	Use this page to record a reason why you're marking the patch as 'Do Not Patch'. You can see this record later to remind yourself why the patch is excluded.
OK to Patch Reason on page 358	If you're removing the patch exclusion for particular groups or endpoints later, you can also provide a reason on why you're marking it 'OK to Patch'.

Select Groups and Endpoints to Mark as 'Do Not Patch'

After opening the *Do Not Patch Groups and Endpoints* wizard, select groups, endpoints, or a combination of both. These endpoints (and groups) won't allow the patch that you selected to be applied to them when the wizard is completed.

From this page, you can either:

- Create a patch exception for groups, endpoints, or a combination of both by adding them to the **Do Not Patch** list.
- Remove existing patch exceptions for groups or endpoints (after resolving the reason that an exception was created).

When you're done modifying the **Do Not Patch** list, click **Add Reason** to proceed.

HEAT software

Adding Groups and Endpoints to the 'Do Not Patch' List
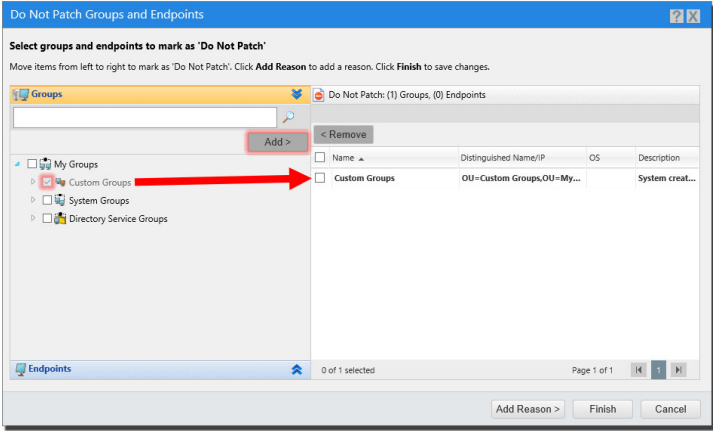
Figure 72: Add Group/Endpoint to Do Not Patch List

Add groups or endpoints to the **Do Not Patch** list when:

- You're creating a brand new patch exception.
- You're adding more groups/endpoints to the **Do Not Patch** list when exceptions for the patch already exist.

Toggle between groups and endpoints by clicking the **Groups** and **Endpoints** headers.
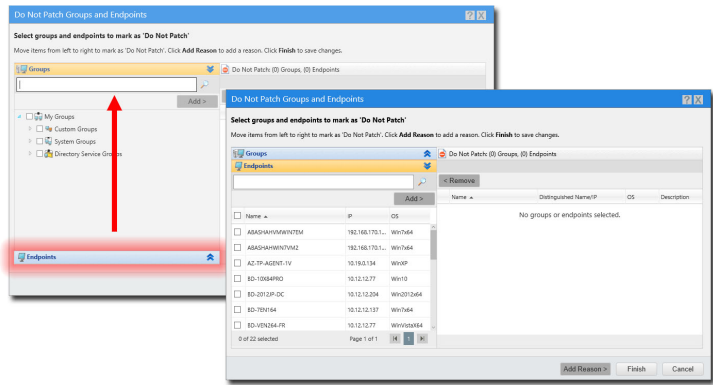
Figure 73: Toggle Group/Endpoint

Groups Panel

Use this panel to create a patch exception for a group.

- Expand the tree to find the groups you want to select.
- You can also type specific group names into the search field.

Endpoints Panel

Use this panel to search for specific endpoints that you want to select.

Removing Groups and Endpoints from the 'Do Not Patch' List
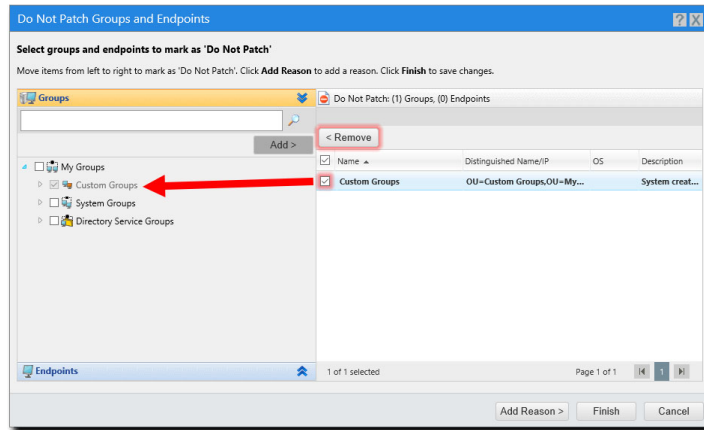
Figure 74: Remove Group/Endpoint

Remove groups or endpoints from the **Do Not Patch** list when you've resolved the reason that you created an exception in the first place.

Tip: You may never want to remove groups/endpoints from the **Do Not Patch** list.

Do Not Patch Reason
When you add groups/endpoints to the **Do Not Patch** list for a patch, you should select a **Do Not Patch** reason. These optional reasons are available for tracking and reporting purposes.

For example, while reviewing reports about networking patching, you can reference this reason for info on why an endpoint wasn't patched.
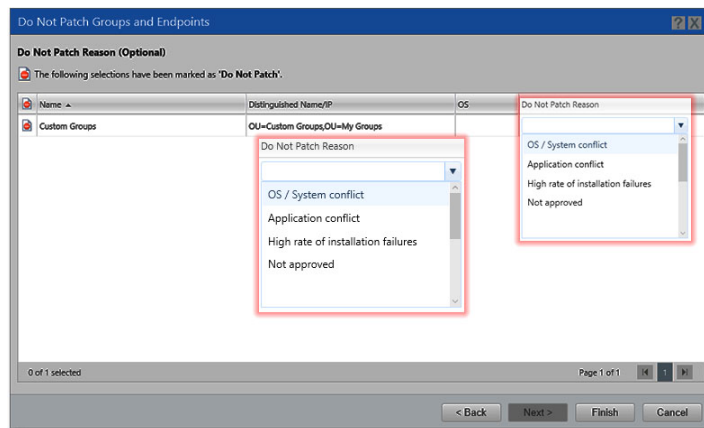
Figure 75: Do Not Patch Reasons

A **Do Not Patch Reason** drop-down is available for each group/endpoint on the **Do Not Patch** list.

- To select from a list of pre-created system reasons, select one from a group/endpoint drop-down.
- To create your own custom reason, type a reason instead.

Note: If you aren't adding groups/endpoints to the **Do Not Patch** list, this page won't appear.

OK to Patch Reason
When you remove groups and endpoints from the **Do Not Patch** list for a patch, you should select an **OK to Patch** reason. These optional reasons are available for tracking and reporting purposes.

For example, if your manager asks why a patch that was marked as **Do Not Patch** is later changed to **OK to Patch**, you can reference this reason to find out why the patch was approved.
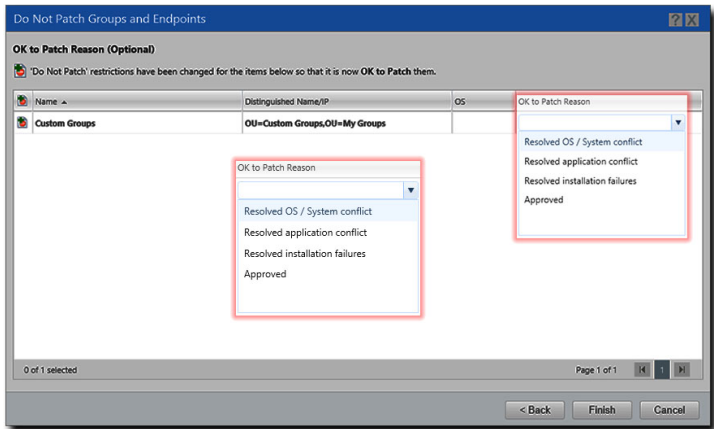
Figure 76: OK to Patch Reasons

A **OK to Patch Reason** drop-down is available for each group/endpoint removed from the **Do Not Patch** list.

- To select from a list of pre-created system reasons, select one from a group/endpoint drop-down.
- To create your own custom reason, type a reason instead.

Note: If you aren't removing groups/endpoints from the **Do Not Patch** list, this screen won't appear.

Enabling Patches for Groups/Endpoints

After you've resolved the reason that you've marked a group or endpoint as "Do Not Patch," you can go back and re-enable it.

1. Open a page that list patches *Patch Content* page.

- Select **Review** > **My Default Patch View**, or any other **Review** menu item to open the *Patch Content* page.
- Select **Manage** > **Endpoints**, click an endpoint link, and then select the **Vulnerabilities/Patch Content** tab.
- Select **Manage** > **Groups** and select the **Vulnerabilities/Patch Content** view.

2. [Optional] Use the *Patch Content* page filters and click **Update View** to find patches that you want to enable for a group/endpoint.

> **Tip:** If the filters are not displayed, click **Show Filters**.

3. Select the patch you want to enable, and then click **Do Not Patch**.

4. Complete the *Do Not Patch Groups and Endpoints* wizard. From the *Select Group and Endpoints to Mark as 'Do Not Patch'* page, remove the groups/endpoints that you want to patch again from the **Do Not Patch** list.

Updating the Cache

Updating the cache initiates a process that gathers the packages associated with the selected vulnerability and copies those packages to your HEAT PatchLink DataCenter Server for Microsoft System Center server.

Within **Review** pages, the **Update Cache** feature is designed to assist with the management and deployment of content items.

> **Note:** For optimum installation order, HEAT recommends caching content prior to deployment. Failure to cache content prior to deployment may result in repeated endpoint reboots that interrupt workflow on those endpoints.

1. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **My Default Patch View**.

2. If necessary, select filter criteria for to find content you're looking for and click **Update View**.

3. Select the check boxes associated with the content to cache.

4. Click **Update Cache**.

> **Step Result:** The *Warning* dialog box opens, informing you that the update request and this action may take an extended period of time.
>
> > **Note:** The cache will not be updated for disabled content items that have had a new version released.

5. Click **OK**.

Result: The selected content begins caching.

Deploying from the Patch Content Page

Within HEAT PatchLink DataCenter for Microsoft System Center, content can be deployed from a number of pages, including any *Content* page. When deploying from these pages, the *Deployment Wizard* is preconfigured according to the content you select.

For additional information, refer to About Deployments on page 289.

HEAT®software

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

2. From the list, select the content you want to deploy.

> **Note:** If you select the **Select All** checkbox, all content visible on the page is selected. However, you can select all available content by clicking the **Select All** link.

3. Click **Deploy**.

Result: The *Deployment Wizard* opens, preconfigured to deploy the selected content.

After Completing This Task:
Review and complete subsequent tasks.

Scanning Endpoints for Vulnerabilities

You can initiate a Discover Applicable Updates (DAU) task at any time. When you initiate this task, the agent scans its host endpoint for vulnerabilities and inventory. Scan results are then uploaded to HEAT PatchLink DataCenter for Microsoft System Center, which you can view.

From the *Content* pages, you can schedule a DAU tasks for all managed endpoints in your network.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

2. Click **Scan Now**.

   Step Result: The *Scan Now* dialog opens.

3. Select the **Yes, scan all endpoints**.

4. Click **Schedule**.

   Step Result: A notification displays, informing you that the scan has been scheduled. The notification contains a link to view the scheduled deployment.

   > **Note:** Although the DAU task is scheduled for immediate execution, it does not execute until the next agent check in.

5. Click **Close**.

Result: The dialog closes.

Exporting Content Data

From the various content pages, you can export all information listed on the page to a comma separated value (`.csv`) file. The exported information can be used for reporting and analytical purposes.

For additional information, refer to

The Patch Status Page

Each patch features a page that lists statistics and details about itself: the **Patch Status** page.
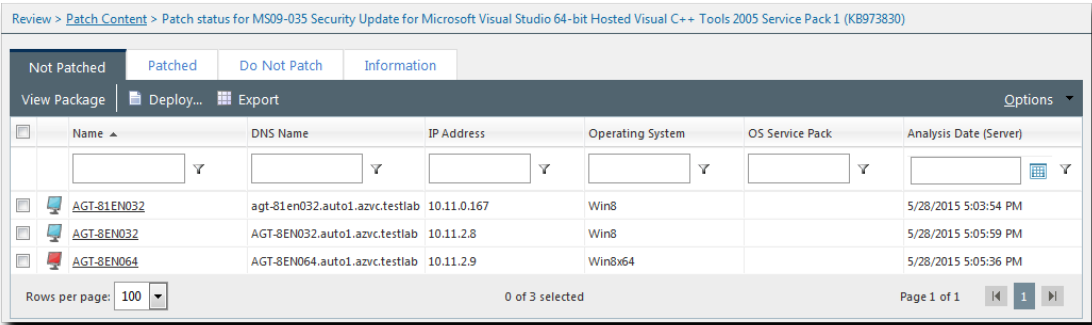
This page is divided into four tabs:

Not Patched	This tab lists each endpoint that the patch applies to. However, the patch is not installed on these endpoints yet. View this page to find out which endpoints you still need to patch for a vulnerability.
Patched	This tab lists each endpoint that the patch is installed on. You can view this page after a deployment to confirm that your endpoints are patched.
Do Not Patch	This tab lists each endpoint marked as *Do Not Patch* for a given patch (*Do Not Patch* means the patch is exempt from being installed on the endpoint). If you determine that an endpoint shouldn't have a certain patch installed, check this tab to see if the endpoint is already marked *Do Not Patch*.
Information	This tab lists metadata about the patch itself.

HEAT software

Viewing Content Patch Statuses

You can view details of a specific content item by selecting the desired content item and clicking the item name.

View a content item's patch status by clicking a content item's hyperlink from a content page list. The **Patch Status** page represents the results of the content item analysis and displays detailed data regarding the content item.

1. From the **Software Library** workspace, select **HEAT PatchLink DataCenter** > **Security Updates** > **All Security Updates**.

2. Select a content item from the list. You can only view the details of one content item at a time.

3. Click the content item's name.

Result: The **Patch Status** page for the selected content item opens.

The Patch Status Page Toolbar

Each tab on the **Patch Status** page contains an identical toolbar. Use this toolbar to complete tasks related to applicable content item.

The following table describes each button in the toolbar.

Table 142: Patch Status Page Toolbar Buttons

Button	Description
View Package	Opens the **Packages** page and displays the package for the applicable content item.
Deploy...	Opens the **Deployment Wizard**. For additional information, refer to Using the Deployment Wizard on page 303.
Export	Exports the page data to a comma-separated value (.csv) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

The Patch Status Page List

Each tab in the **Patch Status** page displays basic information for managed endpoints.

The following table describes the **Patch Status** page columns.

Table 143: Patch Status Page Column Descriptions

Column	Description
Endpoint Status	Displays an icon that indicates the endpoint status. For additiona information, refer to Endpoint Status on page 363.
Name	Indicates the name of the endpoint.
DNS Name	Indicates the DNS name for the endpoint. The endpoint IP address displays if it does not have an assigned DNS name.
IP Address	Indicates the IP address of the endpoint.
Operating System	Indicates the operating system (abbreviated) running on the endpoint.
OS Service Pack	Indicates any additional operating system version information.
Analysis Date	Indicates the date the agent on the device last ran the Discover Applicable Updates system task.

Endpoint Status

An icon in the **Endpoint Status** column indicates the agent status and activity on an endpoint.

Also displayed in the **Patch Status** page is the status of the agent installed on the endpoint.

Table 144: Endpoint Status Icons

Active	Pending	Description
	N/A	The agent is currently working on a deployment (animated icon).
		The agent is idle, and has pending deployments.
		The agent is offline.

HEAT software

Active	Pending	Description
	N/A	The agent is offline because the Endpoint Distribution Service the endpoint is connected to is offline or requires an update.
		The agent is sleeping due to its hours of operation settings.
		This agent is disabled.
		The agent is offline and is in a chain status (can accept chained deployments until only after reboot).
		The agent is offline and is in a reboot status (can accept no more deployments until after it reboots).
		The agent is in a chain status (the agent can accept chained deployments only until after a reboot).
		The agent is in a reboot status (the agent can accept no more deployments until after it reboots).
		The agent is in a chain status (the agent can accept chained deployments only until after a reboot) and is sleeping due to its hours of operation settings.
		The agent is in a reboot status (the agent can accept no more deployments until after it reboots) and is sleeping due to its hours of operation settings.
	N/A	Unable to identify the agent status.

The Information Tab

The **Information** tab, unlike other **Patch Content Details** page tabs, features no list. Rather, it features reference information for the applicable content item.

The Information Tab

This tab lists metadata about the patch itself.

The Information Tab Buttons

[View Package] [Deploy...] [Export]
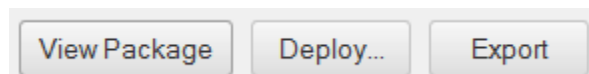
Table 145: Information Tab Buttons

Button	Description
View Package	Opens the **Packages** page and displays the package for the applicable content item.
Deploy...	Opens the **Deployment Wizard**. For additional information, refer to Using the Deployment Wizard on page 303.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 37.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 30.

HEAT®software

The Information Tab List

Table 146: List Text Descriptions

Name	Description
Vulnerability Name	The name of the content item.
Content Type	The content item type.
Beta	Indicates if the content item is in beta.
Downloaded on (UTC)	The date and time on which the content was downloaded.
Modified on (UTC)	The date and time the content item was last modified.
Associated packages	The number of packages associated with the content item.
Package status	The cache status for the content item packages.
HPL ID	The HPL identifier for the content item.
State	The enabled/disabled/completed status of the content item.
Enabled/Disabled by	The HPL user who last disabled or enabled the content.
Enabled/Disabled date (Server)	The date and time the content was disabled or enabled.
Enable/Disable reason	The reason the user provided for disabling or enabling the content. You can click the **Edit** link to change the reason.
Vendor name	The name of the content item vendor.
Vendor product ID	The identifier given to the security content item by the vendor.
Vendor release date/ time (UTC)	The date and time the vendor released the software in the content item.
Common Vulnerability Exploit (CVE) [1]	The CVE number for the content.

Name	Description
Vulnerability Code Description [1]	A description of the vulnerability associated with the content item.
Reference Text [1]	The reference text(s) associated with the content item vulnerability.
Description [1]	The narrative description of the distribution package. This section may include important notes about the content item and a link to more information.
[1]This meta data appears conditionally based on whether it was added for the content item. Additionally, there may be multiple instances of each meta data section.	

Information

This section displays information about the applicable content item.

Table 147: Content Item Field Descriptions

Name	Description
Vulnerability Name	The name of the content item.
Content Type	The content item type.
Beta	Indicates if the content item is in beta.
Downloaded on (UTC)	The date and time on which the content was downloaded.
Modified on (UTC)	The date and time the content item was last modified.
Associated packages	The number of packages associated with the content item.
Package status	The cache status for the content item packages.
HPL ID	The HPL identifier for the content item.
State	The enabled/disabled/completed status of the content item.
Enabled/Disabled by	The HPL user who last disabled or enabled the content.
Enabled/Disabled date (Server)	The date and time the content was disabled or enabled.
Enable/Disable reason	The reason the user provided for disabling or enabling the content. You can click the **Edit** link to change the reason.
Vendor name	The name of the content item vendor.
Vendor product ID	The identifier given to the security content item by the vendor.
Vendor release date/ time (UTC)	The date and time the vendor released the software in the content item.

HEAT®software

Name	Description
Common Vulnerability Exploit (CVE) [1]	The CVE number for the content.
Vulnerability Code Description [1]	A description of the vulnerability associated with the content item.
Reference Text [1]	The reference text(s) associated with the content item vulnerability.
Description [1]	The narrative description of the distribution package. This section may include important notes about the content item and a link to more information.
[1]This meta data appears conditionally based on whether it was added for the content item. Additionally, there may be multiple instances of each meta data section.	

Working with Content Items

From the **Patch Status** page, you can perform tasks related to a specific content item.

From the different page tabs, you can perform the following tasks:

- View Packages on page 368
- Deploying Content on page 369
- Exporting Content Item Data on page 369

View Packages

While viewing the **Patch Status** page for a content item, you can immediately view that content item's page.

Perform this tasks from any **Patch Status** page tab.

1. Select the desired tab:

    - ***Not Patched***
    - ***Patched***
    - ***Error***
    - ***Detecting***
    - ***Information***

2. Click **View Package**.

Result: The **Packages** page opens, displaying the package for the applicable content item.

Deploying Content

Deploying content items to endpoints is a key function of the HEAT PatchLink DataCenter Server for Microsoft System Center module.

Deployments are initiated by clicking **Deploy...** and completing the ***Deployment Wizard***. The ***Deployment Wizard*** provides step-by-step instructions for defining and distributing security content items to the protected endpoints in the network. For additional information, refer to Working With Deployments and Tasks on page 297.

Exporting Content Item Data

When viewing the ***Patch Status*** page, you can export the all data displayed for the selected tab to a comma separated value (`.csv`) file.

For additional information, refer to Exporting Data on page 37.

HEAT software

Chapter

13

HEAT PatchLink DataCenter Reporting

In this chapter:

- About HEAT PatchLink DataCenter Reports
- The HEAT PatchLink DataCenter Report Pages

HEAT PatchLink DataCenter for Microsoft® System Center can generate a variety of reports pertaining to HEAT PatchLink DataCenter functions.

Use these reports for internal reporting, management briefing, and assistance when using HEAT PatchLink DataCenter for Microsoft System Center.

