Casper Site Administrator’s Guide

Version 1.0
Accessing JSS
Test Environment

All site admin will be provided 'full access' (with some restrictions) to a test environment. Test environment can be accessed at the following link:

https://casper1-test.mit.edu:8443

Production Environment

Site Admins will be provided full access to their site, where site name is based on department name. Based on JAMF's implementation of sites, some restrictions apply and will be discussed later in the document. Production Environment can be access at the following link:

https://casper1.mit.edu:8443
The JSS Dashboard

The JSS Dashboard allows you to monitor the status of commonly viewed items in the JAMF Software Server (JSS), such as smart groups, policies, configuration profiles, and licensed software—all in one central location.

You can access the JSS Dashboard while using the JSS by clicking the JSS Dashboard button in the top-left corner of the page.

Note: Until you add one or more items to the JSS Dashboard, it displays setup tips that you can use to configure commonly used settings.
Adding Items to the JSS Dashboard

You can add the following types of items to the JSS Dashboard:
- Smart computer groups
- Smart mobile device groups
- Policies
- OS X configuration profiles
- iOS configuration profiles
- Licensed software

To add an item to the JSS Dashboard, select the **Show in JSS Dashboard** checkbox in the upper-right corner of the pane when viewing the item in the JSS.
Managing Computers
Inventory

Computer Inventory Collection Settings

By default, inventory is collected from computers using the “Update Inventory” policy that is created automatically when you install the JAMF Software Server (JSS). This policy collects inventory from all computers once every day.

Computers can submit many types of inventory information to the JAMF Software Server (JSS). Basic inventory information—such as hardware, operating system, user and location information, storage, and applications—is collected automatically.

The Computer Inventory Collection settings in the JSS also collect the following items:

- Local user accounts and home directory sizes
- Printers
- Active services
- User and location from an LDAP directory service
- Package receipts
- Available software updates

Time and Traffic Estimates for Collecting Additional Items

Collecting additional inventory items may add reporting time and network traffic to the inventory process.

The following table provides estimates of how much time and traffic may be added when collecting user home directory sizes, available software updates, fonts, and plug-ins. These estimates are based on a MacBook Pro with approximately 300 GB of user home directories, 100 applications, 300 fonts, and 900 plug-ins.

<table>
<thead>
<tr>
<th>Additional Inventory Item</th>
<th>Time (Seconds)</th>
<th>Traffic (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(No additional items)</td>
<td>9</td>
<td>102</td>
</tr>
<tr>
<td>Home directory sizes</td>
<td>25</td>
<td>104</td>
</tr>
<tr>
<td>Available software updates</td>
<td>110</td>
<td>104</td>
</tr>
<tr>
<td>Fonts</td>
<td>10</td>
<td>128</td>
</tr>
<tr>
<td>Plug-ins</td>
<td>13</td>
<td>248</td>
</tr>
</tbody>
</table>
The following table provides estimates of how much time and traffic may be added when collecting Application Usage information. These estimates are based on a MacBook Pro with eight applications used per day, one week between inventory reports, and one computer user.

<table>
<thead>
<tr>
<th>Additional Inventory Item</th>
<th>Time (Seconds)</th>
<th>Traffic (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(No additional items)</td>
<td>16</td>
<td>24</td>
</tr>
<tr>
<td>Application Usage information</td>
<td>17</td>
<td>48</td>
</tr>
</tbody>
</table>

### Search Paths for Collecting Applications, Fonts, and Plug-ins

The following table lists the default search paths that are used when collecting applications, fonts, and plug-ins from computers on the Mac and Windows platforms.

<table>
<thead>
<tr>
<th>Collected Item</th>
<th>Mac Platform Default Search Paths</th>
<th>Windows Platform Default Search Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications (and Application Usage information, if collecting)</td>
<td><code>/Applications/</code></td>
<td><code>C:\Program Files\</code></td>
</tr>
<tr>
<td>Fonts</td>
<td><code>/Library/Fonts/</code></td>
<td><code>C:\Windows\Fonts\</code></td>
</tr>
<tr>
<td></td>
<td><code>/System/Library/Fonts/</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>/Library/Application Support/Adobe/Fonts/</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>~/Library/Fonts/</code> (collected at the user level for each account)</td>
<td></td>
</tr>
<tr>
<td>Plug-ins</td>
<td><code>/Library/Internet Plug-Ins/</code></td>
<td><code>--</code></td>
</tr>
</tbody>
</table>

If you store these items in locations not listed in the table, you can use the Computer Inventory Collection settings to specify custom search paths for those locations.
Computer Inventory Display Settings

The Computer Inventory Display settings allow each JSS user to choose which attribute fields to display in the results of a simple computer search.

Configuring the Computer Inventory Display Settings

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click Settings ☰.
3. Click Computer Management.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. In the “Computer Management–Management Framework” section, click Inventory Display 🖥.
5. On each pane, select or deselect the checkbox for each attribute field you want to display or remove.
6. Click Save.
## Simple Computer Searches

A simple computer search functions like a search engine, allowing you to quickly search the items in your inventory for a general range of results.

The following table shows the items that you can search by and the attributes on which you can base each search:

<table>
<thead>
<tr>
<th>Inventory Item</th>
<th>Searchable Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computers</td>
<td>Computer name, MAC address, Bar code, IP address, Asset tag, Serial number, Username, Full name, Email address, Phone number, Position, Department, Building, Room</td>
</tr>
<tr>
<td>(This includes both managed and unmanaged computers.)</td>
<td></td>
</tr>
<tr>
<td>Peripherals</td>
<td>Peripheral type, Customizable peripheral fields, Bar code</td>
</tr>
<tr>
<td>Applications</td>
<td>Application name</td>
</tr>
<tr>
<td>Local User Accounts</td>
<td>Username</td>
</tr>
<tr>
<td>Application Usage</td>
<td>Application name</td>
</tr>
<tr>
<td>Fonts</td>
<td>Font name</td>
</tr>
<tr>
<td>Package Receipts</td>
<td>Package receipt name</td>
</tr>
<tr>
<td>Plug-ins</td>
<td>Plug-in name</td>
</tr>
<tr>
<td>Printers</td>
<td>Printer name</td>
</tr>
<tr>
<td>Services</td>
<td>Service name</td>
</tr>
<tr>
<td>Software Updates</td>
<td>Software update name, Software update version</td>
</tr>
</tbody>
</table>

**Note:** Computers, peripherals, and applications are searchable by default. The other items are searchable if the JSS is configured to collect them as inventory.
Search Syntax

This section explains the syntax to use for the following search functions:

- Wildcard searches
- Including multiple search terms
- Excluding a search term
- Returning all results

In general, searches are not case-sensitive.

*Note:* The default search preference is “Exact Match”. For most items, the option can be changed to either “Starts with” or “Contains”.

**Wildcard Searches**

Asterisks (*) function as wildcard characters in simple searches. The following table explains the different ways asterisks can be used to refine a search:

<table>
<thead>
<tr>
<th>Usage</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use an asterisk after a search term to return all results with attributes that begin with that term.</td>
<td>Perform an application search for “Adobe*” to return all applications that begin with “Adobe”.</td>
</tr>
<tr>
<td>Use an asterisk before a search term to return all results with attributes that end with that term.</td>
<td>Perform a computer search for “*@mycompany.com” to return all computers with email addresses that end with “@mycompany.com”.</td>
</tr>
<tr>
<td>Use an asterisk before and after a search term to return all results that include that term.</td>
<td>Perform an application search for “<em>Word</em>” to return all applications that include “Word”.</td>
</tr>
<tr>
<td>Use an asterisk without any other terms to return all results for the item you are searching.</td>
<td>Perform a peripheral search for “*” to return all peripherals.</td>
</tr>
</tbody>
</table>

**Including Multiple Search Terms**

Use multiple search terms separated by a comma (,) to return all results that include those search terms.

For example, perform an application search for “Adobe*, *.app” to return all applications that begin with “Adobe” and end with “.app”.

**Excluding a Search Term**

Use a hyphen (-) before a search term to exclude results that include the term.

For example, perform a printer search for “abc*, -*West” to return all printers that begin with “abc” except for those that end with “West”.

**Returning All Results**

There are two ways to return all results: use an asterisk (*) without any other characters or terms, or perform a blank search.
Performing a Simple Computer Search

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Choose an item from the **Search** pop-up menu.
5. Enter one or more search terms in the field(s) provided.
6. Press the Enter key.

The list of search results is displayed.

If you searched for an item other than computers or peripherals, you can view the computers associated with a result by clicking **Expand** next to the result. You can also change the item on which the results are based by choosing an item from the pop-up menu at the top of the page.
Advanced Computer Searches

Advanced computer searches allow you to use detailed search criteria to search the managed and unmanaged computers in the JAMF Software Server (JSS). These types of searches give you more control over your search by allowing you to do the following:

- Generate specific search results.
- Specify which attribute fields to display in the search results.
- Save the search.

Creating an Advanced Computer Search

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**. On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **New**.
5. Use the Search pane to configure basic settings for the search. To save the search, select the **Save this Search** checkbox.
6. Click the **Criteria** tab and add criteria for the search:
   a. Click **Add**.
   b. Click **Choose** for the criteria you want to add. To display additional criteria, click **Choose** for "Other Criteria".
   c. Choose an operator from the **Operator** pop-up menu.
   d. Enter a value in the **Value** field or browse for a value by clicking **Browse**.
   e. Repeat steps a through d to add criteria as needed.
7. Choose an operator from the **And/Or** pop-up menu(s) to specify the relationships between criteria.
8. To group criteria and join multiple operations, choose parentheses from the pop-up menus around the criteria you want to group.
9. Click the Display tab and select the attribute fields you want to display in your search results.

10. Click Save.

Operations in the search take place in the order they are listed (top to bottom).

The results of a saved search are updated each time computers check in with the JSS and meet or fail to meet the specified search criteria.

To view the search results, click View.

**Cloning, Editing, or Deleting a Saved Advanced Computer Search**

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Search Inventory.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the advanced computer search you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the search, click Clone and make changes as needed. Then click Save.
   - To edit the search, click Edit and make changes as needed. Then click Save.
   - To delete the search, click Delete. Then click Delete again to confirm.

**Viewing Advanced Computer Search Results**

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Search Inventory.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the advanced computer search you want to view the results for.
5. Click View.

The list of search results is displayed.
Computer Reports

The data displayed in smart or static group membership lists, computer search results, or lists of license usage matches can be exported from the JAMF Software Server (JSS) to the following file formats:

- Comma-separated values file (.csv)
- Tab delimited text file (.txt)
- XML file

You can change the way the data is organized by basing the export on any of the following inventory items:

- Computers
- Applications
- Fonts
- Plug-ins
- Packages installed by the Casper Suite
- Packages installed by Installer.app/Software Update
- Cached packages
- Local user accounts
- Mapped printers
- Available software updates
- Running services
- Computer groups
- Licensed software

The data is displayed in alphanumeric order by the selected inventory item.

Creating Computer Reports

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Do one of the following:
   - View computer group memberships.
   - View simple or advanced computer search results.
   - View license usage matches.
4. At the bottom of the list, click Export.
5. Follow the onscreen instructions to export the data.

The report downloads immediately.
Performing Mass Actions for Computers

Mass actions allow you to perform potentially tedious tasks for multiple computers at the same time. You can use the JSS to perform the following mass actions:

- Edit the building or department.

Mass actions can be performed on smart or static group membership lists, computer search results, or lists of license usage matches.

Mass Editing the Building or Department for Computers

Mass editing the building or department for computers allows you to add the computers to a building or department or change the building or department they belong to.

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Do one of the following:
   - View computer group memberships.
   - View simple or advanced computer search results.

   **Note:** You can only perform mass actions from a simple computer search if you searched by computers.
   - View license usage matches.
4. At the bottom of the list, click Action.
5. Select Edit the Building and Department.
   This option is only displayed if there are one or more buildings or departments in the JSS.
6. Follow the onscreen instructions to edit the building or department.
# Viewing and Editing Inventory Information for a Computer

The JAMF Software Server (JSS) stores detailed inventory information for each computer. You can view and edit this information from the JSS.

The following table lists the information that you can view and edit for each computer.