About HEAT PatchLink DataCenter Reports

Reports are records that document HEAT PatchLink DataCenter activity.

There are multiple reports that collect HEAT PatchLink DataCenter data. HEAT PatchLink DataCenter-related reports include information about content and deployments. Reports are created by selecting a report type and defining its parameters.

Additionally, report formats vary. Some reports are in a `.html` file format, while others are in a `.pdf` format.

HEAT software

The HEAT PatchLink DataCenter Report Pages

From these pages, you can generate all available HEAT PatchLink DataCenter reports. Before generating the report, select the report type and define the report parameters.
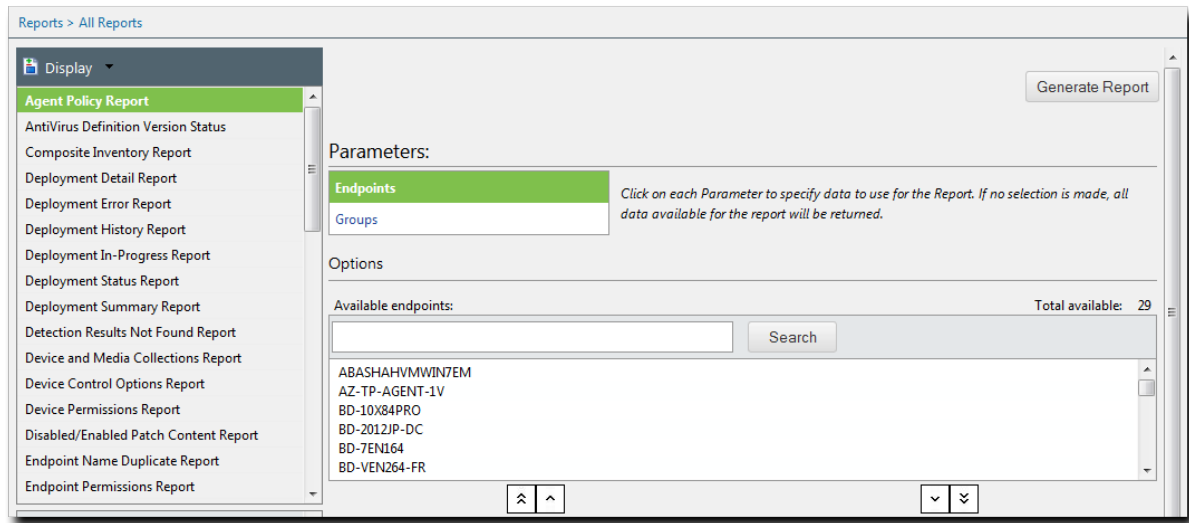
Figure 77: All Reports Page

Note: From the **Reports** menu, you can select multiple **All Reports** page variants. Based on which **Reports** menu item you select, the resulting page that opens groups its **Display** menu differently.

The following table lists the items available in the **Reports** navigation menu when HEAT PatchLink DataCenter is installed.

Table 148: Reports Menu Commands

Command	Description
Deployments	Reports are grouped with the **Deployments** group expanded. Deployment reports display information related to content deployment.
Inventory	Reports are grouped with the **Inventory** group expanded. Inventory reports display information related to network assets and endpoint hardware and software.
Policy and Compliance	Reports are grouped with the **Policy and Compliance** group expanded. These reports display information about agent policy sets, Mandatory Baselines, and Mandatory Baseline endpoint compliance.

Command	Description
Risks	Reports are grouped with the **Risks** group expanded. This report displays information about possible vulnerabilities in your network.
Vulnerabilities/Patch Content	Reports are grouped with the **Vulnerabilities/Patch Content** group expanded. These reports display information about network vulnerabilities.

Viewing the HEAT PatchLink DataCenter Report Pages

Navigate to these pages to generate either HTML or PDF reports related to HEAT PatchLink DataCenter.

Generate the desired report.

Generating a Report

HEAT PatchLink DataCenter for Microsoft System Center provides multiple predefined reports for HEAT PatchLink DataCenter. Generate reports to brief management or to view network behavior and statistics.

Generate reports from any HEAT PatchLink DataCenter report page.

1. From the **Monitoring** workspace, select **HEAT PatchLink DataCenter** > **Reporting** > **Standard Reports**.
2. From the **Display** list, select the report you want to generate.
3. Define parameters using the available fields, drop-downs, lists, and so on. Each report has distinct required and optional parameters.

   Note: Refer to the individual report descriptions for details regarding which parameters are required and which parameters are optional.

4. [Optional] Select the optional report parameters.
5. Click **Generate Report**.

   Step Result: The report generates.

   > **Important:** You may need to disable your pop-up blocker to view the report.

Result: The report is generated in a new window.

HEAT®software

Deployment Detail Report

This report provides information about a selected list of deployments. In the report, each deployment name is listed in the **Deployment Name** column. The report provides information as to the status of the particular deployment activity.

Optional Parameters: `Exclude Do Not Patch Reason, Include Do Not Patch Reason, Deployments, Packages, Date Range`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 149: Deployment Detail Report Column Definitions

Column	Definition
Deployment Name	The name of the deployment.
Package Name	The name of the package.
Endpoint Name	The name of the endpoint.
Deployment Result	The deployment status.
Deployment Start Date	The date the deployment was sent.
Date Installed	The date the package was installed on the endpoint.
Vulnerability Status	The content item patch status.
Do Not Patch - Reason	The reason the endpoint is marked as *Do Not Patch*. This column appears only if you selected **Include Do Not Patch Reason** when generating the report.
Date Last Verified	The date of the last Discover Applicable Updates (DAU) task.

Note: If a selected content item does not have an associated deployment, it will not appear in the report.

Deployment Error Report

This report provides information about deployments that have returned an error.

Optional Parameters: `Deployments, Packages, Endpoints, Date Range`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 150: Deployment Error Report Column Definitions

Column	Definition
Deployment Status	The deployment status.
Status Code	The reference code for support identification. When contacting support, use this code to help identify the deployment issue.
Error Message	The actual error text returned by the deployment.
Install Date	The date the agent was installed on the endpoint.
Package Name	The name of the package.
Deployment Name	The name of the deployment.
Device Name	The name of the endpoint.

Deployment History Report

This report allows selection of multiple patch deployments. It also displays a single pie chart for each deployment and shows deployment status counts for the deployment.

Required Parameters: Selection of one or multiple `deployment(s)`.

The following table describes each report field.

Table 151: Deployment History Report Field Definitions

Field	Definition
Deployment Name	The name of the deployment.
Package Name	The name of the package.
Deployment Status	The deployment status.
Deployment Date	The date the deployment was sent.
Created Date	The date and time the deployment was scheduled.
Created By	The user who created the deployment.
Graph Key	
Added to the Group After the Deployment Started	The number (or percentage) of deployments that did not complete because the endpoint was added to the group after the deployment started.
Already Patched	The number (or percentage) of endpoints that are already patched.

HEAT software

Field	Definition
Caching Package	The number (or percentage) of deployment packages that are being cached.
Deployment Aborted by Client User	The number (or percentage) of deployments that were aborted by endpoint users.
Deployment Aborted by User	The number (or percentage) of deployments that were aborted by HEAT PatchLink DataCenter for Microsoft System Center users.
Disabled	The number (or percentage) of deployments that were disabled.
Do Not Patch - Not Deployed	The number (or percentage) of endpoints that were marked as *Do Not Patch* for the content being deployed.
Failure	The number (or percentage) of deployments that failed.
In-Progress	The number (or percentage) of deployments that are in progress.
Not Applicable	The number (or percentage) of endpoints where the deployment does not apply.
Not Started	The number (or percentage) of deployments that have not started.
Not Started - Recurring	The number (or percentage) of recurring deployments that have not started deploying.
Removed from Deployment and Group	The number (or percentage) of deployments removed from deployments and groups.
Removed from Deployment by User	The number (or percentage) of deployments removed by users.
Success	The number (or percentage) of successful deployments.
Total	The total number of endpoints assessed.

Note: If there are no occurrences of a particular status during a deployment, that status does not appear in the *Deployment History Report* graph key.

Deployment In-Progress Report

This report provides information about deployments that have started but have not yet completed. Reports can be generated for each deployment, package, or endpoint. It also provides the status of the deployment.

Optional Parameters: `Deployments, Packages, Endpoints, Groups`

Note: Selecting no parameters will generate the report using all available data.

The following table describes each report column.

Table 152: Deployment In-Progress Report Column Definitions

Column	Definition
Deployment Name	The name of the deployment.
Package Name	The name of the package.
Total Not Deployed	The total number of endpoints and groups that were excluded from the deployment (because the package was already applied, not applicable, marked *Do Not Patch*, added to the group after the deployment started, or the deployment was aborted by the user).
Total Already Patched	The number of endpoints that are already patched.
Not Applicable	The number of endpoints where the deployment does not apply.
Do Not Patch	The total number of endpoints that are marked as *Do Not Patch*.
Total Deployed	The total number of endpoints that were assigned the deployment.
Total Success	The total number of endpoints successfully patched.
Total In-Progress	The total number of endpoints currently receiving the deployment.
Not Started	The number of endpoints yet to receive the deployments.
Caching Package	Indicates whether the deployment package is being cached. 1 = Caching, 0 = Complete
Total Failed	The total number of deployments that failed.
Total Disabled	The total number of endpoints that are disabled and cannot receive the deployment.
Percent Successful	The percentage of endpoints that successfully received the deployment.
Percent Failure	The percentage of endpoints on which the deployment has failed.

Deployment Status Report

This report provides the current status of a specified package deployment. It also includes a pie chart that shows deployment status counts for the deployment, as well as deployment results.

Required Parameters: Selection of one `deployment`.

Optional Parameters: `Deployment Results`.

HEAT®software

The following table describes the report fields and columns.

Table 153: Deployment Status Report Field and Column Definitions

Field / Column	Definition
General Information	
Deployment Name	The name of the deployment.
Package Name	The name of the package.
Deployment Status	The deployment status.
Deployment Date	The date the deployment was sent.
Created Date	The date and time the deployment was scheduled.
Created By	The user who created the deployment.
Graph Key	
Added to the Group After the Deployment Started	The number (or percentage) of deployments that did not complete because the endpoint was added to the group after the deployment started.
Already Patched	The number (or percentage) of endpoints that are already patched.
Caching Package	The number (or percentage) of deployment packages that are being cached.
Deployment Aborted by Client User	The number (or percentage) of deployments that were aborted by endpoint users.
Deployment Aborted by User	The number (or percentage) of deployments that were aborted by HEAT PatchLink DataCenter for Microsoft System Center users.
Disabled	The number (or percentage) of deployments that were disabled.
Do Not Patch	The number (or percentage) of endpoints that are marked as *Do Not Patch*.
Failure	The number (or percentage) of deployments that failed.
In-Progress	The number (or percentage) of deployments that are in progress.
Not Applicable	The number (or percentage) of endpoints where the deployment does not apply.
Not Started	The number (or percentage) of deployments that have not started.
Not Started - Recurring	The number (or percentage) of recurring deployments that have not started deploying.

Field / Column	Definition
Removed from Deployment and Group	The number (or percentage) of deployments removed from deployments and groups.
Removed from Deployment by User	The number (or percentage) of deployments removed by users.
Success	The number (or percentage) of successful deployments.
Total	The total number of endpoints assessed.
Table Columns	
Server Name	The IP address of the HEAT PatchLink DataCenter for Microsoft System Center server where the deployment originated.
Agent Name	The name endpoint that hosts the agent.
IP Address	The IP address of the endpoint.
Install Date	The date and time the deployment commenced.
Status Detail	Displays the status details applicable to the endpoint.
Failure Reason	Displays applicable failure reasons.

Note: If there are no occurrences of a particular status during a deployment, that status does not appear in the *Deployment Status Report* graph key.

Deployment Summary Report

This report provides information about a selected list of deployments. It also provides a summary of the particular deployment activity.

Optional Parameters: `Deployments, Packages, Date Range`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 154: Deployment Summary Report Column Definitions

Column	Definition
Deployment Name	The name of the deployment.
Package Name	The name of the package.

HEAT software

Column	Definition
Total Not Deployed	The total number of endpoints and groups that were excluded from the deployment (because the package was already applied, not applicable, marked *Do Not Patch*, added to the group after the deployment started, or the deployment was aborted by the user).
Total Already Patched	The number of endpoints that are already patched.
Not Applicable	The number of endpoints where the deployment does not apply.
Do Not Patch	The total number of endpoints that are marked as *Do Not Patch*.
Total Deployed	The total number of endpoints that were assigned the deployment.
Total Success	The total number of endpoints successfully patched.
Total In-Progress	The total number of endpoints currently receiving the deployment.
Not Started	The number of endpoints yet to receive the deployments.
Caching Package	Indicates whether the deployment package is being cached. 1 = Caching, 0 = Complete
Total Failed	The total number of deployments that failed.
Total Disabled	The total number of endpoints that are disabled and cannot receive the deployment.
Percent Successful	The percentage of endpoints that successfully received the deployment.
Percent Failure	The percentage of endpoints on which the deployment has failed.

Note: If a selected content item has no associated deployment, it does not appear in the report.

Detection Results Not Found Report

This report returns a list of endpoints that have not completed a Discover Applicable Updates task with the server. The report lists each agent name, the installation date of the agent, and information required to identify and locate the endpoint.

Optional Parameters: `Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 155: Detection Results Not Found Report Column Definitions

Column	Description
Agent Name	The name endpoint that hosts the agent.
OS Abbr Name	The abbreviated operating system name.
Agent Version	The version of the agent.
Last Contact Date	The last date the HEAT PatchLink DataCenter for Microsoft System Center had contact with the agent.
Installation Date	The date and time the agent was installed on the endpoint.
IP Address	The IP address of the endpoint.
DNS Name	The name used by the Domain Name System (DNS) to identify the endpoint.
OS Info	A description of the operating system.
Last DAU Date	The date of the last Discover Applicable Updates (DAU) task.
Last DAU Status	The status of the last Discover Applicable Updates (DAU) task.

Disabled/Enabled Patch Content Report

This report returns a list of content that has been disabled by an Administrator, with the disable reason text (if applicable) and date. This report can also be configured to show re-enabled content.

Optional Parameters: `Disabled vulnerabilities/patch content`, `Re-enabled vulnerabilities/patch content`

Note: If no parameter selection is made, the report generates using all available data.

Table 156: Disabled / Enabled Patch Content Report

Column	Description
Name	The name of the selected content group.
Content Type	The type of content in the content item.
Vendor	The name of the vendor that created the software in the content item.
Vendor Release Date	The date and time that the vendor released the content item.
State	The state of the content item (disabled or enabled).
Disabled/Enabled By	The user that disabled or enabled the content item.
Disabled/Enabled Date	The date and time that the content item was disabled or re-enabled.

HEAT software

Column	Description
Reason	The reason that the content item was enabled or disabled.

Endpoint Name Duplicate Report

This report returns a list of duplicate endpoints registered with HEAT PatchLink DataCenter for Microsoft System Center. Duplicate endpoints are usually the result of applying the agent uniqueness feature that permits an agent installed on ghost images to register multiple times with HEAT PatchLink DataCenter for Microsoft System Center.

Optional Parameters: `Date Range`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 157: Device Duplicate Report Column Definitions

Column	Definition
Device Name	The name of the endpoint.
Status	The current status of the endpoint.
Install Date	The date the agent was installed on the endpoint.

Hardware Inventory Detail Report

This report provides information about hardware associated with an endpoint and endpoint status.

Optional Parameters: `Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 158: Hardware Inventory Detail Report Column Definitions

Column	Definition
Hardware Device Class	The type of hardware.
Hardware Device Name	The name of the hardware device.
Device Name	The name of the endpoint.
Device OS Info	A description of the operating system.

Hardware Inventory Summary Report

This report provides a summary of reported hardware and the endpoints associated with them.

Optional Parameters: `Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 159: Hardware Inventory Summary Report Column Definitions

Column	Definition
Hardware Device Class	The type of hardware.
Hardware Device Name	The name of the hardware device.
Instances	The number of times this device occurs. (Within the parameters of the report.)

Mandatory Baseline Detail Report

This report provides information about the Mandatory Baseline status associated with an endpoint.

Optional Parameters: `Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 160: Mandatory Baseline Detail Report Column Definitions

Column	Definition
Endpoint Name	The name of the endpoint.
Assigned By Group	The distinguished name of the group that assigned the Mandatory Baseline.
Package Name	The name of the package.
Mandatory Baseline Enabled	Indicates whether the *Assigned By Group* has Mandatory Baselines enabled.
Package Enabled	Indicates whether the package is enabled. If the package is disabled, it cannot be deployed to an endpoint.
Mandatory Status	Identifies whether the endpoint is applicable, patched, not patched, marked as *Do Not Patch*, or needs patching by the Mandatory Baseline.
Deployment Status	The deployment status.

HEAT software

Column	Definition
Package Release Date	The date the package was released.
Date Deployed	The date the package was deployed.
Date Installed	The date the package was installed on the endpoint.
Date Last Verified	The date of the last Discover Applicable Updates (DAU) task.
Assigned	Indicates whether the Mandatory Baseline is assigned to the endpoint. 1 = Assigned, 0 = Not Assigned

Mandatory Baseline Summary Report

This report returns a summary list of patch content and deployment information for all Mandatory Baseline packages and content associated with the selected list of endpoints.

Optional Parameters: `Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each table column.

Table 161: Mandatory Baseline Summary Report Column Definitions

Column	Definition
Mandatory Baseline Item Name	Name of the Mandatory Baseline content item.
Total Endpoints	The total number of endpoints selected for the report.
Total Patched	The total number of endpoints patched by the deployment.
Total Not Applicable	The total number of endpoints for which the deployment does not apply.
Total Do Not Patch	The total number of endpoints that are marked as *Do Not Patch*.
Total In-Progress	The total number of endpoints currently receiving the deployment.
Total Disabled	The total number of endpoints that are disabled and cannot receive the deployment.
Total Error Condition	The total number of endpoints on which the deployment has failed.
Percent Patched	The percentage of applicable endpoints that are patched.

Operating System Inventory Detail Report

This report provides information about the operating system associated with an endpoint and the endpoint status.

Optional Parameters: `Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 162: Operating System Inventory Detail Report Column Definitions

Column	Definition
Operating System	The operating system name and description.
Device Name	The name of the endpoint.

Operating System Inventory Summary Report

This report provides a summary about the operating system associated with an endpoint and the endpoint status.

Optional Parameters: `Endpoints, Groups`

Note: If no parameter selection is made, the report generates all available data.

The following table describes each report column.

Table 163: Operating System Inventory Detail Report Column Definitions

Column	Definition
Operating System	The operating system name and description.
Instances	The number of times this operating system occurs. (Within the parameters of the report.)

Package Compliance Detail Report

This report provides information about patch and deployment status for a specific package or endpoint. The report lists each package associated with the selected endpoint(s) or group(s). In the report, each package is listed in the **Package Name** column. The report also provides details for the vulnerability status for each package, and the associated endpoint, status, and deployment details.

Optional Parameters: `Exclude Do Not Patch Reason, Include Do Not Patch Reason, Packages, Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

HEAT software

The following table describes each report column.

Table 164: Package Compliance Detail Report Column Definitions

Column	Definition
Package Name	The name of the package.
Package Release Date	The date the package was released.
Endpoint Name	The name of the endpoint.
Vulnerability Status	The content item patch status.
Do Not Patch - Reason	The reason the endpoint is marked as *Do Not Patch*. This column appears only if you selected **Include Do Not Patch Reason** when generating the report.
Last DAU Run	The date of the last Discover Applicable Updates (DAU) task.
Last DAU Status	The status of the last Discover Applicable Updates (DAU) task.
Date Last Verified	The date of the last Discover Applicable Updates (DAU) task.
Deployment Name	The name of the deployment.
Deployment Start Date	The date the deployment was sent.
Deployment Status	The deployment status.
Date Installed	The date the package was installed on the endpoint.
Date Scheduled	The date the package was scheduled for deployment to the endpoint.

Note: If a selected package has no associated deployment, it does not appear in the report.

Package Compliance Summary Report

This report returns a summary list of patch and deployment information by package name for all applicable endpoints.

Optional Parameters: `Packages, Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 165: Package Compliance Summary Report Columns

Column	Definition
Package Name	The name of the package.

Column	Definition
Endpoints Selected	The total number of endpoints included within the scope of the report.
Applicable Endpoints	The total number of applicable endpoints.
Endpoints Patched	The number of endpoints that are already patched.
Not Patched/Not Scheduled	The number of endpoints not patched, and have no deployment scheduled.
Not Patched/Scheduled	The number of endpoints not patched, but are scheduled for a deployment.
Deployments Completed	The number of deployments that have completed successfully.
Deployments Failed	The number of failed deployments.
Deployments In-Progress	The number of endpoints currently receiving the deployment.

Note:
- If a package has no associated deployment, it does not appear in the report.
- Endpoints marked as *Do Not Patch* are not included in the report data.

Patch Agent Configuration Report

This report provides a simple-to-read view of patch agent configurations. There are no options for this report. However, when generating this report, you must select an agent group.

Required Parameter: Selection of one `agent group`.

The following table describes each report field.

Table 166: Patch Agent Configuration Report Field Definitions

Field	Definition
Policy (Group) Information	
Name	The name of the selected agent group.
Description	A description of the selected group.
General Information	
Polling Interval (minutes)	Indicates the interval (in minutes) between agent and HEAT PatchLink DataCenter for Microsoft System Center communication.
User Defined	Indicates whether the group policy is user defined or predefined.
Last Modified	The date and time the group policy was last modified.
Deployment Notification Options	

HEAT software

Field	Definition
Patch Deployment: User May Cancel	Indicates if deployment recipients can cancel deployments.
Patch Deployment: Users May Snooze	Indicates if deployment recipients can snooze deployments.
Patch Deployment: Deploy Within	Indicates the maximum time frame a deployment recipient can snooze deployments.
Reboot Notification Options	
Patch Reboot: User May Cancel	Indicates if deployment recipient can cancel reboots.
Patch Reboot: User May Snooze	Indicates if deployment recipients can snooze reboots.
Patch Reboot: Reboot Within	Indicates the maximum time frame a deployment recipient can snooze reboots.
Notification Window Options	
Patch Deployment: Always On Top	Indicates if the deployment notifications window opens on top of all other windows until the recipient acknowledges the notification (yes or no).
Patch Reboot: Always On Top	Indicates if the reboot notifications window opens on top of all other windows until the recipient acknowledges the notification (yes or no).

Patch Agent Inventory Report

This report provides the details of the agents with the patch module installed associated with the specified agent groups. This includes a pie chart that shows the patch status count for the agent groups and details (IP address, name, operating system, and status) for each agent.

Required parameters: Selection of one or multiple agent groups.

Optional parameters (default setting): Sort By (IP address, machine name, operating system [OS]), Included OSs, Included IP adresses.

The following table describes each report field and column.

Table 167: Patch Agent Inventory Report Field and Column Definitions

Field / Column	Definition
General Information	
Server Name	The HEAT PatchLink DataCenter for Microsoft System Center server name.
Agent Groups	The agent groups included in the report.
Agent Status Summary	

Field / Column	Definition
Total Known Endpoints	The total number of endpoints with the patch module installed.
Agents Checking In	The number of agents communicating with HEAT PatchLink DataCenter for Microsoft System Center.
Working	The number (or percentage) of patch modules that are working on a deployment.
Idle	The number (or percentage) of patch modules that are idle.
Sleeping	The number (or percentage) of patch modules that are sleeping due to hours of operation settings.
Agents Not Checking In	The number of patch modules that are not communicating with HEAT PatchLink DataCenter for Microsoft System Center.
Offline	The number (or percentage) of patch modules that are offline.
Disabled	The number (or percentage) of patch modules that are disabled.
Agent Status Summary Graph	
Disabled	The number (or percentage) of patch modules that are disabled.
Idle	The number (or percentage) of patch modules that are idle.
Offline	The number (or percentage) of patch modules that are offline.
Sleeping	The number (or percentage) of patch modules that are sleeping due to hours of operation settings.
Working	The number (or percentage) of patch modules that are working on a deployment.
Total	The total number of patch modules assessed.
Agent Inventory Table	
Agent IP	The IP address of the endpoint the agent is installed on.
Agent Name	The name endpoint that hosts the agent.
Operating System	The operating system name and description.
HEAT PatchLink DataCenter Server for Microsoft System Center Status	The current status.

HEAT software

Patchable Status Report

This report returns the current status of the selected endpoints (or endpoints in the selected groups). In the report, each endpoint is listed in the **Endpoint Name** column. The report then provides information about the particular endpoint.

Optional Parameters: `Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 168: Patchable Status Report Column Definitions

Column	Definition
Device Name	The name of the endpoint.
DNS Name	The name used by the Domain Name System (DNS) to identify the endpoint.
IP Address	The IP address of the endpoint.
OS Name	The operating system name.
OS Build No.	The operating system's build number.
OS Service Pack	The latest service pack applied to the operating system (if applicable).
Agent Version	The version of the agent.
Last Contact Date	The last date HEAT PatchLink DataCenter for Microsoft System Center had contact with the agent.
Patchable Status	The reboot/chained status of the agent.
Group List	A listing of the groups, by distinguished name, to which the endpoint belongs.

Potential Data Leakage Report

This report returns a list of Windows-based endpoints that have removable storage.

Optional Parameters: `Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each table column.

Column	Definition
AgentName	The name of the endpoint hosting the agent.
HardwareClass	The type of external storage device associated with the agent.
HardwareName	The name of the applicable external storage device.

Column	Definition
Quantity	The number of external storage devices associated with the agent.
IPAddress	The IP address of the agent.
DetectionDate	The date and time the endpoint and its external storage device(s) were detected.

Services Inventory Detail Report

This report provides information about the service associated with an endpoint and the endpoint status.

Optional Parameters: `Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 169: Services Inventory Detail Report Column Definitions

Column	Definition
Service Name	The name of the service.
Device Name	The name of the endpoint.
Service Startup State	The state the service should enter upon endpoint boot.
Service Current State	The current state of the endpoint.

Services Inventory Summary Report

This report provides summary information about the services associated with an endpoint and the endpoint status.

Optional Parameters: `Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 170: Services Inventory Summary Report Column Definitions

Column	Definition
Service Name	The name of the service.
Instances	The number of times this service occurs. (Within the parameters of the report.)

HEAT®software

Software Inventory Detail Report

This report provides information about the software associated with an endpoint and the endpoint status.

Optional Parameters: `Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 171: Software Inventory Detail Report Column Definitions

Column	Definition
Software Program	The name of the software installed on the endpoint.
Device Name	The name of the endpoint.

Software Inventory Summary Report

This report provides information about the software associated with an endpoint and the endpoint status.

Optional Parameters: `Endpoints, Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 172: Software Inventory Summary Report Column Definition

Column	Definition
Software Program	The name of the software installed on the endpoint.
Instances	The number of times this software occurs. (Within the parameters of the report.)

Vulnerability Analysis Report

This report summarizes the remediation status for the selected content items. The report lists each vulnerability affecting the selected endpoint or group. The report can also be generated for a single or multiple content items. In the report, each content item is listed in the **Vulnerability Name** column. The report also provides patch status details for each content item and if a deployment is required.

Optional Parameters: `Endpoints, Groups, Vulnerabilities, Custom Patch Lists`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 173: Vulnerability Analysis Report Column Definitions

Column	Definition
Name	The name of the content item.
Content Type	The type of content in the content item.
Vendor	The name of the vendor that created the software in the content item.
Vendor Release Date	The date that the vendor released the patch.
Endpoints Selected	The total number of endpoints included within the scope of the report.
Endpoints Applicable	The total number of endpoints that the patch applies to.
Endpoints Patched	The number of endpoints that are already patched.
Endpoints Not Patched	The number of endpoints not patched.
Percent Patched	The percentage of applicable endpoints that are patched.
Note: If an endpoint (or group) is marked *Do Not Patch* for a content item, the **Endpoints Applicable**, **Endpoints Patched**, **Endpoints Not Patched**, and **Percent Patched** columns do not include that endpoint in their data.	

HEAT software

Chapter

14

Patching Linux and Unix Endpoints

In this chapter:

- Configuring Your Enterprise for Linux and Unix Patching
- Server Configuration Procedures
- Endpoint Configuration Procedures
- Configuring Linux Endpoints for SELinux
- Patch Agent Command Line Usage

You can use HEAT PatchLink DataCenter for Microsoft® System Center to deploy patch content to commonly used Linux and Unix platforms.

This chapter includes information on how to:

- Configure your HEAT Patch Manager DataCenter Server to support patching older Linux and Unix platforms.
- Get started setting up a local respoitory to support newer Linux and Unix endpoints, if necessary.
- Configure your endpoints to support patching newer Linux and Unix platforms.
- Use commands for the HEAT PatchLink DataCenter Agent for Linux/UNIX on Linux and Unix endpoints.

HEAT software

Configuring Your Enterprise for Linux and Unix Patching

There are two ways to configure Linux and Unix endpoints for patching: configuring your server, or configuring your individual endpoints. Depending on the platforms you are supporting in your enterprise, your may need configure your server, configure your indivual endpoints, or both.

- If you support any platforms listed in Server Configuration to Support Linux and Unix Platforms, complete Configuring Your Server for Linux/Unix Patching on page 397. This workflow takes you through each procedure needed to:

  - Register your server with your Linux or Unix vendor.
  - Configure your server to function as a local repository.

- If you support any platforms listed in Endpoint Configuration to Support Linux and Unix Platforms, complete Configuring Your Linux/Unix Endpoints for Patching on page 399 to register the endpoints with their vendors and point them toward the main vendor repository. You must complete this procedure for each individual endpoint running on these platforms.

> **Attention:** If you are supporting any of the platforms listed in Endpoint Configuration to Support Linux and Unix Platforms, you should consider creating a dedicated local repository to host patch content (if you don't have one already). Newer Linux and Unix platforms cannot use the HEAT Patch Manager DataCenter Server as a local repository due to vendor endpoint registration requirements. Creating a dedicated repository can substantially shorten deployment times and reduce bandwidth consumption. If want to use a local repository, follow the vendor documentation referenced in Using HPL with Local Repositories on page 400 instead of completing *Configuring Your Linux/ Unix Endpoints for Patching*.

- If you support platforms listed in both sections listed below, complete both Configuring Your Server for Linux/Unix Patching on page 397 *and* Configuring Your Linux/Unix Endpoints for Patching on page 399.

Server Configuration to Support Linux and Unix Platforms

If you support any of the following operating systems, you must configure your HEAT Patch Manager DataCenter Server to function as a local repository.

- CentOS Linux 6
- CentOS Linux 5
- Hewlett Packard HP-UX 11.31
- Hewlett Packard HP-UX 11.23
- Hewlett Packard HP-UX 11.11
- SUSE Linux Enterprise 10
- SUSE Linux Enterprise 11

- Oracle Solaris 10
- Oracle Enterprise Linux 6
- Oracle Enterprise Linux 5
- Oracle Enterprise Linux 4
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 5

Endpoint Configuration to Support Linux and Unix Platforms

If you support any of the following operating systems, you must register each individual Linux or Unix endpoint with its vendor, and then point it toward a repository available either over the Internet or locally.

- Oracle Enterprise Linux 7
- Red Hat Enterprise Linux 7
- Oracle Solaris 11
- IBM AIX 7.1
- IBM AIX 6.1
- SUSE Linux Enterprise 12
- CentOS Linux 7

> **Note:** CentOS Linux 7 is a bit of an exception here. You *do not* have to register it with CentOS before it will work with HPL. Skip Configuring Your Linux/Unix Endpoints for Patching on page 399 for CentOS Linux 7 endpoints.

Configuring Your Server for Linux/Unix Patching

If you are patching older versions of Linux and Unix, you must subscribe to vendor content and then configure you HEAT Patch Manager DataCenter Server to function as a local repository. Afterwards, install agents and deploy content to your endpoints.

Perform this procedure on your HEAT Patch Manager DataCenter Server if you are supporting older Linux/Unix platforms.

1. Subscribe to the Linux or Unix vendor subscription network for each platform you're supporting in your enterprise.

   - Red Hat Network
   - My Oracle Support for Solaris
   - Oracle Unbreakable Linux Network
   - Novell Customer Center
   - HP IT Resource Center

   > **Note:** You don't need a subscription for CentOS. It's free.

2. Notify HEAT that you have a Linux or Unix subscription, and that you want to use HPL to deploy patch content these platforms. We will update your licensing so that you can access patch content for your platforms.

3. From the HPL Console, replicate with the Global Subscription Service.

   This action downloads new license information and the Content Credentials Manager, a utility you'll use in the next step.

HEAT software

4. From the HEAT Patch Manager DataCenter Server, use Content Credentials Manager to subscribe to a vendor subscription network. Enter credentials for each subscription you have.

Use this command-line utility to enter your vendor subscription credentials in the HEAT Patch Manager DataCenter Server. Once you enter your credentials, HPL uses them to connect to your vendor subscription network and download patch content. Instructions for using Content Credentials Manager on each supported platform are included. Note that the instructions for CentOS are a little different; since that OS doesn't require a subscription, it uses a different utility to simply enter the address information for a content mirror.

- CentOS 5 and 6
- Solaris 10
- Red Hat Enterprise Linux 5 and 6
- Oracle Linux 5 and 6
- Novell SUSE Linux 11
- HP-UX 11.11, 11.21. and 11.31

5. From the HPL Console, replicate again.

Now that you have registered with your Linux/Unix vendors, complete a replication to download new patch content definitions.

6. Install the HEAT PatchLink DataCenter Agent for Linux/UNIX on your Linux and Unix endpoints.

Instructions for installing the HEAT PatchLink DataCenter Agent for Linux/UNIX are available in the HEAT Endpoint Management and Security Suite: Agent Installation Guide (http://portal.lumension.com) .

7. If you have Security-Enhanced Linux installed on any of your endpoints, configure the endpoints to accept deployments from the HEAT Patch Manager DataCenter Server.

If you don't have any SELinux endpoints, skip this step.

8. Deploy content to your endpoints.

This process is similar to deploying Windows patch content using the **Deployment Wizard**. The one discernible difference is setting content flags, a method used to set deployment behavior for a patch. Rather than using the regular options, you'll need to edit a text box to set deployment behavior.

Configuring Your Linux/Unix Endpoints for Patching

If you are working with newer Linux or Unix platforms, you must register your individual endpoints with the vendor before you can begin patching them. This registration is required because Linux/Unix vendors require entitlements on individual endpoints before they are eligible for content from the vendor's repository.

Attention: If you are supporting any of the platforms listed in Endpoint Configuration to Support Linux and Unix Platforms, you should consider creating a dedicated local repository to host patch content (if you don't have one already). Newer Linux and Unix platforms cannot use the HEAT Patch Manager DataCenter Server as a local repository due to vendor endpoint registration requirements. Creating a dedicated repository can substantially shorten deployment times and reduce bandwidth consumption. If want to use a local repository, follow the vendor documentation referenced in Using HPL with Local Repositories on page 400 instead of completing *Configuring Your Linux/Unix Endpoints for Patching*.

Perform this procedure on *all* newer versions of Linux/Unix endpoints you are supporting.

Note: CentOS Linux 7 is a bit of an exception here. You *do not* have to register it with CentOS before it will work with HPL. Skip this procedure for CentOS Linux 7 endpoints.

1. Subscribe to the Linux or Unix vendor subscription network for each platform you're supporting in your enterprise.

   - Red Hat Enterprise Linux 7
   - Solaris 11
   - Oracle Enterprise Linux 7
   - Novell Customer Center
   - IBM AIX 6.1 and 7.1

2. Notify HEAT that you have a Linux or Unix subscription, and that you want to use HPL to deploy patch content these platforms. We can update your licensing so that you can access this content.

3. From the HPL Console, replicate with the Global Subscription Service.

   This action downloads your newly available patch content licensing.

4. Register your endpoints with your vendors and install entitlements on the endpoint.

   This process varies for each Linux/Unix platforms. The following links provide step-by-step intructions on how to complete this process for each supported platform.

   - Red Hat 7 Endpoints Configuration (GUI) on page 409
   - Oracle Enterprise Linux 7 Configuration on page 411
   - Oracle Solaris 11 Endpoint Configuration on page 411
   - SUSE Linux 12 Endpoint Configuration on page 412
   - Configuring AIX 7.1 and 6.1 Endpoints to Download Content on page 412

HEAT software

5. From the HPL Console, replicate again.

Now that you have registered with your Linux or Unix vendor, complete a replication to download new patch content definitions.

6. Install the HEAT PatchLink DataCenter Agent for Linux/UNIX on your Linux and Unix endpoints.

Instructions for installing the HEAT PatchLink DataCenter Agent for Linux/UNIX are available in the HEAT Endpoint Management and Security Suite: Agent Installation Guide (http://portal.lumension.com) .

7. Deploy content to your endpoints.

This process is similar to deploying Windows patch content using the **Deployment Wizard**. The one discernable difference is setting content flags, a method used to set deployment behavior for a patch. Rather than using the regular options, you'll need to edit a text box to set deployment behavior.

Note: If you have completed this workflow, you are likely using the default vendor repositories available on the Internet. When deploying patch content from a default repository to Red Hat Enterprise Linux 7, Oracle Enterprise Linux 7, SUSE Linux Enterprise 12, or CentOS Linux 7, deployments can exceed scheduled maintenance due to endpoints caching content from a remote location. To reduce likelihood of deployment that exceed maintenance schedules, HEAT recommends splitting your deployment into two, smaller deployments using two new flags. These flags are only available for Red Hat Enterprise Linux 7, Oracle Enterprise Linux 7, SUSE Linux Enterprise 12, and CentOS Linux 7:

1. Complete the first deployment using the -CACHEPACKAGES flag. This flag instructs endpoints to cache the patch content you've selected, but not install it.

2. Complete the second deployment using the -INSTALLFROMCACHE flag. This flag instructs endpoints to install the patch content cached during the previous deployment.

Using HPL with Local Repositories

If you are a HPL administrator managing newer Linux platforms, creating a local repository and then pointing your endpoints toward them can substantially reduce deployment times.

When working with older releases of Linux and Unix, your HEAT Patch Manager DataCenter Server functions as a local repository, which speeds deployment time by caching packages to your server.

If you only work with older release of Linux and Unix, don't read on any further; this doesn't apply to you. Refer to Configuring Your Server for Linux/Unix Patching on page 397.

However, if you are working with newer releases of Linux and Unix, you can substantially reduce deployment times by setting up a dedicated local repository, which is an on-premise mirror of the vendor repository. Because newer Linux and Unix platforms require each individual endpoint to register with the vendor, you cannot use your HEAT Patch Manager DataCenter Server as a local repository. By setting up a dedicated local repository, you can maintain the deployment speeds while still conforming to Linux/Unix endpoint registration requirements.

If you want to set up a local repository, complete the following workflow. If you elect to use a local repository, skip completion of Configuring Your Enterprise for Linux and Unix Patching on page 396; The vendor documentation includes this information.

To use local repositories in conjunction with HPL:

1. Set up a local repository for your vendor's patch content. HEAT recommends following the vendor-provided documentation. This documentation includes information on how to set up local repositories and point your endpoints toward them.

Red Hat Satellite 6.0 Documentation	You can set up a local repository for RHEL 7 using Red Hat Satellite 6.0. Red Hat refers to local repositories as *satellitle servers*. This documentation includes info on: • How to set up a satellite server • How to configure your endpoints (which Red Hat refers to as *hosts*) to point toward the satellite server .
How to create a local Unbreakable Linux Network mirror	You can set up a local repository for Oracle Linux 7. Oracle Linux refers to local repositories as *Unbreakable Linux Network Mirrors*. This documentation includes info on: • How to setup an Unbreakable Linux Network Mirror. • How to configure endpoints (which oracle refers to as *clients*) to point toward the mirror.
How to Create a Local Package Repository for Solaris 11	You can setup a local repository for Oracle Solaris 11. If you use this documentation, skip over the content for Oracle Linux 6. It isn't relevant.
YaST: Setting up a local SUSE Linux update Server	You can set up a local repository for SUSE Linux Enterprise 12. SUSE refers to local repositories as *local SUSE Linux update servers*. This documentation includes info on: • How to setup a local SUSE Linux update server. • How to configure endpoints (which SUSE refers to as *clients*) to point toward the server.

2. Configure your endpoints to point toward your local repository. Refer to the vendor documentation above.
3. Install the HEAT PatchLink DataCenter Agent for Linux/UNIX on your Linux and Unix endpoints.

   Instructions for installing the HEAT PatchLink DataCenter Agent for Linux/UNIX are available in the HEAT Endpoint Management and Security Suite: Agent Installation Guide (http:// portal.lumension.com) .
4. Deploy content your endpoint.

   This process is similar to deploying Windows patch content using the **Deployment Wizard**. The one discernable difference is setting content flags, a method used to set deployment behavior for a patch. Rather than using the regular options, you'll need to edit a text box to set deployment behavior.

◢HEAT®software

Server Configuration Procedures

When setting up HPL to be a local repository for a Linux or Unix platform, complete each of the following procedure for platforms you support.

Red Hat Server Configuration

Enable enhanced content to allow HEAT PatchLink DataCenter for Microsoft System Center to download content directly from third parties rather than from the Global Subscription Service. This functionality leads to faster turnaround time when installing content.

If you are running the Red Hat Linux operating system, you must configure your credentials on the Red Hat Network in order to receive content.

Note: To receive patch content from the HEAT Patch Manager DataCenter Server, RHEL endpoints must have Management Base entitlements through the Red Hat Network.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

2. Click **Update Now**.

   Step Result: Replication between your HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) server and the Global Subscription Service begins.

3. When replication is complete, open a command prompt.

4. Navigate to the `Replication Services` directory. You can locate this directory here: `<Installation Directory>\HEAT Software\EMSS\Replication Services`.

5. From a command prompt, enter the following command, replacing the variables listed below with the appropriate parameter values:

```
CredentialsManager.exe  /source:redhat /u:RedHatUserName /p:RedHatPassword /
hostname:MyServerName /release:RedHatRelease /arch:RedHatArchitecture
```

Table 174: Credentials Manager Configuration

Variable	Description
RedHatUserName	Your user name on the Red Hat Network.
RedHatPassword	Your password on the Red Hat Network.

Variable	Description
MyServerName	The server HPL name.
RedHatRelease	The version of Red Hat that you want to receive content for. Enter one of the following: • 6Server • 6Workstation • 5Server • 5Client • 4AS • 4ES • 4WS
RedHatArchitecture	The processor type on the endpoints that you want to receive content for. Enter one of the following: • i386 • x86_64

Note:

- You must perform this step for each Red Hat subscription you are supporting.
- If you use a proxy to separate your HEAT Patch Manager DataCenter Server from the Internet, the proxy settings defined the Subcription Updates page are used during replication of Linux and UNIX content.