**Note:** Extension attributes are displayed in computer inventory information in the category in which they are configured to display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Editable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Category</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Name</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Site</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Last Inventory Update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Check-in</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Reported IP Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>jamf binary Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Managed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enrollment Method</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Enrollment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDM Capability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JSS Computer ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Tag</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Bar Code 1</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Bar Code 2</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Bluetooth Low Energy Capability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logged in to iTunes Store</td>
<td></td>
<td>This value will be reported as “Active” when a user-level configuration profile is installed from Self Service using MDM-enabled credentials</td>
</tr>
<tr>
<td>Management Account Username</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Management Account Password</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Editable</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td><strong>Hardware Category</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Make</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Model</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Model Identifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDID</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Serial Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Processor Speed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Processors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Processor Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Architecture Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bus Speed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cache Size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary MAC Address</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Secondary MAC Address</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Total RAM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Available RAM Slots</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Battery Capacity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMC Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIC Speed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optical Drive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boot ROM</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Operating System Category</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating System Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating System Build</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master Password Set</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FileVault Users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Pack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Editable</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td><strong>User and Location Category</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>✔️</td>
<td>Assign a user to the computer and populate user information from the Users tab.</td>
</tr>
<tr>
<td>Full Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Position</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Department</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Building</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Room</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Purchasing Category</strong></td>
<td>✔️</td>
<td>Look up and populate purchasing information from Apple’s Global Service Exchange (GSX).</td>
</tr>
<tr>
<td>Purchased or Leased</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warranty Expiration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppleCare ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lease Expiration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchase Price</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Life Expectancy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchasing Account</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchasing Contact</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Extension Attributes Category</strong></td>
<td>✔️</td>
<td>Non-script extension attributes only Displays a list of custom data fields collected using extension attributes</td>
</tr>
<tr>
<td><strong>Storage Category</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Model</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revision</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drive Capacity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.M.A.R.T. Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Partitions</td>
<td></td>
<td>Displays the name of the partition</td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td>Displays the size of the partition</td>
</tr>
<tr>
<td>Size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Editable</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Storage Category (continued)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% Used</td>
<td></td>
<td>Displays the % used of the partition</td>
</tr>
<tr>
<td>FileVault 2 State</td>
<td></td>
<td>Displays the FileVault 2 State of the partition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This value will be reported as “Unknown” when:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inventory has not been updated since the last JSS upgrade</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The JSS is unable to detect encryption status due to an error</td>
</tr>
<tr>
<td>Core Storage Partition Scheme</td>
<td></td>
<td>Displays the core storage partition scheme of the partition</td>
</tr>
<tr>
<td><strong>Disk Encryption Category</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Inventory Update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FileVault 2 Partition Encryption State</td>
<td></td>
<td>This value will be reported as “Unknown” when:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inventory has not been updated since the last JSS upgrade</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The JSS is unable to detect encryption status due to an error</td>
</tr>
<tr>
<td>Individual Recovery Key Validation</td>
<td></td>
<td>Displays whether the individual recovery key on a computer matches the individual recovery key stored for that computer in the JSS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This value will be reported as “Unknown” when:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• OS X version is 10.8 or earlier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No recovery key in the JSS to validate against</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inventory has not been updated since the last JSS upgrade</td>
</tr>
<tr>
<td>Field</td>
<td>Editable</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Disk Encryption Category (continued)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Institutional Recovery Key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Encryption Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FileVault 2 Enabled Users</td>
<td></td>
<td>Displays the usernames of FileVault 2-enabled users on the computer</td>
</tr>
<tr>
<td><strong>Peripherals Category</strong></td>
<td></td>
<td>Displays a list of peripherals associated with the computer</td>
</tr>
<tr>
<td><strong>Licensed Software Category</strong></td>
<td></td>
<td>Displays a list of licensed software titles installed on the computer</td>
</tr>
<tr>
<td><strong>Applications Category</strong></td>
<td></td>
<td>Displays a list of applications installed on the computer</td>
</tr>
<tr>
<td><strong>Fonts Category</strong></td>
<td></td>
<td>Displays a list of fonts installed on the computer</td>
</tr>
<tr>
<td><strong>Plug-ins Category</strong></td>
<td></td>
<td>Displays a list of plug-ins installed on the computer</td>
</tr>
<tr>
<td><strong>Profiles Category</strong></td>
<td></td>
<td>Displays a list of profiles installed on the computer</td>
</tr>
<tr>
<td><strong>Certificates Category</strong></td>
<td></td>
<td>Displays a list of certificates installed on the computer</td>
</tr>
<tr>
<td><strong>Package Receipts Category</strong></td>
<td></td>
<td>Displays a list of packages installed by Installer.app or Software Update, and a list of packages installed or cached by the Casper Suite</td>
</tr>
<tr>
<td>Field</td>
<td>Editable</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Software Updates Category</td>
<td></td>
<td>Displays a list of software updates available for the computer</td>
</tr>
<tr>
<td>Local User Accounts Category</td>
<td></td>
<td>Displays a list of local user accounts and information about them</td>
</tr>
<tr>
<td>Printers Category</td>
<td></td>
<td>Displays a list of printers mapped to the computer and information about those printers</td>
</tr>
<tr>
<td>Services Category</td>
<td></td>
<td>Displays a list of active services</td>
</tr>
<tr>
<td>Attachments Category</td>
<td></td>
<td>Displays a list of files attached to the inventory record</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Upload and delete attachments</td>
</tr>
</tbody>
</table>

**Viewing Inventory Information for a Computer**

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer you want to view information for.
   - If you performed a simple search for an item other than computers, you must click **Expand** next to an item to view the computers related to that item.
   - The computer's inventory information is displayed.
5. Use the categories to view information for the computer.
# Editing Inventory Information for a Computer

1. Log in to the JSS with a web browser.

2. Click **Computers** at the top of the page.

3. Perform a simple or advanced computer search.

4. Click the computer you want to edit information for.
   - If you performed a simple search for an item other than computers, you must click **Expand** next to an item name to view the computers related to that item.
   - The computer’s inventory information is displayed.

5. Select the category that contains the information you want to edit and click **Edit**.

6. Make changes as needed.
   - If you are editing purchasing information, you can click **Search** to look up and populate information from Apple’s Global Service Exchange (GSX).
   - If you are editing user and location information, the changes are applied in the **Users** tab. This specified information is also applied in the inventory information for mobile devices, peripherals, and other computers that the user is assigned to.

7. Click **Save**.
Viewing Management Information for a Computer

The JAMF Software Server (JSS) allows you to view the following management information for each computer:

- Pending management commands
- Policies
- eBooks
- Mac App Store apps
- OS X configuration profiles
- Managed Preferences
- Restricted software
- FileVault 2 recovery key(s)
- Group memberships

Requirements

To view pending management commands for a computer, the computer and the JSS must meet the requirements for sending an OS X remote command or installing an OS X configuration profile.

Viewing the Pending Management Commands for a Computer

When viewing management information for a computer, you can view a list of pending management commands for the computer. The list includes all pending actions related to sending an OS X remote command and installing or removing an OS X configuration profile.

You can also cancel a pending management command.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer you want to view pending management commands for.
   If you performed a simple search for an item other than computers, you must click **Expand** next to an item to view the computers related to that item.
5. Click the Management tab.  
A list of pending management commands for the computer is displayed.  
**Note:** You cannot view pending management commands if the MDM profile has been removed from the computer.

6. To cancel a pending management command, click Cancel for the command.

**Viewing Policies for a Computer**

When viewing management information for a computer, you can view a list of policies that have the computer in the scope. You can also view a list of policies for a specific user on that computer.

1. Log in to the JSS with a web browser.

2. Click Computers at the top of the page.

3. Perform a simple or advanced computer search.

4. Click the computer you want to view policies for.  
   If you performed a simple search for an item other than computers, you must click Expand next to an item to view the computers related to that item.

5. Click the Management tab, and then click the Policies category.  
   A list of policies for the computer is displayed.

6. To view policies for a specific user, enter the username in the Username field and click Update.  
   A list of policies for the user is displayed.
Viewing Mac App Store Apps for a Computer

When viewing management information for a computer, you can view a list of Mac App Store apps that have the computer in the scope. You can also view a list of Mac App Store apps for a specific user on that computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer you want to view apps for.
   If you performed a simple search for an item other than computers, you must click **Expand** next to an item to view the computers related to that item.
5. Click the **Management** tab, and then click the **Mac App Store Apps** category.
   A list of apps for the computer is displayed.
6. To view apps for a specific user, enter the username in the **Username** field and click **Update**.
   A list of apps for the user is displayed.

Viewing Configuration Profiles for a Computer

When viewing management information for a computer, you can view a list of OS X configuration profiles that have the computer in the scope. You can also view a list of configuration profiles for a specific user on that computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer you want to view configuration profiles for.
   If you performed a simple search for an item other than computers, you must click **Expand** next to an item to view the computers related to that item.
5. Click the **Management** tab, and then click the **Configuration Profiles** category.
   A list of configuration profiles for the computer is displayed.
6. To view configuration profiles for a specific user, enter the username in the **Username** field and click **Update**.
   A list of configuration profiles for the user is displayed.
**Viewing Managed Preferences for a Computer**

When viewing management information for a computer, you can view a list of Managed Preference profiles that have the computer in the scope. You can also view a list of profiles for a specific user on that computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer you want to view Managed Preferences for.
   If you performed a simple search for an item other than computers, you must click **Expand** next to an item to view the computers related to that item.
5. Click the **Management** tab, and then click the **Managed Preferences** category.
   A list of Managed Preference profiles for the computer is displayed.
6. To view a list of Managed Preference profiles for a specific user, enter the username in the **Username** field and click **Update**.
   A list of Managed Preference profiles for the user is displayed.

**Viewing Restricted Software for a Computer**

When viewing management information for a computer, you can view a list of restricted software that has the computer in the scope. You can also view a list of restricted software for a specific user on that computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer you want to view restricted software for.
   If you performed a simple search for an item other than computers, you must click **Expand** next to an item to view the computers related to that item.
5. Click the **Management** tab, and then click the **Restricted Software** category.
   A list of restricted software for the computer is displayed.
6. To view restricted software for a specific user, enter the username in the **Username** field and click **Update**.
   A list of restricted software for the user is displayed.
Viewing the FileVault 2 Recovery Key for a Computer

When viewing management information for a computer, you can view the FileVault 2 recovery key for the computer if FileVault 2 disk encryption has been activated using the Casper Suite.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer you want to view the FileVault 2 recovery key for.
   If you performed a simple search for an item other than computers, you must click **Expand** next to an item to view the computers related to that item.
5. Click the **Management** tab, and then click the **FileVault 2** category.
6. Click **Get FileVault 2 Recovery Key**.
   - If the key is an institutional recovery key, a **Download** link is displayed. Click the link to download the recovery key.
   - If the key is an individual recovery key, the recovery key is displayed on the pane.

Viewing Group Memberships for a Computer

When viewing management information for a computer, you can view the smart and static group memberships for the computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer you want to view group memberships for.
   If you performed a simple search for an item other than computers, you must click **Expand** next to an item to view the computers related to that item.
5. Click the **Management** tab, and then click the **Computer Groups** category.
   A list of smart computer group memberships is displayed.
6. To view the static computer group memberships, click **Static Groups**.
   A list of static computer group memberships is displayed.
Viewing the History for a Computer

The JAMF Software Server (JSS) allows you to view the history for each computer. The information you can view includes:

- Policy logs
- Management history (completed, pending, and failed management commands)
- Hardware/software history
- User and location history
- Completed, pending, and failed Mac App Store app installations

You can also flush policy logs for a computer.

Viewing and Flushing Policy Logs for a Computer

The policy logs for a computer include a list of the policies that have run on the computer and the following information for each policy:

- The date/time that the policy ran on the computer
- The status of the policy
- The actions logged for the policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer you want to view policy logs for.
   - If you performed a simple search for an item other than computers, you must click Expand next to an item to view the computers related to that item.
5. Click the **History** tab, and then click the **Policy Logs** category.
   - Policy logs for the computer are displayed.
6. To view the actions logged for a policy, click **Show** for the policy.
   - To hide the information when you are done viewing it, click **Hide**.
7. To flush a policy log, click **Flush** for the policy.
8. To flush all policies for the computer, click **Flush All** at the top of the pane.
Viewing Management History for a Computer

The management history for a computer allows you to view lists of completed, pending, and failed management commands for the computer. The lists include all actions related to sending an OS X remote command and installing or removing an OS X configuration profile.

You can also cancel a pending management command.