6. Choose whether you want to encrypt communication between the HEAT Patch Manager DataCenter Server and the Red Hat Network.

   - To use encrypted SSL communication, enter the green word that appears (`yes` or `import`).
   - To use unencrypted communication, enter `No`.

Note: SSL communication with Red Hat Network uses a certificate provided by them. If you want to verify its authenticity or import it to a proxy server following completion of this procedure, enter the following command to export it to <Installation Directory>\Lumension\EMSS\Replication Services\RHNS-CA-CERT.cer.

```
CredentialsManager.exe /source:redhat /export
```

7. Verify that your HEAT Patch Manager DataCenter Server is registered on the Red Hat Network.

   a) Go to http://rhn.redhat.com.
   b) Log in using the username and password combination that you used for the *RedHatUserName* and *RedHatPassword* above.
   c) Verify that the *MyServerName* that you entered above appears in **Subscription Management**.

HEAT software

d) Verify that the subscription details match the details you entered above.

After Completing This Task:

Complete Updating HPL System Files and Content on page 100. You cannot remediate your Linux endpoints until your HEAT PatchLink DataCenter server replicates with the GSS.

Solaris Server Configuration

Enable enhanced content to allow HEAT PatchLink DataCenter for Microsoft System Center server to download content directly from third parties rather than from the Global Subscription Service. This functionality leads to faster turnaround time when installing content.

If you are running the Oracle Solaris 10 or earlier operating system, you must configure your credentials with My Oracle in order to receive content.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

2. Click **Update Now**.

   Step Result: Replication between your HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) server and the Global Subscription Service (GSS) begins.

3. When replication is complete, open a command prompt.

4. Navigate to the `Replication Services` directory. You can locate this directory here: `<Installation Directory>\HEAT Software\EMSS\Replication Services`.

5. From a command prompt, enter the following command and usage, replacing the variables listed below with the appropriate values:

   ```
   CredentialsManager.exe /source:solaris /username:SolarisUserName /password:SolarisPassword
   ```

   Note: If you use a proxy to separate your HEAT Patch Manager DataCenter Server from the Internet, the proxy settings defined the Subcription Updates page are used during replication of Linux and UNIX content.

Result: You can now remediate your Oracle Solaris endpoints through using the HEAT PatchLink DataCenter server.

After Completing This Task:

Complete Updating HPL System Files and Content on page 100. You cannot remediate your Oracle Solaris endpoints until your HEAT PatchLink DataCenter server replicates with the GSS.

You must also allow outbound access through ports 80 and 443 to the following URLs:

- https://getupdates2.sun.com
- http://getupdates.oracle.com
- http://a248.e.akamai.net

Oracle Linux Server Configuration

Enable enhanced content to allow HEAT PatchLink DataCenter server to download content directly from third parties rather than from Global Subscription Service. This leads to faster turnaround time when installing content

If you are running the Oracle Enterprise Linux operating system, you must configure your credentials on the Oracle Unbreakable Linux Network in order to receive enhanced content.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

2. Click **Update Now**.

   Step Result: Replication between your HEAT PatchLink DataCenter server and the Global Subscription Service begins.

3. When replication is complete, open a command prompt.

4. Navigate to the `Replication Services` directory. You can locate this directory here: `<Installation Directory>\HEAT Software\EMSS\Replication Services`.

5. From a command prompt, enter the following line, replacing the variables listed below with the appropriate values:

   ```
   CredentialsManager.exe /source:oracle /u:username /p:password /csi:xxxxxxxx /
   hostname: computername /release: x /arch:architecture
   ```

   > **Note:**
   > - You must perform this step for each Oracle Enterprise Linux subscription that you want HEAT PatchLink DataCenter server to remediate.
   > - If you use a proxy to separate your HEAT Patch Manager DataCenter Server from the Internet, the proxy settings defined the Subcription Updates page are used during replication of Linux and UNIX content.
   > - For a complete list of commands, type `/source: oracle /HELP`.

   Step Result: A successful registration message displays.

After Completing This Task:
Complete Updating HPL System Files and Content on page 100. You cannot remediate your Linux endpoints until your HEAT PatchLink DataCenter server replicates with the GSS.

SUSE Linux Server Configuration

Before you can deploy patch content to your SUSE endpoints, you must configure HPL so that it can log in to SUSE repositories.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

✓HEAT software

2. Click **Update Now**.

> **Step Result:** Replication between your HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) server and the Global Subscription Service begins.

3. When replication is complete, open a command prompt.

4. Navigate to the `Replication Services` directory. You can locate this directory here: `<Installation Directory>\HEAT Software\EMSS\Replication Services`.

5. From a command prompt, enter the following command. Replace the variables with your SUSE subscription credentials.

`CredentialsManager.exe /source:suse /a:mirror /u:<username> /p:<password>`

> **Note:**
> - If you use a proxy to separate your HEAT Patch Manager DataCenter Server from the Internet, the proxy settings defined the Subcription Updates page are used during replication of Linux and UNIX content.
> - For a complete list of commands, enter: `/source:suse /HELP` at the command prompt.

> **Step Result:** A successful registration message displays.

6. Optionally, you can list the operating system types registered with the HEAT PatchLink DataCenter server and validate the status of the channels providing enhanced content. Enter the following commands at the command prompt.

- To list the operating system types registered with the server, enter: `CredentialsManager.exe /source:suse /list`.
- To validate the status of the channels providing the enhanced content, enter: `CredentialsManager.exe /source:suse /validate`.

Result: You can now remediate your Novell SUSE Linux endpoints using HEAT PatchLink DataCenter server.

After Completing This Task:
Complete Updating HPL System Files and Content You cannot remediate your Linux endpoints until your HEAT PatchLink DataCenter server replicates with the GSS.

HP-UX Server Configuration

The HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) server must be configured to download content directly from third-party vendors rather than the Global Subscription Service. This functionality leads to faster turnaround time when installing content.

If you are running the HP-UX operating system, you must configure your credentials with the HP IT Resource Center in order to receive content.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

2. Click **Update Now**.

> **Step Result:** Replication between your HEAT PatchLink DataCenter server and the Global Subscription Service begins.

3. When replication is complete, open a command prompt.

4. Navigate to the `Replication Services` directory. You can locate this directory here: <Installation Directory>\Lumension\EMSS\Replication Services.

5. From a command prompt, enter the following lines, replacing the variables listed below with the appropriate values:

```
CredentialsManager /source:hpux /u:HP IT Resource Center UserName /p:HP IT Resource Center
Password
```

> **Note:** If you use a proxy to separate your HEAT Patch Manager DataCenter Server from the Internet, the proxy settings defined the Subcription Updates page are used during replication of Linux and UNIX content.

Table 175: Credentials Manager configuration

Variable	Description
HP IT Resource Center Username	Your user name on HP IT Resource Center.
HP IT Resource Center Password	Your password on HP IT Resource Center.

> **Step Result:** A warning appears indicating that registering your server with the Credentials Management tool may result in a loss of patch deployment history and increased replication times.

6. Enter `Y` to acknowledge the warning and confirm the registration.

> **Note:** You must perform the previous step and this step for each Red Hat subscription that you want HEAT PatchLink DataCenter to remediate.

Result: You can now remediate your HP-UX endpoints using HEAT PatchLink DataCenter.

After Completing This Task:

Complete Updating HPL System Files and Content on page 100. You cannot remediate your Linux endpoints until your HEAT PatchLink DataCenter server replicates with the GSS.

Additionally, you must also allow outbound access through ports 80 and 443 to the following URLs:

- http://itrc.hp.com
- http://ftp.itrc.hp.com

HEAT®software

CentOS Server Configuration

In environments containing CentOS endpoints, HEAT recommends defining a Mirror site that your HEAT PatchLink DataCenter for Microsoft System Center server can use to download CentOS HEAT PatchLink DataCenter content. Using a mirror site increases content download speeds and reduces download traffic from the CentOS community locations.

Define a content mirror using your Web browser and the HEAT PatchLink DataCenter for Microsoft System Center server **Computer** dialog.

> **Note:** Mirror site definition requires use of the Specify Site Mirror Tool. The HEAT Patch Manager DataCenter Server downloads this tool during its first replication with the Global Subscription Service.

1. From any computer, obtain the address of the content mirror closest to your enterprise geographical location.
   a) Open your web browser and navigate to http://www.centos.org/download/mirrors/.
   b) From the list of mirrors, identify the mirror closest to your geograpical location. Write down or copy the mirror **HTTP Location**. Close the web browser when you're done.

2. From the HEAT PatchLink DataCenter for Microsoft System Center server, open a command prompt.

3. From the command prompt, change directories to your HEAT Patch Manager DataCenter Server Replication Services folder.

   Enter `cd <Installation Directory>\Lumension\EMSS\Replication Services`

4. Enter `SpecifyMirrorSite.exe /name:"name" /uri:"mirrorlist"`.

   > **Note:**
   > - This command only validates that the URI resolves. It does not validate CentOS data.
   > - Your HEAT PatchLink DataCenter for Microsoft System Center must allow outbound access though ports 80 and 443 to the chosen mirror.
   > - If you use a proxy to separate your HEAT Patch Manager DataCenter Server from the Internet, the proxy settings defined the Subcription Updates page are used during replication of Linux and UNIX content.

5. [Optional] Validate the CentOS mirror locations.

   Enter `SpecifyMirrorSite.exe/validate`.

Endpoint Configuration Procedures

When setting up newer Linux or Unix endpoints for patching, complete one of the following procedures on each Linux/Unix endpoint you support.

Red Hat 7 Endpoints Configuration (GUI)

Before you can deploy patch content to your Red Hat Enterprise Linux 7 (RHEL) endpoints using HPL, you must register the endpoint with Red Hat and subscribe to a repository. RHEL 7 includes a wizard that makes this process fast and painless.

Complete this task from your RHEL 7 endpoints.

> **Note:** This procedure contains basic instructions for attaching to the Red Hat repository. For more detailed information about attaching to different repositories, consult the RHEL Systems Registration Guide.

1. From the dashboard, search for `Red Hat Subscription Manager`. When it displays, click **Red Hat Subscription Manager**.

2. Enter your root password.

3. Click **Register**.

4. Define a server to register against.

   - To register with the RHEL repository, leave the default server name.
   - To register with a RHEL sattelite server within your enterprise, type your satellite server name in the **I will register with** field.

5. If you will use a proxy to connect with the defined respository, click **Configure Proxy** and fill in the required information.

   If you aren't using a proxy, skip to the next step.

6. Click **Next**.

7. From **System Registration**, enter your Red Hat account information.

8. If necessary, change your **System Name**, but in most cases just use the default.

9. Click **Register**.

HEAT software

10. When prompted, review your **Subscription**. If the info looks good, click **Attach** to connect to the repository.

Result: Your endpoint is subscribed to the entitlement you chose. Provided that the endpoint has a HEAT PatchLink DataCenter Agent for Linux/UNIX installed, you can begin deploying content to it.

Red Hat 7 Endpoints Configuration (Terminal)

Before you can deploy patch content to your Red Hat Enterprise Linux 7 (RHEL) endpoints using HPL, you must register the endpoint with Red Hat and subscribe to a repository. Power users can finish this process quickly using Terminal.

Complete this task from your RHEL 7 endpoints.

Note: This procedure contains basic instructions for attaching to the Red Hat repository. For more detailed information about attaching to different repositories, consult the RHEL Systems Registration Guide.

1. Open *Terminal*.

2. Elevate your privledges.

   a) Enter `sudo -s`
   b) Enter the root password

3. Register the endpoint with RPM using your Red Hat Network credentials.

   a) Enter `subscription-manager register --username=`*`yourusername`*` --pasword=`*`yourpassword`*

   Step Result: If regitration completes successfully, *Terminal* displays your new RPM registration ID.

4. Subscribe to one or more entitlement.

   a) Enter `subscription-manager list --available | less`

   This command list the entitlements attached to your Red Hat Network account. Write down or copy the **Pool ID** for each entitlement you want to use for the endpoint.

   When you're done copying **Pool ID**s, close out the list by typing `q`.
   b) Enter `subscription-manager attach --pool=`*`YourPoolId`*

   Tip: You can subscribe to all entitlements for your Red Hat Network account by entering `subscription-manager attach --auto`

Result: Your endpoint is subscribed to the entitlement you chose. Provided that the endpoint has a HEAT PatchLink DataCenter Agent for Linux/UNIX installed, you can begin deploying content to it.

Oracle Enterprise Linux 7 Configuration

Before you can deploy patch content your Oracle Linux 7 endpoints, you have to register your endpoints with Oracle Unbreakable Network and attach to a repository.

You can complete this process either before or after you install the HEAT PatchLink DataCenter Agent for Linux/UNIX.

1. Open the dashboard and search for `ULN Registration`. When it displays, click **ULN Registration**.

2. Enter your root password.

3. Click **Forward**.

4. From the **Enter your account information** page, enter your Unbreakable Linux Network account information.

5. If your Oracle Linux 7 endpoint uses a proxy to access the Internet, click **Advanced Network Configuration** to enter proxy information. Close the dialog when you're done.

6. Click **Forward**.

7. [Optional] Enter a **System Name** and choose whether to send Oracle your system profile data.

8. Click **Forward**.

9. Click **Finish** to complete registration.

Result: Your endpoint is subscribed to the Oracle Unbreakable Network. Provided that the endpoint has a HEAT PatchLink DataCenter Agent for Linux/UNIX installed, you can begin deploying content to it.

Oracle Solaris 11 Endpoint Configuration

Before you can deploy patch content to you Oracle Solaris 11 endpoints, you have to register your endpoints Solaris and attach a repository.

Complete this process from you Solaris 11 endpoints.

Note: This procedure will get your endpoints up and running, but it you need full documentation, you can find it at the Oracle Technology Network.

1. Download a certificate and key from Oracle so that the endpoint can access the Oracle Solaris 11 repository you're licensed for.

   a) Open a Web browser and navigate to http://pkg-register.oracle.com.
   b) Click **Request Certificates**.
   c) Sign in using your Oracle Account credentials.
   d) Select a repository and click **Submit**.
   e) If necessary, type a comment in **ADDITIONAL CERTIFICATE DATA**.
   f) Review Oracle's License Agreement and, if you agree to their terms, click **Accept**.

HEAT software

g) Click **Download Key** and **Download Certificate**.

Step Result: The certificate and key are downloaded. **Leave the Web browser open.** It contains instruction for installing your downloads.

2. Install the repository certificate you just downloaded on your endpoint.

a) Open *Terminal*.

b) Follow the instructions listed in your Web browser.

Result: Your endpoint is subscribed to your licensed Solaris repository. Provided that the endpoint has a HEAT PatchLink DataCenter Agent for Linux/UNIX installed, you can begin deploying content to it.

SUSE Linux 12 Endpoint Configuration

Before you can deploy patch content to your SUSE Linux 12 endpoints using HPL, you must register the endpoint with the SUSE Customer Center. SUSE 12 includes a wizard that makes this process fast and painless.

Complete this task from your SUSE 12 endpoints.

1. From the dashboard, search for YaST, open it, and then enter the root password.

2. Open **Online Update**.

3. When prompted, run the configuration workflow.

4. Enter the email address for your SUSE Customer Center account and your registration code.

5. If you have a local registration server, click **Local Registration Server** and enter its URL.

6. Click **Next** to begin registration.

Result: Your endpoint is subscribed. Provided that the endpoint has a HEAT PatchLink DataCenter Agent for Linux/UNIX installed, you can begin deploying content to it.

> **Important:** While using HEAT PatchLink DataCenter to patch your SUSE 12 endpoints, you may need to disable the Snapper snapshot manager. If you leave it enabled, it takes two snapshots every time you make a deployment to your endpoints. These snapshots may lead to disk space issues. See Knowledge Base Article 1734 for information on disabling Snapper.

Configuring AIX 7.1 and 6.1 Endpoints to Download Content

To patch your AIX 6.1 and later endpoints using HPL, your AIX endpoints must have Service Update Management Assistant (SUMA) enabled. SUMA is enabled by default, but you may need to configure some of its variables to work in your environment before you can begin patching the endpoint using HPL.

1. Log on to your AIX endpoint.

2. Elevate your privleges.

From the command line, enter `su` and your password.

3. Preview a maintence download to check if SUMA is working correctly.

Enter `suma -x -w -a Action=Preview`.

The download preview may take a minute.

Step Result: If the preview download succeeds, you'll see output similar to:

```
        ...
        Download SUCCEEDED: /usr/sys/inst.images/installp/ppr/
wio.fcp.6.1.6.18bff
        Summary:
                586 downloaded
                0 failed
                0 skipped
```

If you see this in the command line, you're done! Don't worry about completing the next step.

4. If the preview download fails, SUMA is not configured correctly to work in your environment. You'll need to edit SUMA before you can use HPL to patch AIX.

a) From the command line, enter `smit suma`
b) Select `Configure SUMA` and press **ENTER**.
c) Press **ENTER** to select **Base Configuration**.
d) Edit the list of options that appear for operations in your enterprise. When you're done, close SUMA.
e) Once again, preview a maintence download to check if SUMA is working correctly.

Enter `suma -x -w -a Action=Preview`.

Result: If SUMA is working correctly, you're all set to begin patching your AIX endpoints using HPL. However, if you're still having trouble getting SUMA to work, contact your enterprise IT Helpdesk. You may have restrictive firewall settings in place that are interfering with SUMA.

Configuring Linux Endpoints for SELinux

If you want to use HEAT PatchLink DataCenter for Microsoft System Center on a Linux endpoint that has Security-Enhanced Linux with enforcing mode enabled, you must enter a command after installing the agent. Entering this command lets you install patch content using HPL.

This procedure is only relevant for older versions of Linux. Complete this procedure after the agent completes its initial Discover Applicable Updates task.

Note: Newer versions of Linux are configured to work with SELinux by default. Don't complete this procedure for newer platforms.

1. Log on to your Linux endpoint using the Security-Enhanced Linux module.

2. Open **Terminal**.

HEAT®software

3. Elevate your privileges.

Enter `sudo -s` and the root password.

4. Enter the following command:

```
chcon -t rpm_exec_t/HEAT PatchLink DataCenter Agent for Linux/UNIX path/mcescan/
bin/python
```

Tip: The default HEAT PatchLink DataCenter Agent for Linux/UNIX path is /usr/local/patchagent.

Result: The endpoint running SELinux is configured for deployments from the HEAT Patch Manager DataCenter Server.

Tip: After deploying content to the endpoint, you can confirm it installation by entering this command in **Terminal**:

```
ls -Z /usr/local/patchagent/mcescan/bin/python
```

Patch Agent Command Line Usage

The Patch Agent for Linux, UNIX, and Mac is a command line based application that does not have a user interface.

From the `usr/local/patchagent/` directory within terminal, you can enter a variety of commands to control the agent.

Table 176: Patch Agent Commands

Command	Description
`./patchservice info`	Indicates general information about the agent.
`./patchservice status`	Indicates the status of the agent process.
`./patchservice daustatus`	Indicates the status of the Discover Applicable Updates task.
`./patchservice detect`	Starts the detection task.
`./patchservice stop`	Stops the agent process.
`./patchservice restart`	Stops and starts the agent process.
`./patchservice patchdirectory`	Sets the directory where patches will be temporarily downloaded.
`./patchservice setmacro`	Specifies the macro definitions that should be used by the agent.
`./patchservice archivelogs`	Archives the agent logs so that they can be sent to HEAT.
`./patchservice proxysetup`	Configures your proxy server.

Command	Description
`./patchservice clearAgentLog`	Clears the agent error log file.
`./patchservice clearErrLog`	Clears the agent error log file.
`./patchservice clearDetectLog`	Clears the agent detection log file.
`./patchservice trimlogs`	Reduces the size of the error, agent, and detect log files. Oldest entries are deleted and the file is truncated at 100,000 lines.
`./patchservice setagentnice`	Sets the agent's prioritization value.
`./patchservice help`	Displays the patch server script usage information.

HEAT®software

Chapter

15

Using HEAT Installation Manager

The HEAT Installation Manager is a utility you can use to install, uninstall, or update HEAT PatchLink DataCenter for Microsoft® System Center components.

The HEAT Installation Manager (Installation Manager) is accessible following HEAT PatchLink DataCenter for Microsoft System Center installation.

HEAT Installation Manager

HEAT PatchLink DataCenter for Microsoft System Center is a platform that supports various solutions to security threats. These solutions are called components and consist of *platform components* and *module components*, which are delivered by the HEAT Installation Manager (Installation Manager).

The Installation Manager is installed during the initial HEAT PatchLink DataCenter installation and can be accessed following setup using the SCCM console. Use the Installation Manager to update HEAT PatchLink DataCenter.

HEAT software

Accessing Installation Manager Via HEAT PatchLink DataCenter for Microsoft System Center

You can open Installation Manager using one of several pages within the HEAT PatchLink DataCenter for Microsoft System Center Web console.

Prerequisites:

- Install of HEAT PatchLink DataCenter for Microsoft System Center is completed.
- You have been assigned the *Administrator* role or the **Installation Manager** access right.

You can perform this task from any endpoint in your network.

1. Log in to HEAT PatchLink DataCenter.

2. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

3. Click **Launch Installation Manager**.

Result: The Installation Manager opens in a new browser window to the ***New/Update Components*** tab.

> **Note:** When accessing a HEAT PatchLink DataCenter for Microsoft System Center Server that uses SSL, Microsoft Silverlight may create notification dialogs that you must acknowledge.

The Navigation Menu

This menu appears on all HEAT Installation Manager pages. Use this menu to navigate through the Web console.

This menu organizes product features based on functionality. When you select a menu item, a new page or dialog opens. You can access all features of the system from this menu.

Table 177: Navigation Menu

Menu	Menu Item	Function
Home		Opens the entrance page to HEAT Installation Manager. For additional information, refer to The Home Page on page 420.
Tools	**View Install Log...**	Opens the **Install Log** dialog. For additional information, refer to The Installation Log on page 430.

Menu	Menu Item	Function
Help	**Help Topics...**	Opens the HEAT PatchLink DataCenter for Microsoft System Center Help system.
	Knowledge Base...	Opens the HEAT Knowledge Base at HEAT Support (http://support.lumension.com) .
	Technical Support	Opens the ***Technical Support*** page. For additional information, refer to The Installation Manager Technical Support Page on page 433.
	Product Licensing	Opens the ***Product Licensing*** page. For additional information, refer to The Installation Manager Product Licensing Page on page 436.
	About...	Opens the ***About*** dialog.

HEAT®software

The Home Page

This page is the entrance page to HEAT Installation Manager. It consists of two tabs: the **New/Update Components** tab and the **Existing Components** tab.

For additional information on each tab, refer to:

- The New/Update Components Tab on page 421
- The Existing Components Tab on page 427
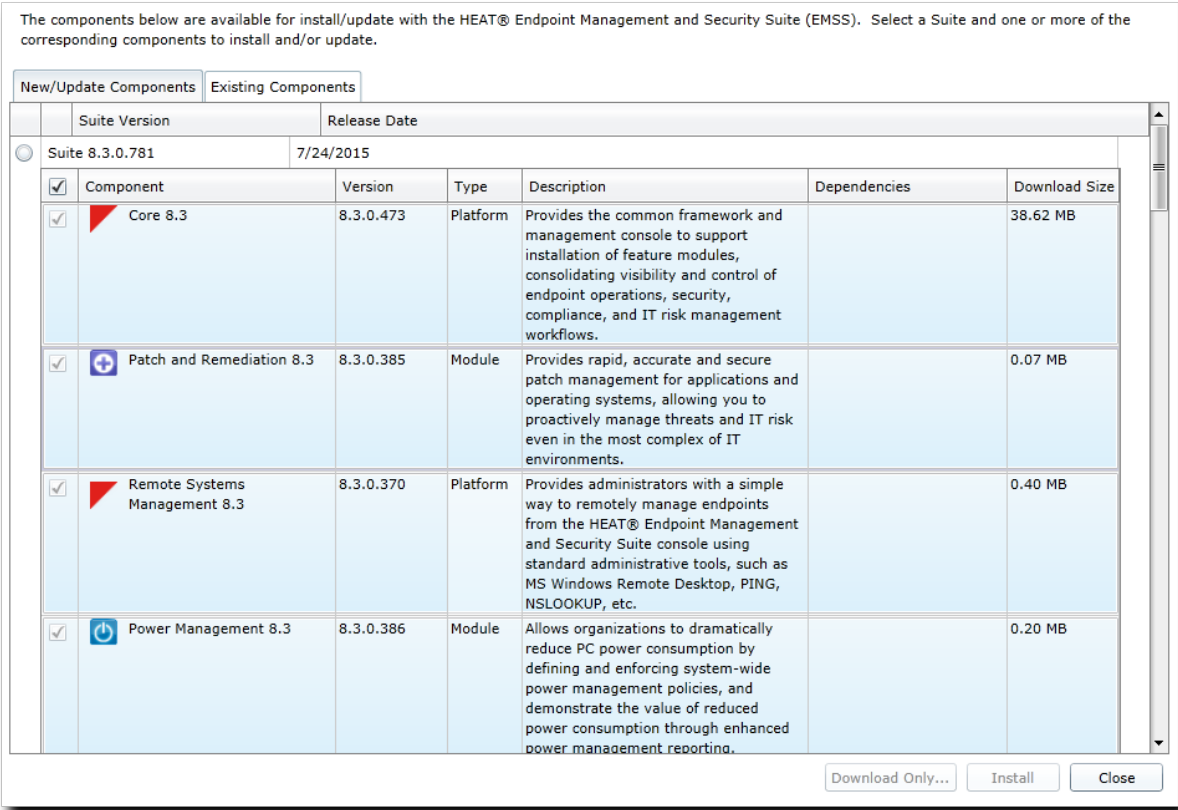
Figure 78: Home Page

The New/Update Components Tab

Use this tab to manage components and your HEAT PatchLink DataCenter for Microsoft System Center version. This tab lists each yet-to-be installed component available for each HEAT PatchLink DataCenter for Microsoft System Center release.
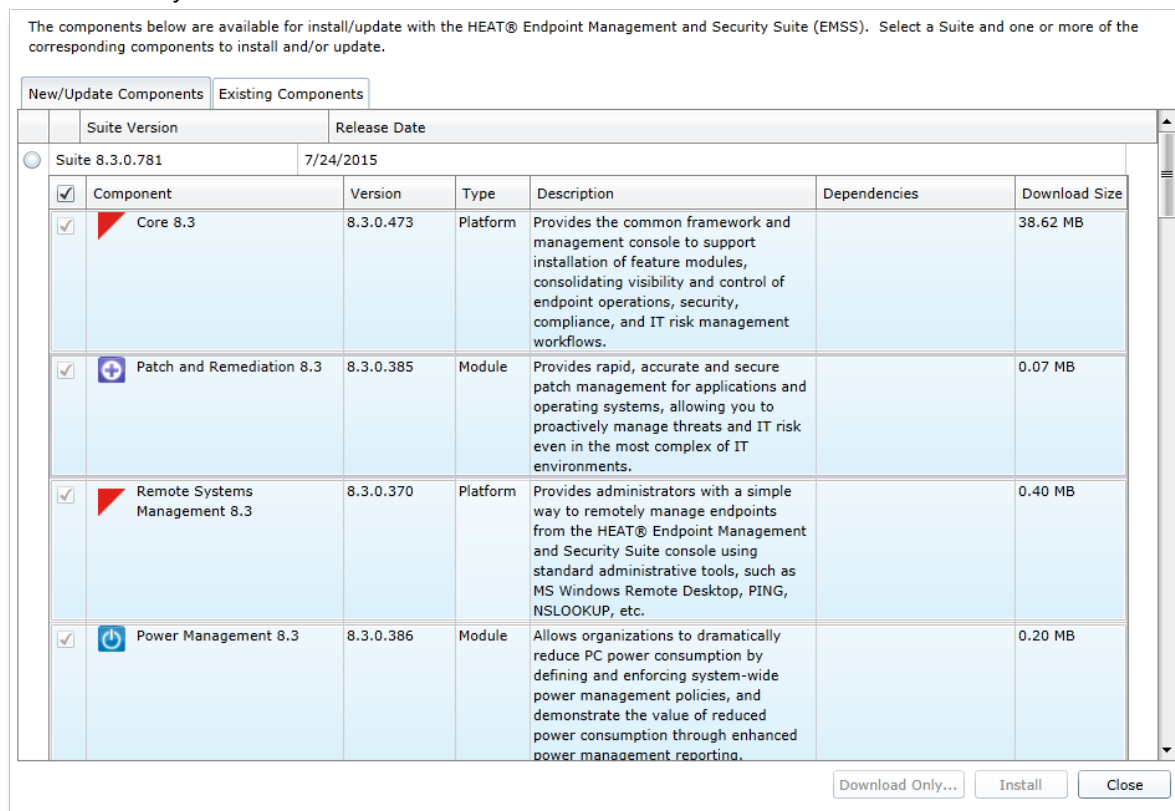
Figure 79: New/Update Components Tab

Use this tab to complete the following component management tasks:

- Download components. For additional information, refer to Downloading Components on page 423.
- Install downloaded components. For additional information, refer to Installing Downloaded Components on page 424.
- Download and install components. For additional information, refer to Installing or Updating Components on page 425.

HEAT®software

The New/Update Components Tab List

The tab list itemizes all unapplied components for each HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) release.

This list is separated into two tiers.

- Tier one lists the HEAT PatchLink DataCenter release.
- Tier two lists unapplied components for the applicable HEAT PatchLink DataCenter release.

The following table describes the first tier of the **New/Update Components** tab list.

Table 178: New/Update Components Tab List (Tier One)

Column	Description
Suite Version	The version number of the applicable HEAT PatchLink DataCenter release.
Release Date	The date and time the associated HEAT PatchLink DataCenter update was released.

The following table describes the second tier of the **New/Update Components** tab list. This tier lists the components available for the applicable HEAT PatchLink DataCenter release.

Table 179: New/Update Components Tab List (Tier Two)

Column	Description
Component	The component available for installation.
Version	The version of the component.
Type	The type of component (`Platform` or `Module`).
Description	The description for the component.
Dependencies	The prerequisite component needed to install the component.
Download Size	The size of the component (in MBs).

The New/Update Components Tab Buttons

After selecting components from the **New/Update Components** tab list, use the available buttons to initiate installations or downloads.

The following table describes the **New/Update Components** tab button functions.

Table 180: New/Update Components Tab Buttons

Button	Function
Download Only...	Downloads the selected components. For additional information, refer to Downloading Components on page 423.

Button	Function
Install	Installs the selected components. For additional information, refer to Installing or Updating Components on page 425.
Close	Closes Installation Manager.

Working with Installs and Updates

You can download, install, or update HEAT PatchLink DataCenter for Microsoft System Center components from the ***New/Update Components*** tab.

You can perform the following tasks from this tab:

- Downloading Components on page 423
- Installing Downloaded Components on page 424
- Installing or Updating Components on page 425

Note: HEAT Installation Manager is updated periodically to take advantage of higher performance or added features. Refer to Updating HEAT Installation Manager on page 438 for additional information.

Downloading Components

You can use the HEAT Installation Manager to download components for later installation.

Prerequisites:

A full replication has completed prior to using the HEAT Installation Manager. Refer to Updating HPL System Files and Content on page 100 for additional information.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.
2. Click **Launch Installation Manager**.
3. If necessary, upgrade Silverlight by clicking **Install**.
4. If necessary, upgrade Installation Manager by clicking **Install**. Click **Close** when the upgrade finishes.
5. If necessary, click **Reboot Server**, and then log back into the Web console.
6. Select a **Suite Version** radio button.

    - If you are updating the entire suite, select the radio button for the latest **Suite Version**.
    - If you are only installing new modules, leave the current suite version selected.

    Tip: When you select a **Suite Version**, other suite versions their components are greyed out to prevent mixing.

HEAT software

7. [Optional] Select any new components you want to install.

When updating the suite version, modules already installed are automatically selected for update and cannot be deselected.

8. Click **Download Only**.

Step Result: The ***Download Components*** dialog opens and the download begins.

> **Note:** If downloading a component with unmet prerequisites, a notification dialog opens, prompting you to download the prerequisites. Click **Yes** to download the prerequisites or **No** to skip them. You cannot install the selected component(s) until the prerequisites are downloaded and installed.

9. When the download completes, click **Close**.

Step Result: The ***Download Components*** dialog closes.

Result: The component(s) are downloaded.

> **Note:** The default location for downloaded components is <Installation Directory>\Lumension \EMSS\Content\.

After Completing This Task:
You may install the component at any time after downloading. Refer to Installing Downloaded Components on page 424 for install information.

Installing Downloaded Components
You can use HEAT Installation Manager to install downloaded components.

Prerequisites:

The components require downloading. Refer to Downloading Components on page 423 for download information.

Complete install of downloaded components from the ***New/Update Components*** tab within the Installation Manager Web console.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

2. Click **Launch Installation Manager**.

3. If necessary, upgrade Silverlight by clicking **Install**.

4. If necessary, upgrade Installation Manager by clicking **Install**. Click **Close** when the upgrade finishes.

5. If necessary, click **Reboot Server**, and then log back into the Web console.

6. Select a **Suite Version** radio button.

   - If you are updating the entire suite, select the radio button for the latest **Suite Version**.
   - If you are only installing new modules, leave the current suite version selected.

   Tip: When you select a **Suite Version**, other suite versions their components are greyed out to prevent mixing.

7. [Optional] Select any new components you want to install.

   When updating the suite version, modules already installed are automatically selected for update and cannot be deselected.

8. Click **Install**.

9. If you haven't already, create a database backup before clicking **Next**.

   Step Result: The *Ready to Install* dialog opens.

10. Click the **terms and conditions** to review the user agreement.

11. After installation completes, review the *Confirmation* page. Click **Finish** when you are done.

   Tip:
   - Click **View install log** to review the install log.
   - Clear the **Launch** checkbox to cancel relaunch of the Web console.

Result: The downloaded component(s) are installed.

After Completing This Task:
Before you can begin using a newly installed module component, you must first install the module's endpoint component on endpoints hosting the HEAT PatchLink DataCenter agent.

Installing or Updating Components

You can use HEAT Installation Manager to download new or update existing components and install them automatically.

Prerequisites:

Complete replication. Refer to Updating HPL System Files and Content on page 100 for additional information.

Complete installs from the *New/Update Components* tab within the Installation Manager Web console.

1. From the **Administration** workspace, select **HEAT PatchLink DataCenter** > **Configuration** > **Subscription Updates**.

2. Click **Launch Installation Manager**.

3. If necessary, upgrade Silverlight by clicking **Install**.

HEAT software

4. If necessary, upgrade Installation Manager by clicking **Install**. Click **Close** when the upgrade finishes.

5. If necessary, click **Reboot Server**, and then log back into the Web console.

6. Select a **Suite Version** radio button.

- If you are updating the entire suite, select the radio button for the latest **Suite Version**.
- If you are only installing new modules, leave the current suite version selected.

Tip: When you select a **Suite Version**, other suite versions their components are greyed out to prevent mixing.

7. [Optional] Select any new components you want to install.

When updating the suite version, modules already installed are automatically selected for update and cannot be deselected.

8. Click **Install**.

9. If the *Prerequisites* dialog opens, resolve the requirements before continuing. Complete the substeps below.

If the *Database backup recommended* dialog opens, proceed to .

a) Click **Install** to install the requirements.

Tip:

- Click **Retry** to re-access the system for requirements.
- Click **Print** to print the requirements.

b) If necessary, **Reboot Server** and then log back in to HEAT PatchLink DataCenter.

10. If you haven't already, create a database backup before clicking **Next**.

Step Result: The *Ready to Install* dialog opens.

11. Click the **terms and conditions** to review the user agreement.

12. Click **Install** to begin installation. If prompted, click **OK** to proceed.

Installation takes several minutes.

13. After installation completes, review the *Confirmation* page. Click **Finish** when you are done.

Tip:

- Click **View install log** to review the install log.
- Clear the **Launch** checkbox to cancel relaunch of the Web console.

Result: The new components are installed.

After Completing This Task:
Before you can begin using a newly installed module component, you must first install the module's endpoint component on endpoints hosting the HEAT PatchLink DataCenter Agent for Linux/UNIX.

The Existing Components Tab

This tab lists the version of HEAT PatchLink DataCenter for Microsoft System Center currently installed on your server and the installed components.
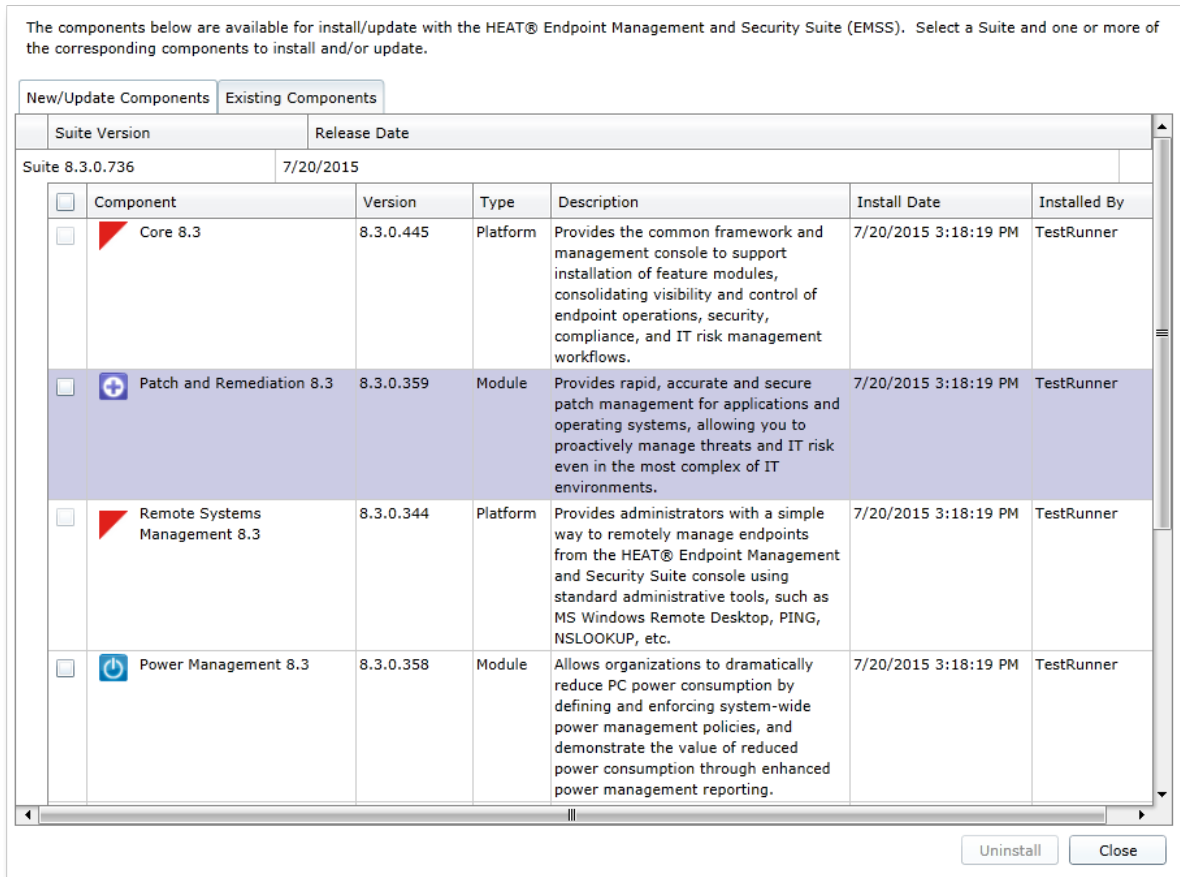
Figure 80: Existing Components Tab

Use this tab to uninstall existing module components.

The Existing Components Tab List

This list identifies which version of HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) is installed on your server and itemizes the components installed.

This list is separated into two tiers.

- Tier one lists the version of HEAT PatchLink DataCenter installed on your server.
- Tier two lists components installed on your platform. The list contains information about each platform and module component installed.

The following table describes the first tier of the **Existing Components** tab list.

Table 181: Existing Components Tab List (Tier One)

Column	Description
Suite Version	The version number of the applicable HEAT PatchLink DataCenter release.
Release Date	The date and time the associated HEAT PatchLink DataCenter update was released.

The following table describes the second tier of the **Existing Components** tab list.

Table 182: Existing Components Tab List (Tier Two)

Column	Description
Component	The name of the component installed on your HEAT PatchLink DataCenter Server.
Version	The version of the component.
Type	The type of component (Platform or Module).
Description	The description for the component.
Install Date	The date and time the component was downloaded from the Global Subscription Service.
Installed By	The person who installed the component.

The Existing Components Tab Buttons

Use tab buttons to uninstall existing HEAT PatchLink DataCenter for Microsoft System Center module components.

The following table describes the **Existing Components** tab button functions.

Button	Function
Uninstall	Uninstalls selected module components. For additional information, refer to Uninstalling Module Components on page 429.
	Note: Platform components cannot be uninstalled.
Close	Closes the HEAT Installation Manager.

Working with Uninstalls

You can uninstall existing HEAT PatchLink DataCenter for Microsoft System Center module components when they are no longer used or needed.

You can perform the following tasks from this tab:

Uninstalling Module Components

You can uninstall module components when they are no longer used or needed.

Uninstall module components from the *Existing Components* tab within the Installation Manager Web console.

1. From the navigation menu, select **Home**.

2. Select the *Existing Components* tab.

3. From the list, select the module component(s) you want to uninstall.

   Note: You may have to uninstall dependent modules as well. Platform components cannot be uninstalled.

4. Click **Uninstall**.

   Step Result: The *Database backup recommended* dialog opens.

5. Click **Next**.

   Step Result: The *Ready to Uninstall* page opens displaying a list of components that will be uninstalled.

6. Click **Uninstall**.

   Step Result: A warning dialog opens, notifying you that all data associated with the selected components will be lost.

HEAT®software

7. Click **Yes**

> **Step Result:** Selected components begin uninstalling.

> > **Tip:** Selecting the **No** or **Cancel** button cancels the uninstall, and you are returned to the ***New/Update Components*** tab.

8. When the component removal finishes, the ***Confirmation*** page listing uninstalled components displays.

> **Note:** Select the following options if needed:
>
> - Click the **View install log** link to view the install log. For additional information, refer to The Installation Log on page 430.
> - Deselect the **Launch HPL** check box to cancel the launch of HEAT PatchLink DataCenter for Microsoft System Center.