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer you want to view group memberships for.
   If you performed a simple search for an item other than computers, you must click Expand next to an item to view the computers related to that item.
5. Click the History tab, and then click the Management History category.
   A list of completed management commands for the computer is displayed.
6. To view pending management commands, click Pending Commands.
   You can cancel a pending management command by clicking Cancel for the command.
7. To view failed management commands, click Failed Commands.

Viewing Hardware/Software History for a Computer

The hardware/software history for a computer allows you to view a list of inventory reports submitted for the computer during a specified date range. Each inventory report includes hardware information for the computer, such as the operating system, make, model, and serial number, and information about any software changes that occurred since the previous inventory report.

Inventory report listings that show a change in a computer's hardware are displayed in red.

Note: You can only view software history for a computer if the Computer Inventory Collection settings are configured to collect applications, fonts, or plug-ins. Fonts and plug-ins collection is turned off.

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Perform a simple or advanced computer search.

4. Click the computer you want to view hardware/software history for.
   If you performed a simple search for an item other than computers, you must click Expand next to an item to view the computers related to that item.

5. Click the History tab, and then click the Hardware/Software History category.
   The hardware/software history for the computer is displayed.

6. To view hardware/software history for a different date range, specify the starting and ending dates using the Date Range pop-up menus on the pane. Then click Update.

---

**Viewing User and Location History for a Computer**

The user and location history for a computer allows you to view a list of the user and location information associated with the computer over time. A record of the current information is added to the list whenever changes are made to the User and Location category in the computer's inventory information.

1. Log in to the JSS with a web browser.

2. Click Computers at the top of the page.

3. Perform a simple or advanced computer search.

4. Click the computer you want to view user and location history for.
   If you performed a simple search for an item other than computers, you must click Expand next to an item to view the computers related to that item.

5. Click the History tab, and then click the User and Location History category.
   The user and location history for the computer is displayed.
Viewing Mac App Store App Installations for a Computer

You can view the completed, pending, and failed Mac App Store app installations for a computer. You can also cancel pending Mac App Store app installations.

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer you want to view app installation information for. If you performed a simple search for an item other than computers, you must click Expand next to an item to view the computers related to that item.
5. Click the History tab, and then click the Mac App Store Apps category. A list of apps installed on the computer is displayed.
6. To view a list of apps that are pending installation, click Pending Apps. You can cancel a pending installation by clicking Cancel for the app.
7. To view a list of apps that failed to install, click Failed Apps.
Deleting a Computer from the JSS

You can remove a computer from your inventory by deleting it from the JAMF Software Server (JSS).

The files and folders installed during enrollment are not removed from the computer when it is deleted from the JSS. For instructions on how to remove these components, see the Removing JAMF Software Components from Computers Knowledge Base article.

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Search Inventory.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Perform a simple or advanced computer search.
5. Click the computer you want to delete.
   If you performed a simple search for an item other than computers, such as computer applications, you must click Expand next to an item name to view the computers related to that item.
6. Click Delete, and then click Delete again to confirm.
Computer Groups

About Computer Groups

Computer groups allow you to organize computers that share similar attributes. You can use these groups as a basis for performing advanced inventory searches, configuring the scope of remote management tasks, and viewing Application Usage logs.

There are two kinds of computer groups: smart computer groups and static computer groups. Smart computer groups are based on criteria and have dynamic memberships. Static computer groups have fixed memberships that you manually assign.
Smart Computer Groups

Smart computer groups give you a way to organize managed computers based on one or more attributes, such as building, model, and operating system. These groups have dynamic memberships that are updated each time computers check in with the JAMF Software Server (JSS).

Creating a Smart Computer Group

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **New**.
5. Use the Computer Group pane to configure basic settings for the group.
   To enable email notifications, select the **Send email notification on membership change** checkbox.
6. Click the **Criteria** tab and add criteria to the group:
   a. Click **Add**.
   b. Click **Choose** for the criteria you want to add.
      To display additional criteria, click **Choose** for "Other Criteria".
   c. Choose an operator from the **Operator** pop-up menu.
   d. Enter a value in the **Value** field or browse for a value by clicking **Browse**.
   e. Repeat steps a through d to add criteria as needed.
7. Choose an operator from the **And/Or** pop-up menu(s) to specify the relationships between criteria.
8. To group criteria and join multiple operations, choose parentheses from the pop-up menus around the criteria you want to group.
9. Click **Save**.

Operations in the group take place in the order they are listed (top to bottom).

Group memberships are updated each time computers check in with the JSS and meet or fail to meet the specified criteria.

To view the group memberships, click **View**.
Cloning, Editing, or Deleting a Smart Computer Group

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Smart Computer Groups.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the smart computer group you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the group, click Clone and make changes as needed. Then click Save.
   - To edit the group, click Edit and make changes as needed. Then click Save.
   - To delete the group, click Delete. Then click Delete again to confirm.

The clone, edit, or delete action is applied to computers the next time they check in with the JSS.

Viewing Smart Computer Group Memberships

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Smart Computer Groups.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the smart computer group you want to view memberships for.
5. Click View.

A list of group memberships is displayed.
Static Computer Groups

Static computer groups give you a way to organize computers by assigning them to a group. These groups have fixed memberships that must be changed manually.

After creating a static computer group, you can view its memberships.

Creating a Static Computer Group

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Static Computer Groups**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **New**.
5. Use the Computer Group pane to configure basic settings for the group.
6. Click the **Assignments** tab and select the checkbox for each computer you want to add.
7. Click **Save**.

Computers become members of the group the next time they check in with the JSS.

To view the group memberships, click **View**.

Cloning, Editing, or Deleting a Static Computer Group

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Static Computer Groups**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the group you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the group, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the group, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the group, click **Delete**. Then click **Delete** again to confirm.

The clone, edit, or delete action is applied to computers the next time they check in with the JSS.
Viewing Static Computer Group Memberships

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Static Computer Groups**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the computer group you want to view memberships for.
5. Click **View**.
   
   A list of group memberships is displayed.
About Policies

Policies allow you to remotely perform common management tasks on managed computers. For example, you can run scripts, manage accounts, and distribute software using a policy.

Policies allow you to automate tasks so that they run on a schedule. When you create a policy, you specify the tasks you want to automate, when the policy should run (called “trigger”), how often it should run (called “execution frequency”), and the users and computers for which it should run (called “scope”).

You can also make policies available in Self Service for users to run on their computers.
Managing Policies

When you create a policy, you use a payload-based interface to configure settings for the policy and add tasks to it.

After you create a policy, you can view the plan, status, and logs for the policy. You can also flush policy logs.

Creating a Policy

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Policies.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New.
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
6. Use the rest of the payloads to configure the tasks you want to perform.
7. Click the Scope tab and configure the scope of the policy.
8. (Optional) Click the Self Service tab and make the policy available in Self Service.
9. (Optional) Click the User Interaction tab and enter messages to display to users or allow users to defer the policy.
10. Click Save.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.
**Cloning, Editing, or Deleting a Policy**

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the policy you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the policy, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the policy, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the policy, click **Delete** and then click **Delete** again to confirm.

The clone, edit, or delete action is applied to computers in the scope the next time they check in with the JSS.

**Viewing the Plan for a Policy**

The plan for a policy includes the following information:

- An indicator light that shows whether the policy is enabled
- The execution frequency for the policy
- The trigger(s) for the policy
- The scope of the policy
- The site that the policy belongs to
- A list of actions for the policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
   A list of policies and their plans are displayed.
4. To view the actions for a policy, click **Expand** for the policy.
**Viewing the Status of a Policy**

For each policy, you can view a pie chart that shows the number of computers for which the policy has completed, failed, and is still remaining.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **Grid View** at the top of the list.

**Viewing and Flushing Logs for a Policy**

The logs for a policy include a list of computers that have run the policy and the following information for each computer:
- The date/time that the policy ran on the computer
- The status of the policy
- The actions logged for the policy

Flushing logs for a policy with an execution frequency of “Once per computer” or “Once per user”

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the policy you want to view logs for.
5. Click **Logs**.
6. To view the actions logged for a computer, click **Show** for the computer.
   To hide the information when you are done viewing it, click **Hide**.
7. To flush a policy log for a single computer, click **Flush** for the computer.
8. To flush all logs for the policy, click **Flush All** at the top of the pane.
Policy Payload Reference

When creating or editing a policy, you use a payload-based interface to configure settings for the policy and add tasks to it. This section provides an overview of each payload.

General Payload

This payload allows you to do the following:

* Enable or disable the policy.
* Add the policy to a category.
* Choose one or more events to use to initiate the policy (called "trigger").
* Choose how often the policy should run (called "execution frequency").
* Make the policy available offline. (This only works with the "Ongoing" execution frequency.)
* Specify the drive on which to run the policy.
* Specify server-side and client-side limitations for the policy. (For example, you can specify an expiration date/time for the policy, or ensure that the policy does not run on weekends.)

Packages Payload

This payload allows you to perform the following software distribution tasks:

- Install packages.
- Cache packages.
- Install cached packages.
- Uninstall packages.

This payload also allows you to do the following when installing packages:

- Specify the distribution point computers should download the packages from.
- Add the packages to the Autorun data of each computer in the scope.

Software Updates Payload

This payload allows you to run Apple's Software Update and choose the software update server that you want computers to install updates from.

Scripts Payload

This payload allows you to run scripts and choose when they run in relation to other tasks in the policy. You can also enter values for script parameters.
Printers Payload

This payload allows you to map and unmap printers. You can also make a printer the default.

Disk Encryption Payload

This payload allows you to enable FileVault 2 on computers with OS X v10.8 or later by distributing disk encryption configurations.

This payload also allows you to issue a new FileVault 2 recovery key for computers with OS X v10.9 or later.

Dock Items Payload

This payload allows you to add and remove Dock items. When you add Dock items, you can also choose to add them to the beginning or end of the Dock.

Local Accounts Payload

This payload allows you to create and delete local accounts, and reset local account passwords. When you create an account, you can do the following:

- Specify a location for the home directory.
-Configure the account picture.
-Allow the user to administer the computer.
-Enable the account for FileVault 2 on computers with OS X v10.9 or later.

This payload also allows you to disable an existing local account for FileVault 2 on computers with OS X v10.9 or later.

Management Account Payload

This payload allows you to reset the management account password. You can choose to specify the new password or randomly generate it.

This payload also allows you to enable or disable the management account for FileVault 2 on computers with OS X v10.9 or later.

Directory Bindings Payload

This payload allows you to bind computers to a directory service.

EFI Password Payload

This payload allows you to set or remove an Open Firmware or EFI password.
**Restart Options Payload**

This payload allows you to restart computers after the policy runs. It also allows you to do the following:
- Specify the disk to restart computers from, such as a NetBoot image.
- Specify criteria for the restart depending on whether or not a user is logged in.
- Configure a restart delay.
- Perform an authenticated restart on computers with OS X v10.8.2 or later that are FileVault 2 enabled.

**Note:** For this to work on computers with FileVault 2 activated, the enabled FileVault 2 user must log in after the policy runs for the first time and the computer has restarted.

**Maintenance Payload**

- Update inventory.
- Reset computer names.
- Install all cached packages.
- Fix disk permissions.
- Fix ByHost files.
- Flush caches.
- Verify the startup disk.

This payload allows you to perform the following maintenance tasks:

**Files and Processes Payload**

This payload allows you to search computers for specific files and processes, and use policy logs to log when they are found. You can kill processes that are found and delete files that are found when searching by path.

This payload also allows you to execute commands.
User Interaction

User Interaction allows you to display custom messages to users about the policies that run on their computers. You can also use it to allow users to defer policies.

Messages

You can display User Interaction messages to users at the following times:
- Before a policy runs
- After a policy runs
- Before a policy restarts computers

This allows you to communicate with users about the policies that run on their computers. For example, you can let users know that software is about to be installed or that a new printer is available.

In OS X v10.8 and later, most User Interaction messages are displayed in the OS X Notification Center in a category called “Management”. Otherwise, messages are displayed using the JAMF Helper utility.

Deferral

You can allow users to defer a policy, and you can specify a date and time at which to prohibit further deferral (called the “deferral limit”). This allows you to give users more control over when the policy runs while ensuring that the policy eventually runs.

Before a policy runs on a computer, the user is prompted to choose to have the policy run immediately or to defer the policy for one of the following amounts of time:
- 1 hour
- 2 hours
- 4 hours
- 1 day
- The amount of time until the deferral limit is reached

If the user chooses to defer the policy, they are prompted with the same message after the chosen amount of time. When the deferral limit is reached, a message is displayed to notify the user, and the policy runs immediately.
Configuring User Interaction for a Policy

1. Log in to the JSS with a web browser.
2. Create or edit a policy.
3. Click the **User Interaction** tab.
4. Configure the settings on the pane.
5. When you are done configuring the policy, click **Save**.
**Scope**

Scope gives you granular control over which computers, mobile devices, and users receive remote management tasks. For example, you can use scope to ensure that a policy to install desktop publishing software only runs on computers in the Design department, or that an eBook is only distributed to students in a particular class.

Scope can be based on the following items:
- Individual computers, mobile devices, or users
- Computer, mobile device, or user groups
- Departments
- Buildings
- LDAP or local users
- LDAP user groups
- Network segments
- Classes
- iBeacon regions

The items available vary depending on the remote management task you are configuring the scope for. For example, only eBook scope can be based on classes.

**Note:** Scope cannot be based on personally owned mobile devices.

**Configuring Scope**

For most remote management tasks, configuring the scope involves adding targets, limitations, and exclusions. (The process varies depending on the remote management task you are configuring the scope for.)

**Adding Targets**

Targets make up the initial pool of computers, mobile devices, or users that receive the remote management task. You can add all computers, mobile devices, or users, or you can add a combination of specific items (e.g. computers, groups, buildings).
1. On the Targets pane, choose an option from the pop-up menu.

![Targets pane](image)

2. If you chose to add specific items:
   a. Click Add.
   b. On each tab, click Add for the items you want to add.
   c. Click Done.

The items you added are displayed in a list on the Targets pane.

### Adding Limitations

Adding limitations to the scope of a remote management task allows you to do the following:

- **Limit the task to specific users in the target.** For example, if you want a certain application to open at login for specific users regardless of the computer they use, you can use all computers as the target and add specific users as limitations.

- **Limit the task to specific network segments in the target.** For example, if you want each computer in a department to install a package but only while on the company’s production network, you can use the department as the target and add a specific network segment as a limitation.
1. On the Limitations pane, click Add.

2. On each tab, add items as needed.
   
   To add a network segment, click the **Network Segments** tab and then click **Add** for the network segment.

   ![Network Segments Tab](image)

   To add an LDAP or local user, click the **LDAP/Local Users** tab. Then enter the username in the search field and click **Add**.

   ![LDAP/Local Users Tab](image)

   To add an LDAP user group, click the **LDAP User Groups** tab, enter the name of the group in the search field, and click **Search**. Then click **Add** for the group you want to add.

   ![LDAP User Groups Tab](image)
3. Click **Done**.

The items you added are displayed in a list on the Limitations pane.

**Adding Exclusions**

Adding exclusions to the scope of a remote management task allows you to exclude specific computers or mobile devices, groups, buildings, departments, users, user groups, or network segments. For example, if you want to restrict an application for everyone except the head of the department, you can add them as an exclusion.

1. On the exclusions pane, click **Add**.

   ![Add button](image)

   **Exclusion**

   **Type**

   **No Exclusions**

2. On each tab, add items as needed.

   To add an LDAP or local user, click the **LDAP/Local Users** tab. Then enter the username in the search field and click **Add**.

   ![LDAP/Local Users tab](image)

   Add LDAP or Local Username: 

   **Add**

   **Done**

   To add an LDAP user group, click the **LDAP User Groups** tab, enter the name of the group in the search field, and click **Search**. Then click **Add** for the group you want to add.

   ![LDAP User Groups tab](image)

   Search LDAP User Groups: 

   **Search**

   **Done**

   To add another type of item, click the appropriate tab and then click **Add** for the item you want to add.

3. Click **Done**.

   The items you added are displayed in a list on the Exclusions pane.
About Self Service

The Self Service application allows users to browse and run policies, install configuration profiles, Mac App Store apps and eBooks, access webpages, and utilize plug-ins developed with the Self Service API. Users can point and click their way through Self Service using an intuitive interface similar to iTunes.

The JAMF Software Server (JSS) allows you to manage every aspect of Self Service, including its installation, user authentication, and the items available to users. In addition, you can configure notifications to be displayed to users as new items are added to Self Service.

You can make any policy, configuration profile, Mac App Store app, or eBook available in Self Service and customize how it is displayed to users. This includes displaying an icon and description, featuring the item on the main page, displaying it in relevant categories, and displaying item-specific notifications. You can also specify which computers display the item in Self Service and which users can access it.

MIT Software Center is installed automatically when a computer is enrolled in the JSS (casper client is installed) and can be found and accessed from the /Applications folder.
Self Service Policies

You can make any policy available in Self Service, but it is up to you to determine which policies are appropriate.

When you make a policy available in Self Service, you can specify which computers display it in Self Service and which users can access it (called “scope”).

You can also customize how Self Service policies are displayed to users by doing the following:

- Entering a description
- Uploading an icon
- Featuring the policy on the main page
- Displaying or featuring the policy in one or more categories

Creating a Self Service Policy

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Policies.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New.
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
6. Use the rest of the payloads to configure the tasks you want to perform.
7. Click the Scope tab and configure the scope of the policy.
8. Click the Self Service tab.
9. Select Make the policy available in Self Service.
10. Configure how the policy is displayed in Self Service using the settings on the pane. You can customize the text displayed in the description for the policy in Self Service by using Markdown in the Description field.
11. (Optional) Click the User Interaction tab and configure messaging and deferral options.
12. Click Save.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.
Self Service Configuration Profiles

You can make any OS X configuration profile available in Self Service, but it is up to you to determine which profiles are appropriate.

When you make a configuration profile available in Self Service, you can specify which computers display it in Self Service and which users can access it (called “scope”).

You can also customize how Self Service configuration profiles are displayed to users by doing the following:
- Entering a description
- Uploading an icon
- Featuring the configuration profile on the main page
- Displaying or featuring the configuration profile in one or more categories

Creating a Self Service Configuration Profile

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Configuration Profiles.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Do one of the following:
   - To use the JSS to manually create a new configuration profile, click New.
   - To upload a configuration profile (.mobileconfig) that was created using Apple’s Profile Manager, click Upload.
5. Use the General payload to set the distribution method to “Make Available in Self Service” and to configure basic settings.
6. Use the rest of the payloads to configure the settings you want to apply.
7. Click the Scope tab and configure the scope of the configuration profile.
8. Click the Self Service tab and configure how the configuration profile is displayed in Self Service using the settings on the pane. You can customize the text displayed in the description for the configuration profile in Self Service by using Markdown in the Description field.
9. Click Save.

Computer-level and user-level profile settings are applied when the user installs the profile from Self Service.
Self Service User Experience

This section provides an overview about what users do to log in to Self Service, run policies, install configuration profiles, Mac App Store apps, and eBooks, use plug-ins, and view notifications in Self Service.

Logging in to Self Service

After opening Self Service, users need to log in using their MIT KerbID.

Running Policies from Self Service

Users can browse policies from the “Featured” section or the list of categories in Self Service. Policies are only displayed in the “Featured” page if you configured the policy to do so.

To run a policy, users click the button next to it. Users can view the status of the policy installation in the status area at the top of Self Service.
Installing Configuration Profiles from Self Service

Users can browse and install computer-level and user-level configuration profiles from the “Featured” page or list of categories in Self Service. Users can view configuration profile installation status in the status area at the top of Self Service.

![Configuration Profiles](image)

If you have configured a configuration profile to allow it, users can also remove a configuration profile using Self Service.
Installing Mac App Store Apps from Self Service

Users can browse and install Mac App Store apps from the “Featured” page or list of categories on the main page.

To install an app, users click the button next to it. Users can view the status of the app installation in the status area at the top of Self Service.

Note: Mac App Store apps installed from Self Service are not managed by the JSS. Users can update apps using the Mac App Store or uninstall apps from their computers.

Viewing Self Service Notifications

Notifications are displayed to users when new items are added to Self Service.
A “Notifications” page allows the user to view a list of notifications for new items added to Self Service. The user can click to install any item in the list.

When the Self Service icon is in the Dock, the icon displays a red badge with a number to indicate how many new items have been added to Self Service since the user last viewed the “Notifications” page.

(Optional) When configured in the JSS for an item, notifications also display in Notification Center and as banners or alerts in OS X (requires OS X v10.8 or later). Users can click any notification to go to the item in Self Service.

(Optional) When configured in the JSS for an item, notification subject and/or message text for the item is displayed in the “Notifications” page of Self Service, in Notification Center, and in banners or alerts in OS X. If subject and message text is not specified, the item name is displayed in the notification by default.
Software Distribution

Mac App Store Apps

The JAMF Software Server (JSS) provides two Mac App Store app distribution methods: make the app available in Self Service, or install the app automatically/prompt users to install the app.

When you distribute a Mac App Store app, you add it to the JSS and configure settings for the app, including the distribution method. Then, you specify the computers and users that should receive it (called “scope”).

**Note:** Mac App Store apps distributed to computers are not managed by the JSS. Users can update apps using the Mac App Store or uninstall apps from their computers.

VPP Codes

When you distribute a Mac App Store app, you can also associate Volume Purchase Program (VPP) codes with the app and track their redemption.

**Note:** The JSS also supports VPP-managed distribution, which involves VPP assignments instead of VPP codes.

For more information on VPP, visit one of the following websites:

MIT Apple Volume Purchase Program
http://ist.mit.edu/iosapps/vpp

Volume Purchase Program for Education
https://www.apple.com/education/volume-purchase-program/

Apple Deployment Programs Help
Requirements

To allow users to install Mac App Store apps from Self Service via MDM, or to allow Mac App Store apps to be installed automatically you need:

- Computers with OS X v10.9 or later
  
  **Note:** If a computer does not have OS X v10.9 or later and the “Install Automatically/Prompt Users to Install” distribution method is selected, the app will instead be made available in Self Service.

- Users must have Mac App Store apps assigned to them via VPP-managed distribution.
  
  **Note:** If the scope for a Mac App Store app is configured to include a computer and the user is not assigned to that computer in the JSS, the app will instead be made available in Self Service.

- Users must be logged in to iTunes or the Mac App Store with the Apple ID used during VPP registration.

To allow users to install apps from the Mac App Store (linked from Self Service), you need:

- Computers with OS X v10.7 or later
- Computers that are bound to a directory service or local user accounts that have been MDM-enabled
- To associate VPP codes with a Mac App Store app, you need an Excel spreadsheet (.xls) that contains VPP codes for the app
- Users may be prompted to enter an Apple ID

Distributing a Mac App Store App

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Mac App Store Apps**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **New**.
5. Do one of the following:
   - To add the app by browsing the App Store, enter the name of the app, choose an App Store country, and click **Next**. Then click **Add** for the app you want to add.
   - To add the app by uploading a VPP code spreadsheet, click **Choose File** and upload the Excel spreadsheet (.xls) that contains VPP codes for the app.
   - To add the app by manually entering information about it, click **Enter Manually**.
6. Use the **General** pane to configure settings for the app, including the distribution method.
7. Click the **Scope** tab and configure the scope of the app.
8. (Optional) Click the **Self Service** tab and configure the way the app is displayed in Self Service. You can customize the text displayed in the description for the app in Self Service by using Markdown in the Description field.

   **Note:** The **Self Service** tab is only displayed if "Make Available in Self Service" is chosen in the **Distribution Method** pop-up menu.

9. (Optional) If you want to upload a VPP code spreadsheet, click the **VPP Codes** tab and upload the Excel spreadsheet (.xls) that contains VPP codes for the app.

   **Note:** The **VPP Codes** tab is only displayed if the **Free** checkbox is not selected.

10. Click **Save**.

---

**Editing or Deleting a Mac App Store App**

1. Log in to the JSS with a web browser.

2. Click **Computers** at the top of the page.

3. Click **Mac App Store Apps**.

   On a smartphone or iPod touch, this option is in the pop-up menu.