9. Click **Finish**.

> **Step Result:** Closes the ***Confirmation*** page.

Result: The selected HEAT PatchLink DataCenter module component(s) are uninstalled.

The Installation Log

The ***Installation Log*** is a dialog that lists details about HEAT Installation Manager events. The log lists occurrences from the last installation or removal of a component.
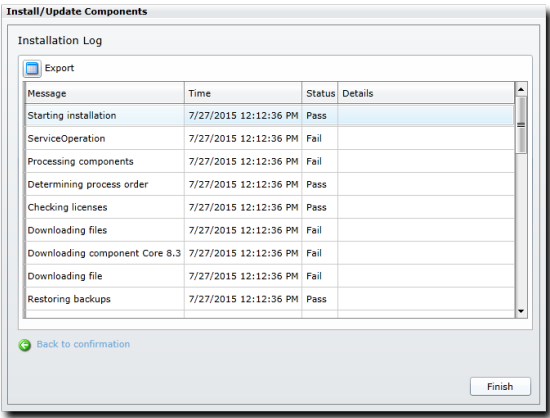
Figure 81: Installation Log

This log is especially useful for troubleshooting installation or removal failures. The log features a list and buttons.

Viewing the Installation Log

View the *Installation Log* for details about the events that occurred during the most recent installation or removal of HEAT PatchLink DataCenter for Microsoft System Center components.

View the *Installation Log* using the navigation menu within the Installation Manager Web console.

Tip: You can view the *Installation Log* from various locations in the HEAT Installation Manager console. For additional information, refer to one of the following topics:

- Installing or Updating Components on page 425
- Uninstalling Module Components on page 429

1. From the navigation menu, select **Tools** > **View Install Log**.

   Step Result: The *Installation Log* opens.

2. Review the log details. For additional information, refer to The Installation Log List on page 431.

The Installation Log List

After selected components are installed or removed, you may view a log of events that occurred during the process.

The following reference describes each column in installation log table.

Table 183: Installation Log Table Columns

Column	Description
Message	The name of the event.
Time	The date and time the event occurred.
Status	The outcome of the event (`Pass` or `Fail`).
Details	The notes regarding the event.

HEAT®software

The Installation Log Buttons

Use *Installation Log* buttons to perform tasks within the dialog.

The following table describes the *Installation Log* button functions.

Table 184: Install Log Buttons

Button	Description
Export	Exports the page data to a comma-separated value (`.csv`) file.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Finish	Closes the *Installation Log*.

Note: When viewing the log following an installation completion or failure, a **back to confirmation** link is available. Click this link to return to the installer *Confirmation* page. This link is not available when opening the log via the navigation menu.

The Installation Manager Technical Support Page

Use this page to contact technical support. Technical support provides assistance for HEAT Installation Manager or any other HEAT product.

Figure 82: Technical Support Page

This page features multiple support links. You can also use this page to contact support or provide comments for product improvement. In addition, this page also provides information about your HEAT PatchLink DataCenter for Microsoft System Center server and its components.

The page is divided into the following sections:

- Technical Support Options on page 434
- Server Information on page 434
- Suite Version Information (Installation Manager) on page 435

Viewing the Technical Support Page (Installation Manager)

Navigate to this page to access support assistance for HEAT Installation Manager or any other HEAT product.

You can access this page at any time from the Installation Manager navigation menu.

1. Select **Help** > **Technical Support**.

2. View the page.

Technical Support Options

HEAT Installation Manager provides access to various support assistance pages. Use these pages to communicate with HEAT. Click each link to open the applicable page in a new window.

The following table describes each link.

Contact Technical Support	When having difficulty using HPL or any of its modules, send an email to HEAT technical support to open a ticket. Support staff will help you resolve your issues.
Access Product Knowledge Base	The HEAT Knowledge Base contains release notes, defects, hotfixes, frequently asked questions, how-to procedures, and troubleshoot information for the HEAT software portfolio.
Access Product Web Site	The HEAT corporate Web site for HPL includes information about its software portfolio and how it can benefit your enterprise. It also contains helpful information about how to identify and prevent IT security issues.
Ask a Question	If you have questions about HPL or other HEAT software, contact us.
Request a Feature	If you want a new feature to improve your HPL user experience, send your request using our feature request page.
Provide Product Feedback	HEAT uses customer feedback to improve HPL. If you have an idea to improve it, see our customer feedback Web page.

Server Information

These fields list general information regarding the HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) system.

Table 185: Server Information Fields

Field	Description
Server Name	The name of the computer HEAT PatchLink DataCenter is installed on.
URL	The URL of the server HEAT PatchLink DataCenter is installed on.
Serial Number	The serial number used by HEAT PatchLink DataCenter.
Operating System	The operating system installed and running on the HEAT PatchLink DataCenter server.
OS Version	The operating system version number.
OS Service Pack	The service pack applied to the operating system, if applicable.

Field	Description
Last Connected	The date and time HEAT PatchLink DataCenter last connected to the Global Subscription Service (GSS).
Subscription Service ID	The ID assigned to HEAT PatchLink DataCenter upon registration with the GSS.
Replication Service Version	The replication service version number.
Last Agent Connection	The date and time a registered HEAT PatchLink DataCenter Agent last connected to the HEAT PatchLink DataCenter server.
Total Agents Registered	The total number of agents registered with HEAT PatchLink DataCenter.
Storage Volume Free Space	The amount of free disk space on your storage volume.
System Root Free Space	The amount of free disk space on your system volume.
IIS Version	The Internet Information Services (IIS) version installed.
.NET Version	The .NET Framework version(s) installed.
MDAC Version	The Microsoft Data Access Components (MDAC) version. The **Detail** button adjacent to the field opens the *MDAC File Version Information* dialog.
SQL File Version	The SQL Server file version installed.
SQL Version	The SQL Server version number followed by detailed information.

Suite Version Information (Installation Manager)

The **Suite Version Information** area displays the version number of HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter), each platform component installed, and each module component installed.

The following table describes each **Suite Version Information** field.

Table 186: Suite Version Information Fields

Field	Description
Server Suite Version	The version of HEAT PatchLink DataCenter installed on your HEAT PatchLink DataCenter server.
Core Version	The version of the HEAT PatchLink DataCenter core component installed on your HEAT PatchLink DataCenter server.
Installation Manager Version	The version of the Installation Manager installed on your HEAT PatchLink DataCenter server.

HEAT®software

Field	Description
Module **Version**	The name and version number of a HEAT PatchLink DataCenter module installed on your HEAT PatchLink DataCenter server. A field appears for each module installed on your server.

The Installation Manager Product Licensing Page

Use this page to view, validate, and export license information. It summarizes product component licenses applicable to your endpoint management activities including their expiration date. Product information is updated during daily replication with the Global Subscription Service.
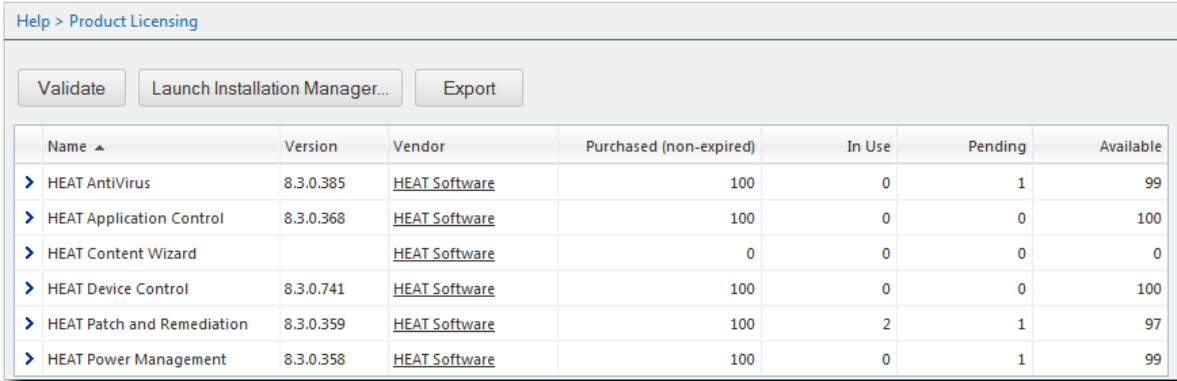
Figure 83: Product Licensing Page

Viewing the Product Licensing Page

View this page for information about the modules you are currently licensed for.

View the **Product Licensing** page using the navigation bar.

> Select **Help** > **Product Licensing**.

Result: The **Product Licensing** page opens.

The Product Licensing Page Buttons

Click these buttons to use functions related to licensing information.

The following table describes each button.

Table 187: Product Licensing Page Buttons

Button	Function
Validate	Initiates a license replication that searches for any changes to your license data. For additional information, refer to Validating License Information on page 437.

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

The Product Licensing Page List

The page list itemizes information about each HEAT PatchLink DataCenter for Microsoft System Center module you are licensed for.

The following table describes each **Product Licensing** page list column.

Table 188: Product Licensing Page List Column

Column	Description
Description	The module you are licensed for.
Version	The version number of the module.
Purchase Date	The date and time you purchased the module.
Vendor	The vendor that you purchased the module from.
Effective Date	The date that the module went into effect (not necessarily the purchase date).
Expiration Date	The date the module licensing expires.
Purchased	The total number of licences purchased for the module.

Validating License Information

Validating license information refreshes information about how many module licenses are available and in use. Validate license information after installing new modules.

Validate license information from the **Product Licensing** page.

1. Select **Help** > **Product Licensing**.
2. Click **Validate**.

Installation Manager Reference

Within HEAT PatchLink DataCenter for Microsoft System Center, you can use Installation Manager to install HEAT PatchLink DataCenter for Microsoft System Center components.

Occasionally, after upgrading HPL, you may be asked to update Installation Manager after opening it.

Updating HEAT Installation Manager

HEAT Installation Manager is updated periodically. Install the new version to take advantage of higher performance or added features.
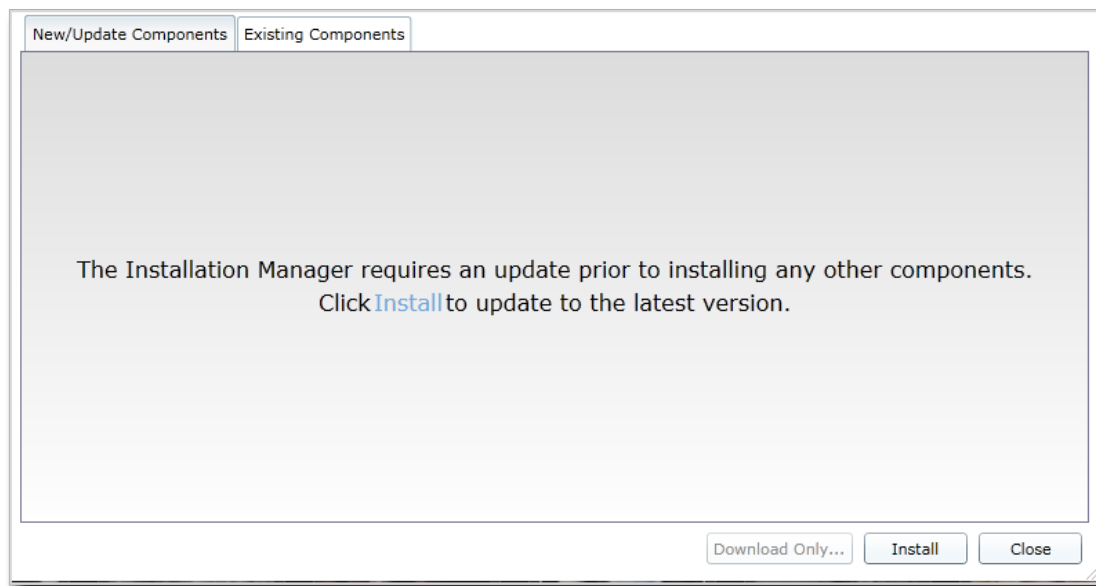
Figure 84: New/Update Components Tab

HEAT Installation Manager updates are downloaded and applied by HEAT PatchLink DataCenter, or you can install them manually as any other component. For additional information, refer to Installing or Updating Components on page 425. HEAT recommends installing updates immediately.

Note: If you are upgrading to HEAT PatchLink DataCenter using the HEAT Installation Manager, you may be asked to reboot the server to continue the update process.

Appendix

A

Appendices

In this appendix:

• System Requirements
• Server Reference
• Securing Your Server
• Creating a Disaster Recovery Solution

When using HEAT PatchLink DataCenter for Microsoft System Center, you may need to configure your server and network endpoints to ensure HEAT PatchLink DataCenter for Microsoft System Center operates optimally.

The appendices that follow describe actions you may need to take outside of the HEAT PatchLink DataCenter for Microsoft System Center system to ensure it is fully operational.

To prepare for HEAT PatchLink DataCenter for Microsoft System Center, you should:

• Familiarize yourself with system messages
• Secure HEAT PatchLink DataCenter for Microsoft System Center
• Configure network endpoints for scanning and agent management
• Prepare a HEAT PatchLink DataCenter for Microsoft System Center backup

System Requirements

HEAT PatchLink DataCenter for Microsoft® System Center, its component modules, and its agents each have software and hardware requirements for the endpoints that host them. Before installing any HEAT PatchLink DataCenter for Microsoft System Center software, verify that the target endpoints meet these requirements.

Some modules may have system requirements applicable specific to themselves. Refer to the topics within this appendix to verify whether your modules have additional requirments.

Note: Modules not referenced in this appendix do not have additional requirements beyond the basic HEAT PatchLink DataCenter for Microsoft System Center server and agent requirements.

HEAT software

Agent Requirements

The HEAT PatchLink DataCenter Agent for Linux/UNIX communicates with the HEAT Patch Manager DataCenter Server and keeps your endpoints secure. Before installing agents on your endpoints, review the endpoints to ensure they meet hosting requirements.

Supported Endpoint Operating Systems

The HEAT PatchLink DataCenter Agent for Linux/UNIX is supported on most operating systems used in enterprise environments.

The agent is supported on endpoints that contain one of the supported endpoint operating system types:

Mac Endpoint Operating Systems
A different agent, the HEAT PatchLink DataCenter Agent for Linux/UNIX 2.x, can be installed on many different versions of OSX. This version of the agent offers only HEAT PatchLink DataCenter functionality.

Table 189: Supported Mac Endpoint Operating Systems

Supported OS Versions	Supported Editions	Supported Processor(s)	Supported Agent
Mac OS X 10.10	All	Intel	Patch Agent for Linux, UNIX, and Mac 2.x
Mac OS X 10.9	All	Intel	Patch Agent for Linux, UNIX, and Mac 2.x
Mac OS X 10.8	All	Intel	Patch Agent for Linux, UNIX, and Mac 2.x
Mac OS X 10.7 [1]	All	Intel	Patch Agent for Linux, UNIX, and Mac 2.x
Mac OS X 10.6 [1]	All	Intel	Patch Agent for Linux, UNIX, and Mac 2.x
Mac OS X 10.5[1]	All	• Intel • PowerPC	Patch Agent for Linux, UNIX, and Mac 2.x
Mac OS X 10.4[1]	All	• Intel • PowerPC	Patch Agent for Linux, UNIX, and Mac 2.x
Mac OS X 10.3[1]	All	PowerPC	Patch Agent for Linux, UNIX, and Mac 2.x

Supported OS Versions	Supported Editions	Supported Processor(s)	Supported Agent
1. The installation wizard is not supported for OS X 10.7.2 and lower. It is only supported on 10.7.3 and higher.			

Linux Endpoint Operating System
A different agent, the HEAT PatchLink DataCenter Agent for Linux/UNIX 2.x, can be installed on many different versions of Linux. This version of the agent offers only HEAT PatchLink DataCenter functionality.

Table 190: Supported Linux Endpoint Operating Systems

Supported OS Versions	Supported Editions	Supported Processor(s)	Supported Agent
CentOS Linux 7		Intel	Patch Agent for Linux, UNIX, and Mac 2.x
CentOS Linux 6		Intel	Patch Agent for Linux, UNIX, and Mac 2.x
CentOS Linux 5		Intel	Patch Agent for Linux, UNIX, and Mac 2.x
Oracle Enterprise Linux 7		Intel	Patch Agent for Linux, UNIX, and Mac 2.x
Oracle Enterprise Linux 6		Intel	Patch Agent for Linux, UNIX, and Mac 2.x
Oracle Enterprise Linux 5		Intel	Patch Agent for Linux, UNIX, and Mac 2.x
Oracle Enterprise Linux 4		Intel	Patch Agent for Linux, UNIX, and Mac 2.x
SUSE Linux Enterprise 12	• Desktop • Server	Intel	Patch Agent for Linux, UNIX, and Mac 2.x
SUSE Linux Enterprise 11	• Desktop • Server	Intel	Patch Agent for Linux, UNIX, and Mac 2.x
SUSE Linux Enterprise 10	• Desktop • Server	Intel	Patch Agent for Linux, UNIX, and Mac 2.x

HEAT®software

Supported OS Versions	Supported Editions	Supported Processor(s)	Supported Agent
Red Hat Enterprise Linux 7	Server	Intel	Patch Agent for Linux, UNIX, and Mac 2.x
Red Hat Enterprise Linux 6	• Client • Server	Intel	Patch Agent for Linux, UNIX, and Mac 2.x
Red Hat Enterprise Linux 5	• Client • Server	Intel	Patch Agent for Linux, UNIX, and Mac 2.x

UNIX Endpoint Operating System
A different agent, the HEAT PatchLink DataCenter Agent for Linux/UNIX 2.x, can be installed on many different versions of UNIX. This version of the agent offers only HEAT PatchLink DataCenter functionality.

Table 191: Supported UNIX Endpoint Operating Systems

Supported OS Versions	Supported Editions	Supported Processor(s)	Supported Agent
Oracle Solaris 11	All	• Intel • SPARC	Patch Agent for Linux, UNIX, and Mac 2.x
Oracle Solaris 10	All	• Intel • SPARC	Patch Agent for Linux, UNIX, and Mac 2.x
Hewlett Packard HP-UX 11.31	All	• PA-RISC • Itanium	Patch Agent for Linux, UNIX, and Mac 2.x
Hewlett Packard HP-UX 11.23	All	PA-RISC	Patch Agent for Linux, UNIX, and Mac 2.x
Hewlett Packard HP-UX 11.11	All	PA-RISC	Patch Agent for Linux, UNIX, and Mac 2.x
IBM AIX 7.1	All	Power	Patch Agent for Linux, UNIX, and Mac 2.x
IBM AIX 6.1	All	Power	Patch Agent for Linux, UNIX, and Mac 2.x

Recommended Agent Configuration

HEAT recommends configuring server-to-agent communication according to the number of managed endpoints in your network.

After installing HEAT PatchLink DataCenter for Microsoft System Center Server and Agents, HEAT recommends configuring agent settings according to your network size.

HEAT recommends the following settings for the Patch Agent. Agent settings are edited within the HEAT PatchLink DataCenter for Microsoft System Center Web console.

Table 192: Application Settings: Options - Deployment Defaults

Node Count	< 50	< 500	< 1,000	< 5,000	< 10,000
Communication Interval (min)	15	30	30	60	60
Concurrent Deployment Limit (CDL) - Global	1000	1000	1000	2500	5000
CDL - Reboot	200	200	200	500	1000
CDL - DAU	500	500	500	500	1000
CDL - MB	200	200	200	400	800

HEAT recommends the following settings for the HEAT PatchLink DataCenter Agent.

Table 193: Application Settings: Agent Policy Sets - HEAT PatchLink DataCenter Agent Communication

Node Count	< 50	< 500	< 1,000	< 5,000	< 10,000
Send interval (sec)	2	3	4	5	6
Receive interval (sec)	0	0	0	0	0
Timeout interval (hour)	12	12	12	12	12
Heartbeat interval (min)	15	30	30	60	60

Note: If you are managing 10000+ endpoints, contact HEAT Support (http://support.lumension.com) for a recommended configuration.

Mac, Linux, or UNIX Endpoint Requirements

Before installing the HEAT PatchLink DataCenter Agent on a supported Mac, Linux, or UNIX endpoint, ensure that it meets the necessary hardware and software requirements.

Processor	500 MHz processor or higher

HEAT®software

Physical RAM	256 MBs or greater
	Note: Your HEAT PatchLink DataCenter endpoint may require additional RAM depending on the RAM requirements of other applications installed.
Disk Requirements	• Presence of a `/tmp` directory (`/var/tmp` on Oracle Solaris) with 100 MB of free space. • 50 MB of free space for the agent installation directory. • HEAT PatchLink DataCenter also recommends 100 Mb of unused disk space to download and install content.
Java Runtime Environment (JRE)	• Ensure Java Runtime Environment (JRE) 1.4.0 or later is installed.

	Note:
	• If installing using the installation wizard for OS X (versions 10.7.3-10.10), JDK 1.7 or later is required.
	• Open JDK can be substituted for Oracle Java JRE on the following operating systems:
	
	   • Cent OS Linux
	   • Novell SUSE Linux
	   • Oracle Linux
	   • Red Hat Enterprise Linux
	
	   Refer to IcedTea Project (http://openjdk.java.net/projects/icedtea/) for additional information.

Perl	Perl is needed for Linux content. Perl is automatically installed for all open-source Linux operating systems unless uninstalled.
	Tip: To determine if you have perl installed, type `perl -v` on a command line. Refer to Perl Download (http://www.perl.org/get.html) to download.
Network Connection	A 10 Mbps network connection with access to the HEAT PatchLink DataCenter for Microsoft System Center.