4. Click the app you want to edit or delete.

5. Do one of the following:

   - To edit the app, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the app from Self Service and the JSS, click **Delete** and then click **Delete** again to confirm.
Managing Packages

Packages in the following formats can be administered using the Casper Suite:

- DMG
- PKG
- MPKG

Before you can deploy a package, it must exist on the distribution point you plan to deploy it from and in the JAMF Software Server (JSS). There are two ways to achieve this:

- Add the package to Casper Admin
- Upload the package directly to the JSS - Preferred Method

Each of these methods also involves configuring settings for the package. When you configure settings for a package, you can do the following:

* Add the package to a category.
* Choose a priority for deploying or uninstalling the package.
* Fill user templates with the contents of the home directory in the package’s Users folder.
* Fill existing user home directories with the contents of the home directory in the package’s Users folder.
* Allow the package to be uninstalled.
* Specify whether computers must be restarted after installing the package.
* Choose whether the package must be installed on the boot drive after imaging.
* Specify operating system and architecture type requirements for deploying the package. Only allow the package to be installed if it is available in Software Update.
Adding a Package to Casper Admin

Adding a package to Casper Admin adds the package to the master distribution point and the JSS.

1. Open Casper Admin and authenticate to the JSS.

2. Drag the package to the main repository in Casper Admin. The package is displayed in blue text in the Unknown category until you add it to a category.

3. Double-click the package in the main repository.

4. Click the **General** tab and configure basic settings for the package, including the display name and category.

5. Click the **Options** tab and configure additional settings for the package, including the priority, and operating system and architecture type requirements.

6. Click **OK**.
Uploading a Package to the JSS - Preferred Method

If your master distribution point is the cloud distribution or a JDS instance, you can upload the package directly to the JSS. This adds the package to the master distribution point and the JSS.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click Settings.
3. Click Computer Management.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. In the "Computer Management" section, click Packages.
5. Click New.
6. Use the General pane to configure basic settings for the package, including the display name and category.
   Note: If you do not add the package to a category, Casper Admin displays the package in blue text in the Unknown category. Packages without a category will be DELETED.
7. Click Upload Package and upload the package.
8. Click the Options tab and configure additional settings for the package, including the priority.
9. (Optional) Click the Limitations tab and configure limitations for the package, including operating system and architecture type requirements.
10. Click Save.

Editing or Deleting a Package Using Casper Admin

1. Open Casper Admin and authenticate to the JSS.
2. In the main repository, select the package you want to edit or delete.
3. Do one of the following:
   - To edit the package, double-click it and make changes as needed. Then click OK.
   - To delete the package, click Delete and then click Delete again to confirm.

The edit or delete action is applied immediately on the master distribution point. The action is applied to your other distribution points when replication occurs.
**Editing or Deleting a Package Using the JSS**

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings**.
3. Click **Computer Management**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. In the “Computer Management” section, click **Packages**.
5. Click the package you want to edit or delete.
6. Do one of the following:
   - To edit the package, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the package, click **Delete** and then click **Delete** again to confirm.

   The edit or delete action is applied immediately on the master distribution point. The action is applied to your other distribution points when replication occurs.

**Indexing a Package**

Indexing a package creates a log of all the files contained within the package. This allows you to uninstall the package and view the contents of the package from the JSS.

Packages can be indexed using Casper Admin only. The time it takes to index a package depends on the amount of data in the package.

1. Open Casper Admin and authenticate to the JSS.
2. In the main repository, select the package you want to index and click **Index** at the bottom of the pane.
3. If prompted, authenticate locally.

   When the indexing process is complete, Casper Admin defaults back to the main repository.
Viewing the Contents of an Indexed Package

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click Settings.
3. Click Computer Management.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. In the “Computer Management” section, click Packages.
5. Click the package you want to view the contents of.
6. Click Contents.
   A table that contains the package contents is displayed.

Calculating a Checksum

The checksum is calculated when a package is uploaded to the JSS. The checksum ensures authenticity when the package is downloaded.

The checksum can also be calculated manually using Casper Admin:

1. Open Casper Admin and authenticate to the JSS.
2. In the main repository, select the package you want to calculate checksum for.
3. Control-click (or right-click) and select Calculate Selected Package Checksum(s).

Installing Packages

When you install a package, you can do the following:

- Fill user templates.
- Fill existing user home directories.
- Add the package to Autorun data.
- Specify a distribution point for computers to download the package from.

Requirements

To install a package on computers, the package must exist on the distribution point you plan to deploy it from and in the JSS.
Installing a Package Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **New**.
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
6. Select the Packages payload and click **Configure**.
7. Click **Add** for the package you want to install.
8. Choose "Install" from the **Action** pop-up menu.
9. Configure the settings for the package.
   To add the package to each computer's Autorun data, select the **Update Autorun data** checkbox.
10. Specify a distribution point for computers to download the package from.
11. Use the Restart Options payload to configure settings for restarting computers.
Caching Packages

Caching packages allows you to download them on computers without installing them right away. When you cache a package, you can specify a distribution point for computers to download the package from.

There are two ways to cache packages on computers: using a policy or using Casper Remote.

Requirements

To cache a package on computers, the package must exist on the distribution point you plan to deploy it from and in the JSS.

Caching a Package Using a Policy

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Policies. On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
6. Select the Packages payload and click Configure.
7. Click Add for the package you want to cache.
8. Choose "Cache" from the Action pop-up menu.
9. Configure the settings for the package. To add the package to each computer's Autorun data, select the Add to Autorun data checkbox.
10. Specify a server for computers to download the package from.
11. Use the Restart Options payload to configure settings for restarting computers.
12. Click the Scope tab and configure the scope of the policy.
13. (Optional) Click the Self Service tab and make the policy available in Self Service.
14. (Optional) Click the User Interaction tab and configure messaging and deferral options.
15. Click Save.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.
Installing Cached Packages

You can choose to install one or more specific cached packages, or all cached packages.

When you install one or more specific cached packages, you can do the following:
- Fill user templates.
- Fill existing user home directories.
- Add the package to Autorun data.

Requirements

To install a specific cached package, the package must exist on the distribution point you plan to deploy it from and in the JSS.

Installing a Cached Package Using a Policy

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Policies.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
6. Select the Packages payload.
7. Click Configure.
8. Click Add for the cached package you want to install.
9. Choose "Install Cached" from the Action pop-up menu.
10. Configure the settings for the package.
    To add the package to each computer’s Autorun data, select the Update Autorun data checkbox.
11. (Optional) Use the Restart Options payload to change the settings for restarting computers.
12. Click the Scope tab and configure the scope of the policy.
13. (Optional) Click the Self Service tab and make the policy available in Self Service.
14. (Optional) Click the User Interaction tab and configure messaging and deferral options.
15. Click Save.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.
Installing All Cached Packages Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **New**.
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
6. Select the Maintenance payload and click **Configure**.
7. Select **Install Cached Packages**.
8. Use the Restart Options payload to configure settings for restarting computers.
9. Click the **Scope** tab and configure the scope of the policy.
10. (Optional) Click the **Self Service** tab and make the policy available in Self Service.
11. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.
12. Click **Save**.

   The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.
Uninstalling Packages

Requirements

To uninstall a package from computers, you need:

- The package indexed in Casper Admin.
- The package configured so that it can be uninstalled.

Uninstalling a Package Using a Policy

1. Log in to the JSS with a web browser.
2. Click the Computers tab at the top of the page.
3. Click Policies.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New.
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
6. Select the Packages payload and click Configure.
7. Click Add for the package you want to uninstall.
8. Choose “Uninstall” from the Action pop-up menu.
9. Configure the settings for the package.
   To remove the package from each computer’s Autorun data, select the Update Autorun data checkbox.
10. Use the Restart Options payload to configure settings for restarting computers.
11. Click the Scope tab and configure the scope of the policy.
12. (Optional) Click the Self Service tab and make the policy available in Self Service.
13. (Optional) Click the User Interaction tab and configure messaging and deferral options.
14. Click Save.

   The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.
Patch Management

Running Software Update Using a Policy

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Policies.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New.
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
6. Select the Software Updates payload and click Configure.
7. Specify a server for computers to install software updates from.
8. Use the Restart Options payload to configure settings for restarting computers.
9. Click the Scope tab and configure the scope of the policy.
10. (Optional) Click the Self Service tab and make the policy available in Self Service.
11. (Optional) Click the User Interaction tab and configure messaging and deferral options.
12. Click Save.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.
Managed Preferences

Managed Preferences are manifest files that define preferences for computers and users. You can use the JAMF Software Server (JSS) to create Managed Preference profiles, which contain groups of Managed Preferences. You can also specify the users and computers for which a profile should be applied (called “scope”).

The JSS comes with manifest files for many common Managed Preferences so that you can easily add them to profiles. You can also add custom Managed Preferences by creating them manually or uploading a manifest file.

Levels for Managed Preferences

When you add a Managed Preference to a profile, you must specify a level at which to apply the preference. The level determines how and when the preference is applied. The levels available for each Managed Preference depend on the application or utility for which you are defining the preference.

If you have applied Managed Preferences using Apple’s Workgroup Manager, the level names in the JSS may be unfamiliar to you. The following table shows each level, its Workgroup Manager equivalent, when and how it is applied, and whether it is available for some or all Managed Preferences.

<table>
<thead>
<tr>
<th>JSS Levels</th>
<th>Workgroup Manager Levels</th>
<th>Applied at</th>
<th>Available for</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-level enforced</td>
<td>Always</td>
<td>Login with a login hook</td>
<td>Some Managed Preferences</td>
</tr>
<tr>
<td>User-level at every login</td>
<td>Often</td>
<td>Login with a login hook</td>
<td>All Managed Preferences</td>
</tr>
<tr>
<td>User-level at next login only</td>
<td>Once</td>
<td>Login with a login hook</td>
<td>All Managed Preferences</td>
</tr>
<tr>
<td>JSS Levels</td>
<td>Workgroup Manager Levels</td>
<td>Applied at</td>
<td>Available for</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------</td>
<td>----------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Computer-level enforced</td>
<td>Always (Applied to a computer object)</td>
<td>Reboot with a startup script</td>
<td>Some Managed Preferences</td>
</tr>
<tr>
<td>Unmanaged</td>
<td>Unset</td>
<td>Login or reboot</td>
<td>All Managed Preferences</td>
</tr>
</tbody>
</table>
Creating a Managed Preference Profile

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Managed Preferences**.
   
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **New**.
5. Use the General payload to configure basic settings for the profile.
6. Use the rest of the payloads to configure the Managed Preferences you want to apply.
7. (Optional) Manually create a custom Managed Preference:
   a. Select the Custom payload.
   b. Click **Add** for **Manual Setting**.
   c. Configure the Managed Preference using the options on the pane.
8. (Optional) Upload a manifest file:
   a. Select the Custom payload.
   b. Click **Add** for **Upload Manifest**.
   c. Upload the manifest file.
9. Click the **Scope** tab and configure the scope of the profile.
10. Click **Save**.

   The profile is applied the next time computers in the scope check in with the JSS.

Cloning, Editing, or Deleting a Managed Preference Profile

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Managed Preferences**.
   
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the Managed Preference profile you want to clone, edit, or delete.

5. Do one of the following:
   - To clone the profile, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the profile, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the profile, click **Delete** and then click **Delete** again to confirm.

The clone, edit, or delete action is applied to computers in the scope the next time they check in with the JSS.
OS X Configuration Profiles

OS X configuration profiles are XML files (.mobileconfig) that provide an easy way to define settings and restrictions for computers and users.

You can use the JAMF Software Server (JSS) to manually create an OS X configuration profile or upload a configuration profile that was created using Apple's Profile Manager.

Before creating a configuration profile, you should have basic knowledge of configuration profile payloads and settings, and how they affect computers. For detailed information about each payload and setting, see Apple's Profile Manager documentation at:


Some configuration profile settings are unique to the JSS. For more information on these settings, see the following Knowledge Base article:

Configuration Profiles Reference

When you create an OS X configuration profile, you must specify the level at which to apply the profile—computer level or user level. Each level has a unique set of payloads and a few that are common to both. There are two different ways to distribute an OS X configuration profile: install it automatically (requires no interaction from the user) or make it available in Self Service. You can also specify the computers and users to which the profile should be applied (called "scope").

Payload Variables for OS X Configuration Profiles

There are several payload variables that you can use to populate settings in an OS X configuration profile with attribute values stored in the JSS. This allows you to create payloads containing information about each computer and user to which you are distributing the profile.

To use a payload variable, enter the variable into any text field when creating a configuration profile in the JSS. When the profile is installed on a computer, the variable is replaced with the value of the corresponding attribute in the JSS.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Computer Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>$COMPUTERNAME</td>
<td>Computer Name</td>
</tr>
<tr>
<td>$UDID</td>
<td>UDID</td>
</tr>
<tr>
<td>$SERIALNUMBER</td>
<td>Serial Number</td>
</tr>
<tr>
<td>$USERNAME</td>
<td>Username associated with the computer in the JSS (computer-level profiles only)</td>
</tr>
<tr>
<td>$FULLNAME or $REALNAME</td>
<td>Full Name</td>
</tr>
</tbody>
</table>
### Manually Creating an OS X Configuration Profile

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Configuration Profiles**.
   - On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **New**.
5. Use the General payload to configure basic settings, including the level at which to apply the profile and the distribution method.
   - Only payloads and settings that apply to the selected level are displayed for the profile.
6. Use the rest of the payloads to configure the settings you want to apply.
7. Click the **Scope** tab and configure the scope of the profile.
8. (Optional) If you chose to distribute the profile in Self Service, click the **Self Service** tab to configure Self Service settings for the profile.
9. Click **Save**.

For configuration profiles set to the “Install Automatically” distribution method, computer-level profiles are installed the next time computers in the scope check in with the JSS. User-level profiles are installed the next time users in the scope log in to their computers.

For configuration profiles set to the “Make Available in Self Service” distribution method, computer-level and user-level profile settings are applied when the user installs the profile from Self Service.
Uploading an OS X Configuration Profile

You can create an OS X configuration profile by uploading a profile that was created using Apple's Profile Manager.

**Note:** Some payloads and settings configured with Profile Manager are not displayed in the JSS. Although you cannot view or edit these payloads, they are still applied to computers and users.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Configuration Profiles**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **Upload** and upload the configuration profile (.mobileconfig).
5. Use the General payload to change or configure basic settings for the profile, including a distribution method.
6. Use the rest of the payloads to configure or edit settings as needed.
7. Click the **Scope** tab and configure the scope of the profile.
8. (Optional) If you chose to distribute the profile in Self Service, click the **Self Service** tab to configure Self Service settings for the profile.
9. Click **Save**.

For configuration profiles set to the “Install Automatically” distribution method, computer-level and user-level profile settings are applied when the user installs the profile from Self Service.

For configuration profiles set to the “Make Available in Self Service” distribution method, computer-level profiles are installed the next time computers in the scope check in with the JSS. User-level profiles are installed the next time users in the scope log in to their computers.
Cloning, Editing, or Deleting an OS X Configuration Profile

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Configuration Profiles**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the configuration profile you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the profile, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the profile, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the profile, click **Delete** and then click **Delete** again to confirm.

For computer-level profiles, the clone, edit, or delete action is applied to computers in the scope the next time they check in with the JSS. For user-level profiles, the clone, edit, or delete action is applied the next time users in the scope log in to their computers.

Downloading an OS X Configuration Profile

If you want to view the contents of an OS X configuration profile for troubleshooting purposes, you can download the profile (.mobileconfig) from the JSS.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Configuration Profiles**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the configuration profile you want to download.
5. Click **Download**.

The profile downloads immediately.
OS X Remote Commands

The OS X remote commands available in the JAMF Software Server (JSS) allow you to remotely perform the following tasks on a computer:

- Lock a computer.
- Remove the MDM profile.
- Wipe a computer.
- Send a blank push notification.

You can send an OS X remote command to a single computer.

The following table describes the OS X remote commands that you can send from the JSS.

<table>
<thead>
<tr>
<th>OS X Remote Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Computer</td>
<td>Logs the user out of the computer, restarts the computer, and then locks the computer. To unlock the computer, the user must enter the passcode that you specified when you sent the Lock Computer command.</td>
</tr>
</tbody>
</table>
| Remove MDM Profile        | Removes the MDM profile from the computer, along with any configuration profiles that were distributed with the Casper Suite. If the MDM profile is removed, you can no longer send remote commands or distribute configuration profiles to the computer.  
**Note:** Removing the MDM profile from a computer does not remove the computer from the JSS or change its inventory information. |
| Wipe Computer             | Permanently erases all data on the computer. **Note:** Wiping a computer does not remove the computer from the JSS or change its inventory information.  
To restore the computer to the original factory settings, the user must enter the passcode that you specified when you sent the Wipe Computer command, and then reinstall the operating system.  
For detailed information on OS X Recovery, see the following Apple Knowledge Base article: [https://support.apple.com/kb/HT4718](https://support.apple.com/kb/HT4718) |
| Send Blank Push           | Sends a blank push notification, prompting the computer to check in with Apple Push Notification service (APNs) |

Requirements

To manage OS X remote commands, you need:

- Computers with OS X v10.7 or later and a Recovery Partition
Sending an OS X Remote Command

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer you want to send the OS X remote command to.
   If you performed a simple search for an item other than computers, you must click **Expand** next to an item to view the computers related to that item.
5. Click the **Management** tab, and then click the button for the remote command that you want to send.
   - If you are sending a Lock Computer command, type a password that the user must enter to unlock the computer.
   - If you are sending a Wipe Computer command, type a password that the user must enter to restore the computer.

   The remote command runs on the computer the next time the computer checks in with the JSS.

Viewing the Status of OS X Remote Commands

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer you want to view OS X remote commands for.
   If you performed a simple search for an item other than computers, you must click **Expand** next to an item to view the computers related to that item.
5. Click the **History** tab.
6. Use the Management History pane to view completed, pending, or failed commands.

Canceling an OS X Remote Command

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.
4. Click the computer for which you want to cancel an OS X remote command.
   If you performed a simple search for an item other than computers, you must click **Expand** next to an item to view the computers related to that item.
5. Click the **History** tab, and then click **Pending Commands**.
6. Find the command you want to cancel, and click **Cancel** across from it.
Managing Scripts

The way you manage scripts depends on the way scripts are stored in your environment. There are two ways scripts can be stored:

- **As data in the jamfsoftware database**—Before you can run a script in this type of environment, the script must exist in the database. There are two ways to achieve this:
  - Add the script to Casper Admin
  - Add the script to the JSS using the script editor

- **As files on your distribution point(s)**—Before you can run a script in this type of environment, the script must exist on the distribution point you plan to deploy it from and in the JSS. You can add the script to the master distribution point by adding it to Casper Admin. Then you can add the script to other distribution points via replication.

**Note:** For more information on migrating the scripts on your master distribution point, see the following Knowledge Base article:

* Migrating Packages and Scripts

Each of these methods also involves configuring settings for the script. When you configure settings for a script, you can do the following:

* Add the script to a category.
* Choose a priority for running the script during imaging.
* Enter parameter labels.
* Specify operating system requirements for running the script.

Requirements

To add a script to Casper Admin, the script file must be non-compiled and in one of the following formats:

- Perl (.pl)
- Bash (.sh)
- Shell (.sh)
- Non-compiled AppleScript (.applescript)
- C Shell (.csh)
- Zsh (.zsh)
- Korn Shell (.ksh)
- Tool Command Language (.tcl)
- Hypertext Preprocessor (.php)
- Ruby (.rb)
- Python (.py)
Adding a Script to Casper Admin

Adding a script to Casper Admin adds the script to the jamfsoftware database or the master distribution point, and to the JSS.

1. Open Casper Admin and authenticate to the JSS.
2. Drag the script to the main repository in Casper Admin.
   The script is displayed in blue text in the Unknown category until you add it to a category.
3. Double-click the script in the main repository.
4. Click the **General** tab and configure basic settings for the script, including the display name and category.

5. Click the **Options** tab and configure additional settings for the script, including the priority and parameter labels.

6. Click **OK**.
Adding a Script to the JSS

If your environment is one in which scripts are stored in the jamfsoftware database, you can add a script to the JSS using the script editor.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings**.
3. Click **Computer Management**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. In the “Computer Management” section, click **Scripts**.
5. Click **New**.
6. Use the General pane to configure basic settings for the script, including the display name and category.
   **Note:** If you do not add the script to a category, Casper Admin displays the script in blue text in the Unknown category.
7. Click the **Script** tab and enter the script contents in the script editor.
8. Click the **Options** tab and configure additional settings for the script, including the priority.
9. (Optional) Click the **Limitations** tab and configure operating system requirements for the script.
10. Click **Save**.

Editing or Deleting a Script Using Casper Admin

1. Open Casper Admin and authenticate to the JSS.
2. In the main repository, select the script you want to edit or delete.
3. Do one of the following:
   - To edit the script, double-click it and make changes as needed. Then click **OK**.
   - To delete the script, click **Delete** and then click **Delete** again to confirm.

If the script is stored in the jamfsoftware database, the edit or delete action is applied immediately.

If the script is stored on your distribution point(s), the edit or delete action is applied immediately on the master distribution point. The action is applied to your other distribution points when replication occurs.
Cloning, Editing, Deleting a Script Using the JSS

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click Settings.
3. Click Computer Management.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. In the “Computer Management” section, click Scripts.
5. Click the script you want to edit or delete.
6. Do one of the following:
   - To clone the script, click Clone and make changes as needed. Then click Save.
   - To edit the script, click Edit and make changes as needed. Then click Save.
   - To delete the script, click Delete and then click Delete again to confirm.

If the script is stored in the jamfsoftware database, the clone, edit, or delete action is applied immediately.

If the script is stored on your distribution point(s), the clone, edit, or delete action is applied immediately on the master distribution point. The action is applied to your other distribution points when replication occurs.
Running Scripts

When you run a script, you can choose a priority for running the script. You can also enter parameter values for the script.

Running a Script Using a Policy

1. Log in to the JSS with a web browser.
2. Click the Computers tab at the top of the page.
3. Click Policies.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New.
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
6. Select the Scripts payload and click Configure.
7. Click Add for the script you want to run.
8. Configure the settings for the script.
9. Use the Restart Options payload to configure settings for restarting computers.
10. Click the Scope tab and configure the scope of the policy.
11. (Optional) Click the Self Service tab and make the policy available in Self Service.
12. (Optional) Click the User Interaction tab and configure messaging and deferral options.
13. Click Save.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.
Managing Printers

Adding printers to Casper Admin or the JAMF Software Server (JSS) is the first step to administering printers on computers.

When you add a printer to Casper Admin, you choose from a list of printers that are on the computer running Casper Admin. When you add a printer to the JSS, you manually specify information about the printer, such as the CUPS name and device URI.

When you add, edit, or delete a printer in Casper Admin, the changes are reflected in the JSS and vice versa.

When you configure a printer, you can do the following:
- Add the printer to a category.
- Choose whether or not the printer is set as the default when mapped during imaging.
- Specify an operating system requirement for mapping the printer.

Adding a Printer to Casper Admin

Several settings in Casper Admin have tool tips. To read more about a specific setting, hover your mouse over it until a tool tip is displayed.

1. Open Casper Admin and authenticate to the JSS.
2. Click Add Printers.
3. If prompted, authenticate locally.
4. Select the checkbox next to each printer you want to add.
5. (Optional) Choose a category to add printer(s) to.
6. Click Add.
7. Select the printer in the main repository and double-click it.
8. Click the **General** tab and configure basic settings for the printer, including the display name and category.

9. Click the **Options** tab.

10. Choose whether or not the printer is set as the default when mapped during imaging, and configure the operating system requirement.

11. Click **OK**.

---

**Adding a Printer to the JSS**

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings**.
3. Click **Computer Management**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. In the “Computer Management” section, click **Printers**.
5. Click **New**.
6. Use the General pane to configure basic settings for the printer, including the display name and category.
7. Click the **Definition** tab and specify information about the printer, including the CUPS name and device URI.
8. (Optional) Click the **Limitations** tab and specify an operating system requirement.
9. Click **Save**.

**Editing or Deleting a Printer in Casper Admin**

Several settings in Casper Admin have tool tips. To read more about a specific setting, hover your mouse over it until a tool tip is displayed.

1. Open Casper Admin and authenticate to the JSS.
2. In the main repository, select the printer you want to edit or delete.
3. Do one of the following:
   - To edit the printer, double-click it and make changes as needed. Then click **OK**.
   - To delete the printer, click **Delete** and then click **Delete** again to confirm.

**Cloning, Editing, or Deleting a Printer in the JSS**

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings**.
3. Click **Computer Management**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. In the “Computer Management” section, click **Printers**.
5. Click the printer you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the printer, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the printer, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the printer, click **Delete** and then click **Delete** again to confirm.
Administering Printers

There are two ways to map or unmap printers on computers: using a policy or using Casper Remote. When you map a printer, you can choose whether or not to make the printer the default.

Requirements
To map or unmap a printer, the printer must be added to Casper Admin or the JSS.