Antivirus	Ensure any antivirus software installed on the applicable endpoint computer is disabled.
Port Requirements	• Port `80`. This must be open for HEAT PatchLink DataCenter module downloads. • Port `443`. This must be open for HEAT PatchLink DataCenter policy download and general communication. • Ports `49152-65535`. These ports are used as listener ports for *check now* commands, which are server-sent requests that agents use to check for tasks. Closing these ports delays agent tasks until they check in themselves.

Supported Proxy Server Technologies

You can use proxy servers to facilitate the communication between your HEAT PatchLink DataCenter for Microsoft System Center components.

A proxy server can help a company ensure network security and provide administrative control. HEAT PatchLink DataCenter supports use of the following proxy technologies:

• Microsoft Security and Acceleration Server (ISA). Refer to About Internet Security and Acceleration Server (http://msdn.microsoft.com/en-us/library/ms811801.aspx) for additional information.
• Apache Web Server with Proxy Mod. Refer to Apache Module mod_proxy (http://httpd.apache.org/docs/2.4/mod/mod_proxy.html) for additional information.
• Squid Proxy Server 3.2 or later. Refer to Squid: Optimising Web Delivery (http://www.squid-cache.org) for additional information.

The following table displays which authentication types that are supported when using a proxy for communications between different HEAT PatchLink DataCenter components.

Table 194: Supported Proxy Technologies

Proxy Type	Authentication Types					
	NTLM (Challenge) Authentication		Basic Authentication		Non-Authenticated	
	HPL to GSS	HPL Agent to HPL	HPL to GSS	HPL Agent to HPL	HPL to GSS	HPL Agent to HPL
Microsoft Security and Acceleration Server (ISA)	Yes	No	Yes	Yes	Yes	Yes

HEAT®software

Apache Web Server with Proxy Mod	Yes	No	Yes	Yes	Yes	Yes
Squid Proxy Server	Yes	No	Yes	Yes	Yes	Yes

Note: A Squid proxy server will only properly resolve using a fully qualified domain name.

Refer to HEAT KnowledgeBase Article 1625 (http://www.lumension.com/kb/1625) for additional information on a Squid proxy server configuration.

Server Reference

Within HEAT PatchLink DataCenter for Microsoft® System Center, certain pages or code messages notify you of errors or events.

Refer to this appendix for a thorough definition of these pages and codes messages. This appendix also contains reference information regarding endpoint statuses, how to define scan targets using imported files, and how to restart the STATEngine Service.

Server Security

HEAT PatchLink DataCenter for Microsoft System Center limits access to only authorized users. Referring to the definitions in this topic will help you understand how security operates within Windows and the product.

There are multiple layers of security for HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter). These layers include:

Web Site Authentication	Internet Information Services (IIS) controls authentication for access to the HEAT PatchLink DataCenter Web site, which means the operating system itself is validating credentials.
Web Site Encryption via SSL	SSL provides an encrypted wrapper around all Web communication to and from the product. Therefore, installing HEAT PatchLink DataCenter with SSL provides an additional level of protection.
User (Security) Roles	Every feature, page, and action throughout HEAT PatchLink DataCenter is assigned to a series of access rights. These access rights combine to form a user role. Roles also contain a list of accessible endpoints and endpoint groups. Regardless of how a user is authenticated, the access and permissions are defined solely by the HEAT PatchLink DataCenter administrator.

Server Error Pages

When an error occurs within HEAT PatchLink DataCenter for Microsoft System Center, a special page opens that explains the error. Understanding these pages and what they mean will help you resume operations.

The HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) server provides several distinct error pages. These pages are:

Access Denied	Displays when a user fails to provide valid credentials during log in to the HEAT PatchLink DataCenter server. Also display when a user attempts to access a page or feature they do not have access to.
Internal Server Error	Displays when an unspecified internal error occurs. In most cases, closing the browser window and restarting your task will resolve the issue.
Refresh User Data	Displays when the current session expires. Usually displays following an extended period of inactivity.
Requested Page Not Found	Displays when a user attempts to navigate to a nonexistent server address. This page features links to other pages. Users can navigate from these links back to the desired page.
System Component Version Conflict	Displays when a system component version conflict is detected. To ensure optimal behavior, the system components of HEAT PatchLink DataCenter are checked every time a user logs in. If a conflict is detected, this page identifies the component(s) that caused the conflict.
	Note: HEAT PatchLink DataCenter also sends a notification email to the HEAT PatchLink DataCenter administrator when a conflict occurs.
Cache Expired	Displays when the user session expires. Usually displays following an extended period of inactivity.
Unsupported Browser Version	Displays when a user attempts to open the HEAT PatchLink DataCenter server with an unsupported browser.

HEAT®software

WinInet Error Codes

HEAT PatchLink DataCenter for Microsoft System Center uses Microsoft Window Internet application programming interface (WinInet API) for communication between the server and agents. When agent-server communication fails, a WinInet error code displays. Understanding these codes can help you resolve the communication errors.

The following table defines the most common error codes.

Note: Refer to Microsoft Knowledgebase article #193625 (http://support.microsoft.com/default.aspx?scid=kb;EN-US;193625) for additional WinInet error code descriptions.

Table 195: WinInet Error Code Descriptions

Agent Error Description	WinInet Error Code	Description
`Head failed: Head request failed. Error is 12002. . Host=1116 HTTP Error=0`	12002	The Internet connection timed out.
`Head failed: Head request failed. Error is 12031. . Host=1109 HTTP Error=0`	12031	The connection with the server has been reset.
`Head failed: Head request failed. Error is 12007. . Host=1109 HTTP Error=0`	12007	The server name could not be resolved.

HTTP Status Codes

As a Web-based application that uses Internet Information Services (IIS), HEAT PatchLink DataCenter for Microsoft System Center subsequently uses HTTP status codes. These codes appear when an HTTP error occurs while using the product. Understanding these codes will help you solve any issue that may arise.

While many of the status codes are informational only, the following table defines a few of the common error codes.

Table 196: HTTP Status Codes

Code	Description
`HTTP 401.1 - Login failed`	Log in attempt was unsuccessful (typically due to invalid user name or password).
	Note: HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenter) will display a custom error page (as defined under Server Error Pages on page 447) instead of the default **HTTP 401.1 - Logon failed** error page.

Code	Description
`HTTP 403.4 - SSL required`	You must use HTTPS instead of HTTP when accessing this page.
`HTTP 403.9 - Too many users`	The number of connected users exceeds the defined connection limit.
`HTTP 404 - Not found`	The requested file cannot be found.
	Note: HEAT PatchLink DataCenter will display a custom error page (as defined under Server Error Pages on page 447) instead of the default **HTTP 404 - Not Found** error page.

Setting Up HEAT PatchLink DataCenter for Microsoft System Center

Following installation and initial log in, the **Application Setup Manager** dialog opens. This dialog appears only once, the first time you log in to HEAT PatchLink DataCenter for Microsoft System Center and you use it to configure basic options within the system.

Prerequisites:

Complete HEAT PatchLink DataCenter installation and open the Web console in your browser.

You cannot reopen this dialog following its completion. However, you can access these settings from various HEAT PatchLink DataCenter pages.

1. Log in to HEAT PatchLink DataCenter. For additional information, refer to Logging In.

   Step Result: HEAT PatchLink DataCenter opens to the **Customer Info** tab of the **Application Setup Manager** page. This dialog only appears the first time HEAT PatchLink DataCenter is opened.

2. Ensure the **Customer Info** tab is selected.

3. Type the applicable information in the following fields.

Field	Description
First name	Your first name.
Last name	Your last name.
Company name	Your company name.
	Note: The company name specified during installation appears by default, but can be edited.

4. Click **Apply**.

   Step Result: The information is saved.

HEAT software

5. Select the *Languages* tab.

6. Select the check box associated with the languages you want to receive content in.

Each content item available in HEAT PatchLink DataCenter may be available in multiple versions for different languages.

7. Ensure the *Uninstall Password* tab is selected.

8. Define the **Global uninstall password**.

This password is used to manually uninstall HEAT PatchLink DataCenter agents and should be kept confidential. Type the password in the following fields.

a) In the **Global uninstall password** field, type the desired password.

b) In the **Confirm password** field, retype the password.

Tip: For information on how to edit this password outside of the *Application Setup Manager*, refer to Changing the Global Uninstall Password on page 242.

9. Click **Apply**.

Step Result: The information is saved.

10. Select the *Email Notifications* tab.

11. Define the host and email information.

Email notifications are alerts sent by HEAT PatchLink DataCenter when certain system events occur. Type the applicable information in the following fields.

Field	Description
SMTP Host	The local SMTP mail host name. HEAT PatchLink DataCenter uses your corporate Internet (SMTP) mail server.
'From' email address	The email address used when the system sends email notifications.
'To' email address	An email address you use to receive system notifications.

12. Click **Apply**.

Step Result: The information is saved.

13. Select the *Install an Agent* tab.

14. [Optional] The **Automatically install an agent on the server** check box is checked by default.

This installs the agent on the server and is the recommended setting.

a) Select the check boxes for the applicable modules.

Selecting these modules activates agent functionality associated with the module.

> **Tip:** For additional information about installing an agent on the server outside of the ***Application Setup Manager***, refer to Downloading the Agent Installer on page 112.

15. Click **Apply**.

Step Result: Your initial settings are saved.

16. Click **Close**.

Step Result: The ***Application Setup Manager*** closes with your saved changes.

Result: Initial configuration is complete. You are now ready to begin monitoring your network with HEAT PatchLink DataCenter.

Securing Your Server

HEAT PatchLink DataCenter for Microsoft® System Center protects your network endpoints. Server operation is critical to your network's overall security.

To ensure your server is secure as possible, HEAT suggests implementing the following security practices:

> **Note:** For additional information on securing your server, refer to Securing Your Application Server (http://msdn.microsoft.com/en-us/library/ff648657.aspx).

Secure Your Server With SSL

Implement Secure Sockets Layer (SSL) to secure all HEAT PatchLink DataCenter for Microsoft System Center communication.

SSL is a protocol which is designed to provide secure data transmission over the Internet. SSL support is included in Web browsers, Web servers, and operating systems.

HEAT PatchLink DataCenter uses SSL when downloading vulnerability data and packages from the Global Subscription Service.

HEAT software

In addition, SSL can be used for transmitting data between the HEAT PatchLink DataCenter server and HEAT PatchLink DataCenter Agent by enabling SSL during the installation of HEAT PatchLink DataCenter. The installation process requires obtaining a SSL certificate (`.CER`).

Use Secure Passwords

When setting passwords for HEAT PatchLink DataCenter for Microsoft System Center, using secure passwords significantly lowers the probability that your server can be compromised.

Worm attacks, which attempt to install malicious software on a target endpoint, frequently test log ins with weak and commonly used passwords. For secure passwords, HEAT recommends a 12 character password that combines mixed-case alpha characters, numeric characters, and punctuation characters.

Disabling File and Printer Sharing

When installing HEAT PatchLink DataCenter for Microsoft System Center, you should disable the File and Printer Sharing for Microsoft Networks protocol on the target server. If this protocol is left active, it creates a security risk that intruders can exploit: a Windows networking share. Therefore, File and Printer Sharing for Microsoft Networks should be disabled.

Placing Your Server Behind a Firewall

HEAT recommends placing your HEAT PatchLink DataCenter for Microsoft System Center server behind a firewall. This procedure is considered best-practice.

Since the HEAT PatchLink DataCenter for Microsoft System Center (HEAT PatchLink DataCenterserver receives content updates from the Global Subscription Service (GSS), allowing the HEAT PatchLink DataCenter server specific Internet access is unnecessary. However, access to the GSS must be specified in your firewall configuration.

Disable Non-Critical Services

HEAT PatchLink DataCenter for Microsoft System Center only requires several essential services to operate. Disabling services that are not critical to its operation reduces security risks.

The default installation of Microsoft Windows sets most features and services to active. Therefore, there may be a number of services that can be disabled (e.g.: RPC, Remote Registry, etc.) to reduce security compromises. HEAT does not encourage a lock down by disabling Windows services. However, it can be an effective method to reduce the risk of hacker attacks.

The following services are required to run HEAT PatchLink DataCenter for Microsoft System Center:

- World Wide Web Publishing Service
- IIS Admin Service
- SQL Server
- Replication Service
- STATEngine
- EDS Server
- EDS InstallerService

Prior to disabling non-essential services, contact HEAT Support (http://support.lumension.com) to ensure disabling services does not impact your server performance.

Lock Down Unused TCP and UDP Ports

Unused ports within the Windows Server operating system pose a security risk to HEAT Patch Manager DataCenter Servers. Therefore, these ports should be closed.

Use a firewall to prevent network traffic on various unused and vulnerable TCP and UDP ports. However, if a firewall is not available or additional server-level disablement is desired, TCP and UDP ports can be disabled as a function of the network connection.

Apply All Security Patches

The HEAT PatchLink DataCenter for Microsoft System Center server should have the most recent security patches installed.

Apply all applicable Microsoft Security Patches to ensure that the server remains protected against all known security threats. Be sure to apply the most recent patches for Internet Information Services, SQL Server, and the version of Windows server in use.

Creating a Disaster Recovery Solution

HEAT PatchLink DataCenter for Microsoft System Center uses Microsoft SQL Server to store data values; therefore, you should prepare your instance of Microsoft SQL Server for a disaster.

The most important part of an effective disaster recovery solution is having a current and valid backup. You can create backups either manually or as part of a Database Maintenance Plan.

Note: This appendix applies to Microsoft SQL Server 2008 and requires the Microsoft SQL Server Management Studio. The Management Studio is available by upgrading to SQL Server 2008 Standard or Enterprise. For further information, see Microsoft SQL Server 2008 (http://www.microsoft.com/sqlserver/2008/en/us/default.aspx).

Preparing Your Database

In the event of a disaster, detailed transaction logs are useful when restoring your database. You can control the level of detail that your logs record.

The installation of HEAT PatchLink DataCenter for Microsoft System Center sets your database to a recovery model of `Simple`. To use *Transaction Logs*, and thus increase the quality of your disaster recovery solution, you should change the recovery model to `Full`.

Changing the Database Recovery Model

Modify the database recovery model to record more robust details about the events leading to a disaster.

Database recovery model edits take place in the ***SQL Server Management Studio***.

1. Open the ***Microsoft SQL Server Management Studio***.

2. Log into your database server.

3. In the directory tree, expand ***Server Name\SQL Instance*** > **Databases**.

HEAT software

4. Right-click the PLUS database.

5. Select **Properties**.

Step Result: The *Database Properties* window opens.
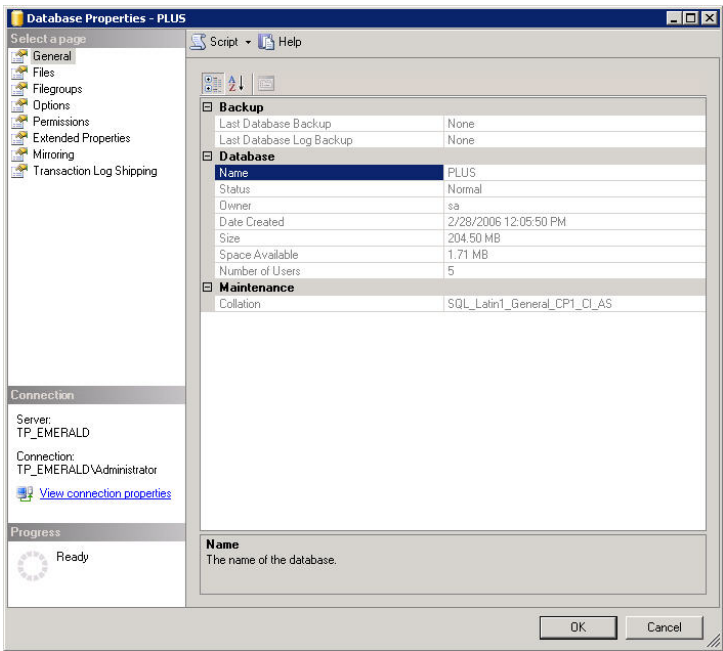
Figure 85: Database Properties

6. In the **Select a Page** pane, click **Options**.

Step Result: The *Options* page opens.

7. In the **Recovery model** list, select **Full**.

> **Note:** A full database backup backs up the whole database. This includes part of the transaction log so that full database backup can be recovered.

8. Click **OK**.

Step Result: The changes are saved and the *Database Properties* window closes.

9. Repeat the recovery model modification process for the following databases:

Table 197: Database Names

Database Name	Product
STAT_Guardian	HEAT PatchLink DataCenter for Microsoft System Center
UPCCommon	HEAT PatchLink DataCenter for Microsoft System Center

Database Name	Product
UPCExtended	HEAT PatchLink DataCenter for Microsoft System Center
PLUS_Reports	HEAT Enterprise Reporting Client
SCM	HEAT Security Configuration Management
ERS	HEAT Enterprise Reporting
ERS_Staging	HEAT Enterprise Reporting
ReportServer [1]	Microsoft SQL Server Reporting Services
ReportServerTempDB [1]	Microsoft SQL Server Reporting Services
SafeGuard [2]	powered by Sophos®
(1) Subscription features available in Microsoft SQL Server Reporting Services can be implemented in HEAT Enterprise Reporting. By default, the database names are ReportServer and ReportServerTempDB. (2) Data protection capabilities in is enhanced with a full disk encryption add-on from Sophos. The installation of results in a Safeguard database.	

After Completing This Task:

You must create a backup of each database before any Transaction logs will be created. Refer to Creating a Database Backup on page 455 to create a one-time backup of your database.

Creating a Manual Solution

To prevent data loss, create a database solution, and implement it in the event of a disaster.

While a Maintenance Plan will allow you to automate the backup of your databases and transaction logs, you can also create and restore individual backups using the SQL Server Management Studio.

Creating a Database Backup

The most important part of an effective disaster recovery technique is having a current and valid backup. Create a backup for the SQL Server instance associated with HEAT PatchLink DataCenter for Microsoft System Center to assure minimal system data is lost if a disaster occurs.

Backups are created within SQL Server Management Studio.

1. Open the *Microsoft SQL Server Management Studio*.

2. Log into your database server.

3. In the directory tree, expand to **Databases** (*Server Name* > *SQL Instance* > **Databases**).

4. Right-click the PLUS database.

HEAT®software

5. Select **Tasks** > **Backup**.

   Step Result: The *Back Up Database* window opens.
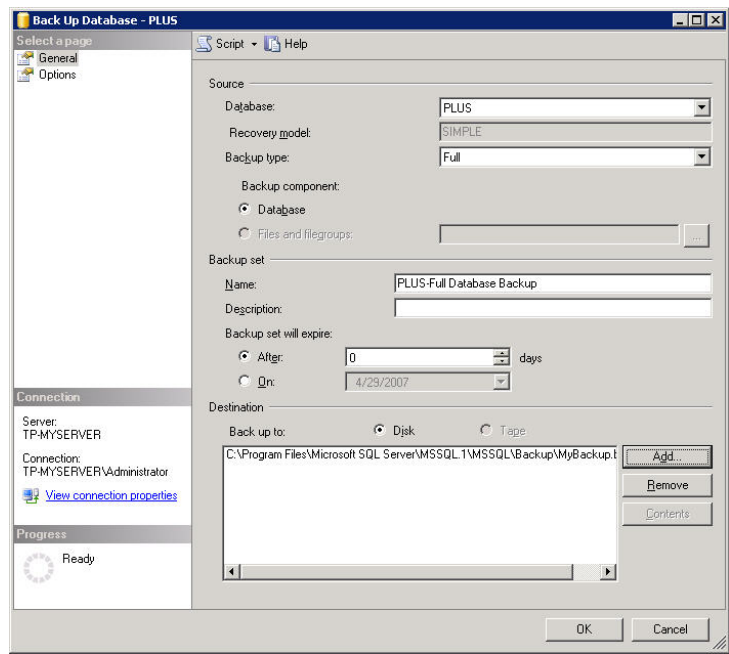
Figure 86: Back Up Database

6. Ensure that the Source values are set as follows:

- **Database**: `PLUS`
- **Recovery model**: `Full`

   Note: If the **Recovery model** is not set to Full, refer to Changing the Database Recovery Model on page 453.

- **Backup Type**: `Full`
- **Backup Component**: `Database`

7. Define the **Backup set** identification fields.

   The following table describes each field.

Field	Description
Name	The name of the backup set.
Description	The description of the backup set.

8. Define the backup set expiration date.

Use one of the following methods.

Method	Steps
To define an expiration date based on a set number of days:	1. Select the **After** option. 2. Type the desired number in the **After** field.
To define an expiration date based on a set date:	1. Select the **On** option. 2. Select the desired date frm the **On** list.

9. Define your backup **Destination** settings.

   a) Select either the **Disk** or **Tape** option.

   b) Define the destination **Folder**.

> **Note:** For performance reasons, it is recommended that you create your database backup in a directory that is not on the same physical drive as your database.