Mapping or Unmapping a Printer Using a Policy

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Policies.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New.
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
6. Select the Printers payload and click Configure.
7. Click Add across from the printer you want to map or unmap.
8. Choose "Map" or "Unmap" from the Action pop-up menu.
9. (Optional) If you are mapping the printer, make it the default printer by selecting the Set as Default checkbox.
10. Use the Restart Options payload to configure settings for restarting computers.
11. Click the Scope tab and configure the scope of the policy.
12. (Optional) Click the Self Service tab and make the policy available in Self Service.
13. (Optional) Click the User Interaction tab and configure messaging and deferral options.
14. Click Save.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.
Managing Dock Items

Adding Dock items to Casper Admin or the JAMF Software Server (JSS) is the first step to administering Dock items on computers.

When you add a Dock item to Casper Admin, you choose from a list of Dock items that are on the computer running Casper Admin. When you add a Dock item to the JSS, you manually specify information about the Dock item.

When you add, edit, or delete a Dock item in Casper Admin, the changes are reflected in the JSS and vice versa.

Adding a Dock Item to Casper Admin

1. Open Casper Admin and authenticate to the JSS.
2. Click Add Dock Items.
3. Select the checkbox next to each Dock item you want to add.
4. Click Add.

Adding a Dock Item to the JSS

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click Settings.
3. Click Computer Management.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. In the “Computer Management” section, click Dock Items.
5. Click New.

6. Configure the Dock item using the settings on the pane.

7. Click Save.

Deleting a Dock Item in Casper Admin

1. Open Casper Admin and authenticate to the JSS.
2. In the main repository, select the Dock item you want to delete.
3. Click Delete and then click Delete again to confirm.

Cloning, Editing, or Deleting a Dock Item in the JSS

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click Settings.
3. Click Computer Management.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. In the “Computer Management” section, click Dock Items.
5. Click the Dock item you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the Dock item, click Clone and make changes as needed. Then click Save.
   - To edit the Dock item, click Edit and make changes as needed. Then click Save.
   - To delete the Dock item, click Delete and then click Delete again to confirm.
Administering Dock Items

There are two ways to add or remove Dock items on computers: using a policy or using Casper Remote.

When you add a Dock item on computers, you can choose whether to add it to the beginning or the end of the Dock.

Requirements

To add or remove a Dock item on computers, the Dock item must be added to Casper Admin or the JSS.

Adding or Removing a Dock Item Using a Policy

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Policies.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New.
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
6. Select the Dock Items payload and click Configure.
7. Click Add for the Dock item you want to add or remove.
8. Choose "Add to Beginning of Dock", "Add to End of Dock", or "Remove from Dock" from the Action pop-up menu.
9. Use the Restart Options payload to configure settings for restarting computers.
10. Click the Scope tab and configure the scope of the policy.
11. (Optional) Click the Self Service tab and make the policy available in Self Service.
12. (Optional) Click the User Interaction tab and configure messaging and deferral options.
13. Click Save.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.
Administering Local Accounts

You can perform the following local account administration tasks using a policy or Casper Remote:

- Create a new account.
- Delete an existing account.
- Reset the password for an existing account.
- (Policy only) Disable an existing account for FileVault 2 on computers with OS X v10.9 or later.

When you create a new account, you can do the following:

- Specify the password and password hint.
- Specify a location for the home directory.
- Configure the account picture.
- Give the user administrator privileges to the computer.
- (Policy only) Enable the account for FileVault 2 on computers with OS X v10.9 or later.

When you delete an existing account, you can permanently delete the home directory or specify an archive location.

Requirements

To enable a new account for FileVault 2, the computer must have OS X v10.9 or later and have an existing, valid individual recovery key that matches the recovery key stored in the JSS.

To disable an existing account for FileVault 2, the computer must have OS X v10.9 or later.

Administering Local Accounts Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   - On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **New**.
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
6. Select the Local Accounts payload and click **Configure**.
7. Choose an action from the **Action** pop-up menu.
8. Configure the action using the options on the pane.

9. Use the Restart Options payload to configure settings for restarting computers.

10. Click the **Scope** tab and configure the scope of the policy.

11. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

12. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

13. Click **Save**.

   The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.
Administering Open Firmware/EFI Passwords

You can administer Open Firmware or EFI passwords to ensure the security of managed computers.

There are two ways to set and remove an Open Firmware/EFI password: using a policy or using Casper Remote.

Requirements

If you are setting or removing an Open Firmware/EFI password on models "Late 2010" or later, the "setregproptool" must be present on the volume(s) used to set firmware. (For more information, see the Setting EFI Passwords on Mac Computers (Models Late 2010 or Later Knowledge Base article.)

Setting or Removing an Open Firmware/EFI Password Using a Policy

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Policies.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New.
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
6. Select the EFI Password payload and click Configure.
7. Do one of the following:
   - To set an Open Firmware/EFI password, choose "Command" from the pop-up menu and enter and verify the password.
   - To remove an Open Firmware/EFI password, choose "None" from the pop-up menu.
8. Use the Restart Options payload to configure settings for restarting computers.
9. Click the Scope tab and configure the scope of the policy.
10. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

11. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

12. Click **Save**.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.
License Management

About Licensed Software

Licensed software allows you to store and track licenses for the software in your environment so you can easily access license and purchasing information and monitor license compliance.

For each software product that you want to track licenses for, you must create a licensed software record in the JAMF Software Server (JSS). These records allow you to store information about the licenses owned and the software titles that count toward each license (called “software definitions”).

Each time a computer submits inventory to the JSS, the software on the computer is compared to the software definitions in the licensed software records. If they match, the computer counts toward the number of licenses in use.

After creating licensed software records, you can use the JSS to evaluate and monitor license compliance, view and report on the licenses in use, and view Application Usage information for the software you’re tracking licenses for.
Licensed Software Records

For each software application you want to track licenses for, you must create a licensed software record in the JAMF Software Server (JSS). These records allow you to store the number of licenses owned and the software titles that count toward each license (called “software definitions”). They also allow you to store detailed license and purchasing information in the JSS.

Each time a computer submits inventory to the JSS, the software titles on the computer are compared to the software definitions in each record. If they match, the computer counts toward the number of licenses in use.

Licensed software records also allow you to determine whether a license supersedes or is superseded by another license in the JSS. For example, you may have licenses for Adobe Illustrator and Adobe CS 5.5 Design Standard, both of which contain Adobe Illustrator. The licenses for Adobe Illustrator will not be counted toward the licenses for CS 5.5 Design Standard even though CS 5.5 Design Standard contains Adobe Illustrator. Viewing the licensed software record for Adobe Illustrator would show that the licenses are superseded by CS 5.5 Design Standard. Alternatively, viewing the record for CS 5.5 Design Standard would show that the licenses supersede Adobe Illustrator.

There are several ways to create a licensed software record in the JSS. You can manually create the record, use a licensed software template available in the JSS, or upload a licensed software template obtained from JAMF Nation. All licensed software templates have predefined software definitions.

Software definitions can be based on one of two items: the name and version number of each application, font, and plug-in, or the software identification (SWID) tags associated with each software title. For more information on SWID tags and how they are useful for tracking licensed software with the Casper Suite, see the following Knowledge Base article:

Requirements

To create a licensed software record based on SWID tags, the software you want to track must have a SWID tag associated with it and the SWID tag must be in the JSS database.

Note: The JSS collects SWID tags from a computer each time the computer submits inventory. SWID tags are not listed in a computer’s inventory information in JSS, but they are stored in the JSS database for use with licensed software.
Manually Creating a Licensed Software Record

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Licensed Software**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **New**.
5. Use the General pane to configure basic settings for the licensed software record.
   To enable email notifications, select the **Send email notification on violation** checkbox.
6. Click the **Licenses** tab and add license and purchasing information:
   a. Click **Add**.
   b. Specify information about the license, including the license type and license count.
   c. (Optional) Click the **Purchasing Information** tab and enter purchasing information.
   d. (Optional) Click the **Attachments** tab and click **Upload** to upload an attachment.
   e. Click **Save**.
   f. Repeat steps a through e to add more license and purchasing information as needed.
7. Click the **Software Definitions** tab.
8. To specify software definitions based on applications, fonts, and plug-ins, do the following:
   a. Choose “Applications, Fonts, and Plug-ins” from the **Software Definitions Type** pop-up menu.
   b. Click **Add** for the item you want to add.
   c. Specify a name, connector (“is” or “like”), and version number using the fields and pop-up menu provided.
   d. Click **Save**.
   e. Repeat steps a through d to specify additional software definitions as needed.
   The items you added are displayed in a list.
9. To specify software definitions based on SWID tags, do the following:
   a. Choose “Software ID Tags” from the **Software Definitions Type** pop-up menu.
   b. Browse for and choose a reg ID.
   c. Add a SWID tag by clicking **Add**. Then browse for and choose the SWID tag you want to add.
   d. Select the activation statuses you want to include in the software definitions.
10. Click **Save**.
Creating a Licensed Software Record From a Template

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Licensed Software.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New From Template.
5. Click the licensed software template you want to use.
6. Use the General pane to change or configure basic settings for the licensed software record.
   To enable email notifications, select the Send email notification on violation checkbox.
7. Click the Licenses tab and add license and purchasing information:
   a. Click Add.
   b. Enter information about the license, including the license type and license count.
   c. (Optional) Click the Purchasing Information tab and enter purchasing information.
   d. (Optional) Click the Attachments tab and click Upload to upload an attachment.
   e. Click Save.
   f. Repeat steps a through e to add more license and purchasing information as needed.
8. To view or edit software definitions, click the Software Definitions tab and make changes as needed.
9. Click Save.

Uploading a Licensed Software Template

You can create a licensed software record by uploading a licensed software template obtained from JAMF Nation. Licensed software templates are available in JAMF Nation at:

https://jamfnation.jamfsoftware.com/licensedSoftwareTemplates.html

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Licensed Software.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click Upload and upload the licensed software template.
5. Use the General pane to change or configure basic settings for the licensed software record.
   To enable email notifications, select the Send email notification on violation checkbox.
6. Click the **Licenses** tab and add license and purchasing information:
   a. Click **Add**.
   b. Enter information about the license, including the license type and license count.
   c. (Optional) Click the **Purchasing Information** tab and enter purchasing information.
   d. (Optional) Click the **Attachments** tab and click **Upload** to upload an attachment.
   e. Click **Save**.
   f. Repeat steps a through e to add more license and purchasing information as needed.

7. To view or edit software definitions, click the **Software Definitions** tab and make changes as needed.

8. Click **Save**.

---

**Cloning, Editing, or Deleting a Licensed Software Record**

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Licensed Software**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the licensed software record you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the licensed software record, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the licensed software record, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the licensed software record, click **Delete** and then click **Delete** again to confirm.
License Compliance

You can evaluate license compliance by viewing the licensed software records in the JSS and comparing the number of licenses in use to the number of licenses owned.

You can also monitor software compliance by allowing email notifications to be sent to JSS users each time a license limit is exceeded.

Evaluating License Compliance

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Licensed Software.
   On a smartphone or iPod touch, this option is in the pop-up menu.

A list of licensed software records is displayed along with the number of licenses in use and the number of licenses owned for each record.

Viewing License Usage

If you are using licensed software records to track software licenses, you can view a list of computers with the licenses in use (called “license usage matches”).

Viewing License Usage Matches

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Licensed Software.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the licensed software record you want to view license usage matches for.
5. Click View Matches.
   Note: This button is only displayed if the licenses associated with the record are in use on managed computers.

A list license usage matches is displayed.
Restricted Software

Restricted software allows you to prevent users or groups of users from accessing certain applications. For instance, you might want to prevent all users from accessing a peer-to-peer file sharing application or restrict everyone except the IT staff from accessing common administrative utilities.

For each application that you want to restrict, you must create a restricted software record. This allows you to specify the users to which the restriction applies and control what happens when the application is opened by those users. For instance, you can kill the restricted process, delete the application, and even display a message to the user.

Creating a Restricted Software Record

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Restricted Software.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New.
5. Configure the restricted software record using the fields and options on the pane. To enable email notifications, select the Send email notification on violation checkbox.
6. Click the Scope tab and configure the scope of the restricted software record.
   For more information, see Scope.
7. Click Save.

The restriction is applied to computers in the scope the next time they check in with the JSS.