10. Select `Options` within the **Select a page** pane.

Step Result: The *Options* page displays.
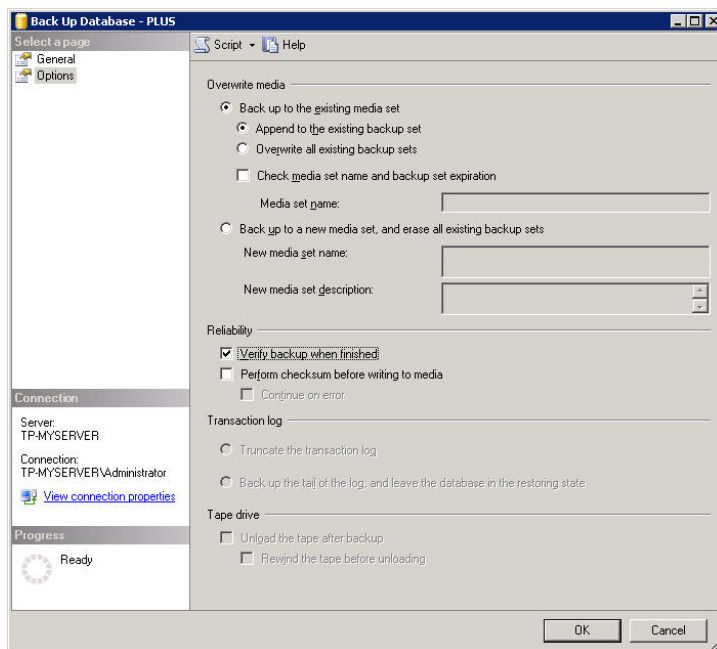
Figure 87: Back Up Database - Options

HEAT software

11. Select whether to **Backup up to the existing media set** or **Back up to a new media set, and erase all existing backup sets** as is appropriate for your organization.

12. Select the **Verify backup when finished** option to ensure a valid backup.

13. Click **OK**.

14. Repeat steps 5 through 13 for the following databases:

Table 198: Database Names

Database Name	Product
STAT_Guardian	HEAT PatchLink DataCenter for Microsoft System Center
UPCCommon	HEAT PatchLink DataCenter for Microsoft System Center
UPCExtended	HEAT PatchLink DataCenter for Microsoft System Center
PLUS_Reports	HEAT Enterprise Reporting Client
SCM	HEAT Security Configuration Management
ERS	HEAT Enterprise Reporting
ERS_Staging	HEAT Enterprise Reporting
ReportServer [1]	Microsoft SQL Server Reporting Services
ReportServerTempDB [1]	Microsoft SQL Server Reporting Services
SafeGuard [2]	powered by Sophos®
(1) Subscription features available in Microsoft SQL Server Reporting Services can be implemented in HEAT Enterprise Reporting. By default, the database names are ReportServer and ReportServerTempDB.	
(2) Data protection capabilities in is enhanced with a full disk encryption add-on from Sophos. The installation of results in a Safeguard database.	

After Completing This Task:
You must also backup the HEAT PatchLink DataCenter content directory.

Tip: The default location of the content directory is `<Installation Directory>\HEAT\EMSS\Content`. However, if this directory was modified during installation, you can verify its location by viewing the `\HKEY_LOCAL_MACHINE\SOFTWARE\Patchlink.com\Update\ISAPI\Storage` registry key.

Restoring a Database Backup

Another important part of an effective Disaster Recovery Solution is having a process defined in which to restore your database backup.

Prerequisites:

Prior to restoring the database backup you must install the HEAT PatchLink DataCenter for Microsoft System Center server using the same serial number that was used previously.

Important: After installing the HEAT PatchLink DataCenter for Microsoft System Center server do not open the user interface until after you have restored the databases.

1. Open the *Services Management Console*.

2. Right-click the `World Wide Web Publishing` service.

3. Select **Stop** to stop the `World Wide Web Publishing` (IIS) service.

4. Repeat steps 2 and 3 for the following services:

   - `EDS Server`
   - `EDS InstallerService`
   - `Replication Service`
   - `STATEngine`

5. Restore the backup you made of the content directory, over the new content directory (`<Installation Directory>\HEAT\EMSS\Content` by default). However, if this directory was modified during installation, you can verify its location by viewing the `\HKEY_LOCAL_MACHINE \SOFTWARE\Patchlink.com\Update\ISAPI\Storage` registry key.

6. Open the *Microsoft SQL Server Management Studio* (**Start** > **Programs** > **Microsoft SQL Server 2008** > **SQL Server Management Studio**).

7. Using an user account that has *sysadmin* rights, log into your database server.

8. In the directory tree, expand *Server Name\SQL Instance* > **Databases**.

9. Right-click on the **Databases** folder.

HEAT®software

10. Select **Restore Database**

> **Step Result:** The *Restore Database* window opens.
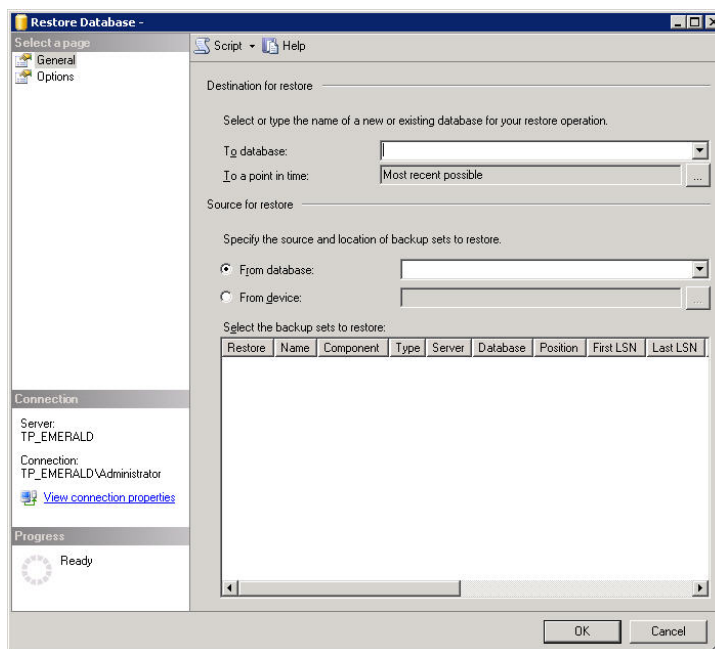
Figure 88: Restore Database

11. In the **To database** field, type or select the PLUS database.

12. Select **From device** and click the **Ellipses** button (...).

> **Step Result:** The *Specify Backup* dialog opens.

13. Click **Add**.

> **Step Result:** The *Locate Backup File* dialog opens.

14. Locate and select your backup (.bak) file.

15. Click **OK**.

16. Click **OK** to return to the *Restore Database* window.

17. Select the check-box associated with your backup within the **Select the backup sets to restore** table.

18. Click `Options` within the **Select a page** pane.

> **Step Result:** The *Options* page displays.
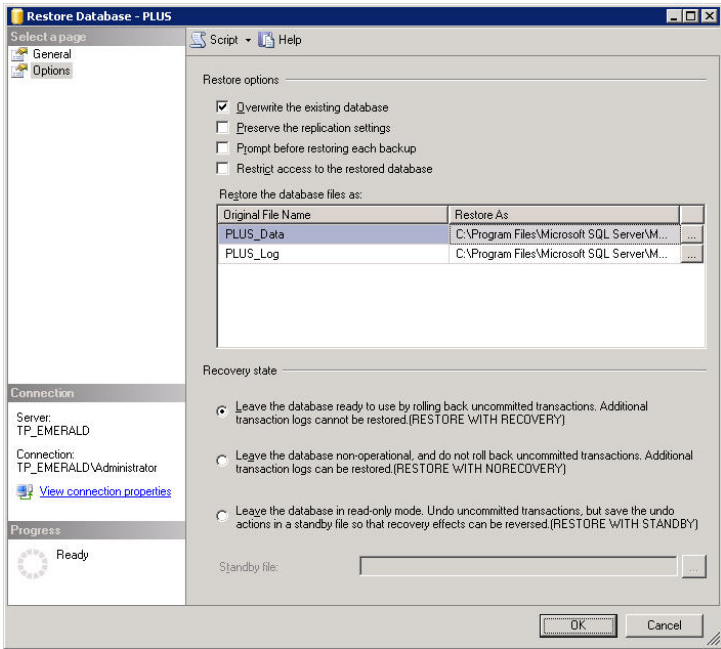
Figure 89: Restore Database - Options

19. Ensure the **Overwrite the existing database** option is selected.

20. Verify, and correct if necessary, the directory path within the **Restore the database files as** table.

21. Ensure the **Leave the database ready to use** option is selected.

22. Click **OK** to begin the database restoration.

23. After the restore is complete run the following SQL command against the database.

```
exec sp_changedbowner 'sa'
```

24. Repeat steps 9 through 23, restoring each of the following databases:

Table 199: Database Names

Database Name	Product
STAT_Guardian	HEAT PatchLink DataCenter for Microsoft System Center
UPCCommon	HEAT PatchLink DataCenter for Microsoft System Center
UPCExtended	HEAT PatchLink DataCenter for Microsoft System Center
PLUS_Reports	HEAT Enterprise Reporting Client

HEAT software

Database Name	Product
SCM	HEAT Security Configuration Management
ERS	HEAT Enterprise Reporting
ERS_Staging	HEAT Enterprise Reporting
ReportServer [1]	Microsoft SQL Server Reporting Services
ReportServerTempDB [1]	Microsoft SQL Server Reporting Services
SafeGuard [2]	powered by Sophos®
(1) Subscription features available in Microsoft SQL Server Reporting Services can be implemented in HEAT Enterprise Reporting. By default, the database names are ReportServer and ReportServerTempDB. (2) Data protection capabilities in is enhanced with a full disk encryption add-on from Sophos. The installation of results in a Safeguard database.	

25. Against the master database run the following SQL command.

```
exec sp_dboption N'STAT_Guardian', N'DB CHAINING', N'true'
exec sp_dboption N'UPCCommon', N'DB CHAINING', N'true'
exec sp_dboption N'UPCExtended', N'DB CHAINING', N'true'
exec sp_dboption N'PLUS', N'DB CHAINING', N'true'
exec sp_dboption N'PLUS_Reports', N'DB CHAINING', N'true'
exec sp_dboption N'SCM', N'DB CHAINING', N'true'
exec sp_dboption N'ERS', N'DB CHAINING', N'true'
exec sp_dboption N'ERS_Staging', N'DB CHAINING', N'true'
exec sp_dboption N'ReportServer', N'DB CHAINING', N'true'
exec sp_dboption N'ReportServerTempDB', N'DB CHAINING', N'true'
exec sp_dboption N'SafeGuard', N'DB CHAINING', N'true'
```

26. If you changed the computer name, Service account name, or Client account name, then you must perform the following steps.

a) Delete the previous Service account and Client account users from **each** database.

b) Add the new Service and Client account users to the following roles for each database.

- PLUS - EMSS Server and aspnet_ChangeNotification_ReceiveNotificationsOnlyAcccess
- PLUS_Reports - EMSS Server
- SCM - EMSS Server
- STAT_Guardian - Guardian_Admin
- UPCCommon - EMSS Server and aspnet_ChangeNotification_ReceiveNotificationsOnlyAcccess
- UPCExtended - EMSS Server and aspnet_ChangeNotification_ReceiveNotificationsOnlyAcccess
- ERS - EMSS Server
- ERS_Staging - EMSS Server

27. If you re-installed the HEAT PatchLink DataCenter server with a different user name than was used when originally installed, run the following SQL command.

```
UPDATE AccountContacts SET UserName = 'NewUserName' WHERE UserName = 'OldUserName'
```

28. If you re-installed the HEAT PatchLink DataCenter server with the content directory in a different location than the original installation, run the following SQL command.

```
UPDATE SystemConfig SET SystemConfig_Value = 'NewStorageSystemPath' WHERE SystemConfig_Name =
'Storage'
```

29. If you re-installed the HEAT PatchLink DataCenter server with a different installation directory than the original installation, run the following SQL command.

```
UPDATE SystemConfig SET SystemConfig_Value = 'NewWebInstallPath' WHERE SystemConfig_Name =
'InstallPath'
```

30. Restart the `World Wide Web Publishing Service`, `EDS LanPortal`, `EDS MessageBroker`, `EDS Server`, `Replication Service`, and `STATEngine` services.

31. Install the HEAT PatchLink DataCenter Agent from the ***Download Agent Installers*** page.

Creating an Automated Solution

A Maintenance Plan allows you to create an automated backup and schedule the backup to occur as frequently as your organizational needs dictate. Maintenance Plans allow you to define your back up options as well as which databases and transaction logs to include.

Note: If you have not already done so, you should change your Database Recovery Model to `FULL` before continuing. For additional information, refer to Changing the Database Recovery Model on page 453.

Creating a Maintenance Plan

You can automate a database maintenance plan for the SQL Server instances associated with HEAT PatchLink DataCenter for Microsoft System Center.

Prerequisites:

Prior to creating a Maintenance Plan you must upgrade your database server to ***Microsoft SQL Server 2008 Standard*** or ***Microsoft SQL Server 2008 Enterprise***, install SSIS (***SQL Server Integration Services***), and set the ***SQL Server Agent*** startup type to `Automatic`.

1. Open the ***Microsoft SQL Server Management Studio***.

2. Log into your database server.

3. In the directory tree, expand ***Server Name\SQL Instance*** > **Databases**.

4. Right-click on the **Maintenance Plans** folder.

HEAT®software

5. Select **Maintenance Plan Wizard**.

> **Step Result:** The *SQL Server Maintenance Plan Wizard* opens.
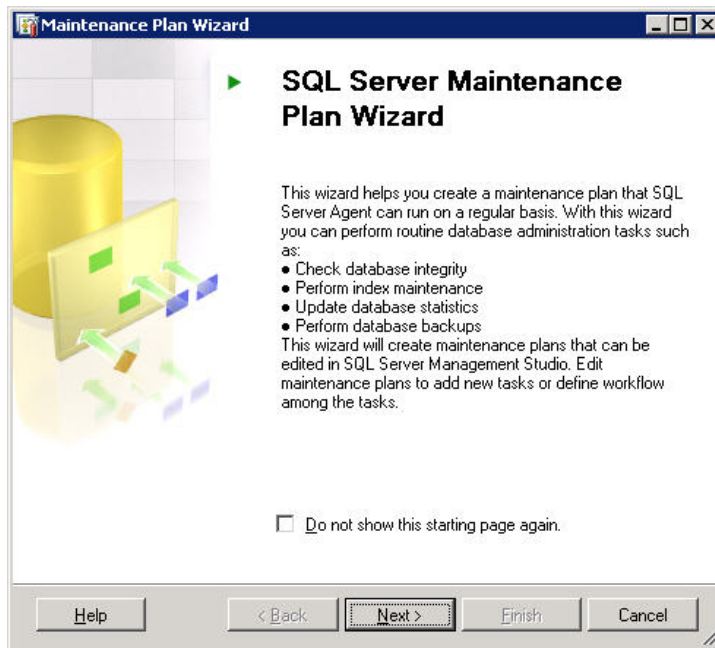
Figure 90: SQL Server Maintenance Plan Wizard

6. Click **Next**.

> **Step Result:** The *Select a Target Server* page opens.

7. Define the maintenance plan **Name**, **Description** [optional], target **Server**, and **Authentication** method.

8. Click **Next**.

> **Step Result:** The *Select Maintenance Tasks* page opens.

9. Select the following maintenance tasks:

- **Check Database Integrity**
- **Clean Up History** [optional]
- **Back Up Database (Full)**
- **Back Up Database (Transaction Log)**

10. Click **Next**.

> **Step Result:** The *Select Maintenance Task Order* page opens.

11. Set the tasks to execute in the following order:

- **Check Database Integrity**
- **Back Up Database (Full)**
- **Back Up Database (Transaction Log)**
- **Clean Up History** [optional]

12. Click **Next**.

Step Result: The *Define Database Check Integrity Task* page opens.

13. Click the **Database** drop-down.

a) Select the **These databases** option.

b) Select the `PLUS` database.

> **Tip:** You may choose all databases that require a database maintenance plan from the drop-down list.

c) Click **OK**.

14. Ensure that the **Include indexes** option is selected.

HEAT software

15. Click **Next**.

Step Result: The *Define Back Up Database (Full) Task* page opens.

Figure 91: Define Back Up Database (Full) Task

16. Click the **Database** drop-down.

a) Select the **These databases** option.

b) Select the PLUS database.

> **Tip:** You may choose all databases that require a database maintenance plan from the drop-down list.

c) Click **OK**.

17. Define your Back up **Destination** settings.

   a) Select either the **Disk** or **Tape** option.
   b) Select to **Create a backup file** for every database.
   c) Select to **Create a sub-directory** for each database.
   d) Define your destination **Folder**.

   > **Note:** For performance reasons, it is recommended that you create your database backup in a directory that is not on the same physical drive as your database.

   e) Ensure the **Backup file extension** is set as `.bak` for the database backup.
   f) Select **Verify backup integrity**.

18. Click **Next**.

   Step Result: The *Define Back Up Database (Transaction Log) Task* page opens.

19. Click the **Database** drop-down.

   a) Select the **These databases** option.
   b) Select the `PLUS` database.

   > **Tip:** You may choose all databases that require a database maintenance plan from the drop-down list.

   c) Click **OK**.

20. Define your Back up **Destination** settings.

   a) Select either the **Disk** or **Tape** option.
   b) Select to **Create a backup file** for every database.
   c) Select to **Create a sub-directory** for each database.
   d) Define your destination **Folder**.

   > **Note:** For performance reasons, it is recommended that you create your database backup in a directory that is not on the same physical drive as your database.

   e) Ensure the **Backup file extension** is set as `.trn` for the transaction backup file.
   f) Select **Verify backup integrity**.

HEAT software

21. Click **Next**.

> **Step Result:** If the **Clean Up History** option was selected, the *Define Cleanup History Task* page opens. Otherwise the *Select Plan Properties* page will open.
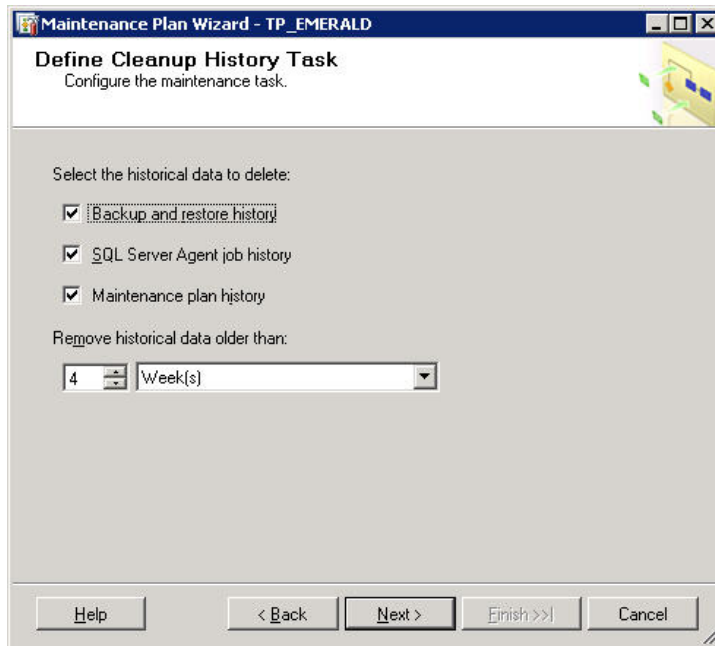
Figure 92: Define Cleanup History Task

22. If the **Clean Up History** option was selected, define the *Cleanup History Task* options.

    a) Ensure that **Backup and restore history** is selected.
    b) Ensure that **SQL Server Agent job history** is selected.
    c) Ensure that **Maintenance plan history** is selected.
    d) Define the **Remove historical data older than** setting as appropriate for your organization.
    e) Click **Next**.

> **Step Result:** The *Select Plan Properties* page will open.

23. [Optional] Click **Change** to open the *New Job Schedule* page and define the maintenance plan schedule.

Figure 93: New Job Schedule

a) Enter a **Name** for the schedule.
b) Select a **Schedule** type.
c) Ensure that **Enabled** is selected.
d) Define the **Occurrence** frequency (**Daily**, **Weekly**, or **Monthly**) and options.
e) Define the **Daily frequency**.
f) Define the **Duration**.
g) Click **OK**.

> **Step Result:** The changes are saved and the *New Job Schedule* page closes.

24. Click **Next**.

> **Step Result:** The *Select Report Options* page opens.

25. Set your desired reporting options.

26. Click **Next**.

> **Step Result:** The *Complete the Wizard* page opens.

27. Click **Finish** to complete the wizard.

HEAT®software

28. Repeat steps 13 through 27 for the following databases:

Table 200: Database Names

Database Name	Product
STAT_Guardian	HEAT PatchLink DataCenter for Microsoft System Center
UPCCommon	HEAT PatchLink DataCenter for Microsoft System Center
UPCExtended	HEAT PatchLink DataCenter for Microsoft System Center
PLUS_Reports	HEAT Enterprise Reporting Client
SCM	HEAT Security Configuration Management
ERS	HEAT Enterprise Reporting
ERS_Staging	HEAT Enterprise Reporting
ReportServer [1]	Microsoft SQL Server Reporting Services
ReportServerTempDB [1]	Microsoft SQL Server Reporting Services
SafeGuard [2]	powered by Sophos®
(1) Subscription features available in Microsoft SQL Server Reporting Services can be implemented in HEAT Enterprise Reporting. By default, the database names are ReportServer and ReportServerTempDB.	
(2) Data protection capabilities in is enhanced with a full disk encryption add-on from Sophos. The installation of results in a Safeguard database.	

After Completing This Task:
You must now establish a backup procedure which will archive all of your backup files and the contents of the UpdateStorage directory on a regular basis. This can be done through the use of any file backup utility.