Cloning, Editing, or Deleting a Restricted Software Record

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Restricted Software.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the restricted software record you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the restricted software record, click Clone and make changes as needed. Then click Save.
   - To edit the restricted software record, click Edit and make changes as needed. Then click Save.
   - To delete the restricted software record, click Delete and then click Delete again to confirm.
Inventory

User Assignments

The JAMF Software Server (JSS) allows you to assign users to computers, mobile devices, and peripherals.

There are two ways to assign a user to a computer or mobile device:

- Manually (Requires the computer or mobile device to be enrolled with the JSS)
- During user-initiated enrollment

Users must be assigned to peripherals manually.

**Note:** You can only assign a user to a peripheral if you have completed the Migration Assistant and the peripheral is not already assigned to a computer.

This section explains how to do the following:

- Manually assign a user to a computer, mobile device, or peripheral.
- Remove the user assignment from a computer, mobile device, or peripheral.

**Manually Assigning a User to a Computer or Mobile Device**

1. Log in to the JSS with a web browser.
2. Click **Computers** or **Mobile Devices** at the top of the page.
3. Perform a simple or advanced search.
4. Click the computer or mobile device you want to assign a user to.

5. Select the **User and Location** category and click **Edit**.

6. Do one of the following:
   - To assign an existing user, enter the user’s partial or full username in the **Username** field and click the **Search** icon. Click **Choose** across from the user you want to assign, and then click **Save**. The **Full Name**, **Email Address**, **Phone Number**, and **Position** fields are populated automatically.
   - To assign and create a new user, enter information about the user and click **Save**.

**Assigning a User to a Peripheral**

1. Log in to the JSS with a web browser.

2. Click **Computers** at the top of the page.

3. Click **Search Inventory**.
   On a smartphone or iPod touch, this option is in the pop-up menu.

4. Choose “Peripherals” from the **Search** pop-up menu.

5. Enter one or more search terms in the field provided.
   You can base peripheral searches on peripheral type, customizable peripheral fields, or bar code.

6. Press the Enter key.
   The list of search results is displayed.

7. Click the peripheral you want to assign a user to.

8. Select the **User and Location** category and click **Edit**.

9. Do one of the following:
   - To assign an existing user, enter the user’s partial or full username in the **Username** field and click the **Search** icon. Click **Choose** across from the user you want to assign, and then click **Save**. The **Full Name**, **Email Address**, **Phone Number**, and **Position** fields are populated automatically.
   - To assign and create a new user, enter information about the user and click **Save**.

   **Note:** You can only assign a user to a peripheral if you have completed the Migration Assistant and the peripheral is not already assigned to a computer.

   If you specified user and location information, the information is applied in the **Users** tab and the user is assigned to the peripheral. This specified information is also applied in the inventory information for computers, mobile devices, and other peripherals that the user is assigned to.
Removing a User Assignment from a Computer or Mobile Device

1. Log in to the JSS with a web browser.
2. Click Computers or Mobile Devices at the top of the page.
3. Perform a simple or advanced search.
4. Click the computer or mobile device you want to remove a user assignment from.
5. Select the User and Location category and click Edit.
6. Remove the username from the Username field and click Save.
   The information in the Full Name, Email Address, Phone Number, and Position fields is removed automatically.

Removing a User Assignment from a Peripheral

1. Log in to the JSS with a web browser.
2. Click Computers at the top of the page.
3. Click Search Inventory.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Choose "Peripherals" from the Search pop-up menu.
5. Enter one or more search terms in the field provided.
   You can base peripheral searches on peripheral type, customizable peripheral fields, or bar code.
6. Press the Enter key.
7. The list of search results is displayed.
8. Click the peripheral you want to remove a user assignment from.
9. Select the User and Location category and click Edit.
10. Remove the username from the Username field and click Save.
    The information in the Full Name, Email Address, Phone Number, and Position fields is removed automatically.
Simple User Searches

A simple user search functions like a search engine, allowing you to quickly search the users in your inventory for a general range of results.

You can base searches on any of the following attributes:

- Username
- Full name
- Email address

Search Syntax

This section explains the syntax to use for the following search functions:

- Wildcard searches
- Including multiple search terms
- Excluding a search term
- Returning all users

In general, searches are not case-sensitive.

**Note:** The default search preference is “Exact Match”. For most items, the option can be changed to either “Starts with” or “Contains”.

Wildcard Searches

Asterisks (*) function as wildcard characters in simple searches. The following table explains the different ways asterisks can be used to refine a search:

<table>
<thead>
<tr>
<th>Usage</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use an asterisk after a search term to return all results with attributes that begin with that term.</td>
<td>Perform a search for “John*” to return all users with full names that begin with “John”.</td>
</tr>
<tr>
<td>Use an asterisk before a search term to return all results with attributes that end with that term.</td>
<td>Perform a search for “*@mycompany.com” to return all users with email addresses that end with “@mycompany.com”.</td>
</tr>
<tr>
<td>Use an asterisk before and after a search term to return all results that include that term.</td>
<td>Perform a search for “<em>Jane</em>” to return all users that include “Jane”.</td>
</tr>
<tr>
<td>Use an asterisk without any other terms to return all results for the item you are searching.</td>
<td>Perform a search for “*” to return all users.</td>
</tr>
</tbody>
</table>
Including Multiple Search Terms

Use multiple search terms separated by a comma (,) to return all results that include those search terms.

For example, perform a search for “John*, *Doe” to return all users that begin with “John” and end with “Doe”.

Excluding a Search Term

Use a hyphen (-) before a search term to exclude results that include the term.

For example, perform a search for “Jane*, -*@mycompany.com” to return all users with full names that begin with “Jane” except for those with email addresses that end with “@mycompany.com”.

Returning All Users

There are two ways to return all users: use an asterisk (*) without any other characters or terms, or perform a blank search.

Performing a Simple User Search

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Search Users**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Enter one or more search terms in the field provided.
5. Press the Enter key.

   The list of search results is displayed.
Advanced User Searches

Advanced user searches allow you to use detailed search criteria to search for users in the JAMF Software Server (JSS). These types of searches give you more control over your search by allowing you to do the following:

- Generate specific search results.
- Specify which attribute fields to display in the search results.
- Save the search.

Creating an Advanced User Search

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
   If the migration assistant is displayed on the pane, you must migrate your users before you proceed.
3. Click **Search Users**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **New** .
5. Use the Search pane to configure basic settings for the search.
   To save the search, select the **Save this Search** checkbox.
6. Click the **Criteria** tab and add criteria for the search:
   a. Click **Add** .
   b. Click **Choose** for the criteria you want to add.
   c. Choose an operator from the **Operator** pop-up menu.
   d. Enter a value in the **Value** field or browse for a value by clicking **Browse** .
   e. Repeat steps a through d to add criteria as needed.
7. Choose an operator from the **And/Or** pop-up menu(s) to specify the relationships between criteria.
8. To group criteria and join multiple operations, choose parentheses from the pop-up menus around the criteria you want to group.
9. Click the **Display** tab and select the attribute fields you want to display in your search results.
10. Click **Save**.

Operations in the search take place in the order they are listed (top to bottom).

The results of a saved search are updated each time user information is modified and users meet or fail to meet the specified search criteria.

To view the search results, click **View**.

**Cloning, Editing, or Deleting a Saved Advanced User Search**

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Search Users**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the advanced user search you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the search, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the search, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the search, click **Delete**. Then click **Delete** again to confirm.

**Viewing Advanced User Search Results**

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Search Users**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the advanced user search you want to view the results for.
5. Click **View**.

The list of search results is displayed.
User Reports

The data displayed in smart or static group membership lists or user search results can be exported from the JAMF Software Server (JSS) to the following file formats:
- Comma-separated values file (.csv)
- Tab delimited text file (.txt)
- XML file

Creating User Reports

1. Log in to the JSS with a web browser.
2. Click Users at the top of the page.
3. Do one of the following:
   - View user group memberships.
   - View simple or advanced user search results.
4. At the bottom of the list, click Export.
5. Follow the onscreen instructions to export the data.
   The report downloads immediately.
Simple Content Searches

A simple content search functions like a search engine, allowing you to quickly search the mobile device apps, Mac App Store apps, and eBooks in your inventory for a general range of results.

Content searches are based on the name of the application or eBook you are searching for.

Search Syntax

This section explains the syntax to use for the following search functions:

- Wildcard searches
- Including multiple search terms
- Excluding a search term
- Returning all content

In general, searches are not case-sensitive.

**Note:** The default search preference is “Exact Match”. For most items, the option can be changed to either “Starts with” or “Contains”.

**Wildcard Searches**

Asterisks (*) function as wildcard characters in simple searches. The following table explains the different ways asterisks can be used to refine a search:

<table>
<thead>
<tr>
<th>Usage</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use an asterisk after a search term to return all results with attributes that begin with that term.</td>
<td>Perform a search for “key*” to return all content with names that begin with “key”.</td>
</tr>
<tr>
<td>Use an asterisk before a search term to return all results with attributes that end with that term.</td>
<td>Perform a search for “*note” to return all content with names that end with “note”.</td>
</tr>
</tbody>
</table>
| Use an asterisk before and after a search term to return all results that include that term. | Perform a search for “**ABC**” to return all content that includes “ABC”.
| Use an asterisk without any other terms to return all results for the item you are searching. | Perform a search for “**” to return all content. |

**Including Multiple Search Terms**

Use multiple search terms separated by a comma (,) to return all results that include those search terms.

For example, perform a user search for “key*, *note” to return all content that begins with “key” and ends with “note”.
Excluding a Search Term

Use a hyphen (-) before a search term to exclude results that include the term.

For example, perform a user search for “ABC*, -*note” to return all content with names that begin with “ABC” except for those that end with “note”.

Returning All Content

There are two ways to return all content: use an asterisk (*) without any other characters or terms, or perform a blank search.

Performing a Simple Content Search

1. Log in to the JSS with a web browser.
2. Click Users at the top of the page.
   If the migration assistant is displayed on the pane, you must migrate your users before you proceed.
3. Click Search Content.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Enter one or more search terms in the field provided.
5. Press the Enter key.

   The list of search results is displayed.
Advanced Content Searches

Advanced content searches allow you to use detailed search criteria to search mobile device apps, Mac App Store apps, and eBooks in the JAMF Software Server (JSS). These types of searches give you more control over your search by allowing you to do the following:

- Generate specific search results.
- Specify which attribute fields to display in the search results.
- Save the search.

Creating an Advanced Content Search

1. Log in to the JSS with a web browser.
2. Click Users at the top of the page.
   If the migration assistant is displayed on the pane, you must migrate your users before you proceed.
3. Click Search Content.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New.
5. Use the Search pane to configure basic settings for the search.
   To save the search, select the Save this Search checkbox.
6. Click the Criteria tab and add criteria for the search:
   a. Click Add.
   b. Click Choose for the criteria you want to add.
   c. Choose an operator from the Operator pop-up menu.
   d. Enter a value in the Value field or browse for a value by clicking Browse.
   e. Repeat steps a through d to add criteria as needed.
7. Choose an operator from the And/Or pop-up menu(s) to specify the relationships between criteria.
8. To group criteria and join multiple operations, choose parentheses from the pop-up menus around the criteria you want to group.
Click the **Display** tab and select the attribute fields you want to display in your search results.

Click **Save**.

Operations in the search take place in the order they are listed (top to bottom).

The results of a saved search are updated each time content is modified and meets or fails to meet the specified search criteria.

To view the search results, click **View**.

**Cloning, Editing, or Deleting a Saved Advanced Content Search**

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Search Content**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the advanced content search you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the search, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the search, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the search, click **Delete**. Then click **Delete** again to confirm.

**Viewing Advanced Content Search Results**

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Search Content**.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the advanced content search you want to view the results for.
5. Click **View**.
   The list of search results is displayed.
## Content Reports

The data displayed in content search results can be exported from the JAMF Software Server (JSS) to the following file formats:

- Comma-separated values file (.csv)
- Tab delimited text file (.txt)
- XML file

### Creating Content Reports

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Search Content**.
   - On a smartphone or iPod touch, this option is in the pop-up menu.
4. View simple or advanced content search results.
   - **Note:** You can only create a report from a simple content search if you searched by all content.
5. At the bottom of the list, click **Export**.
6. Follow the onscreen instructions to export the data.
   - The report downloads immediately.
## Viewing and Editing Inventory Information for a User

The JAMF Software Server (JSS) stores detailed inventory information for each user. You can view and edit this information from the JSS.

The following table lists the information that you can view and edit for each user.

**Note:** Extension attributes are displayed in the General category of user inventory information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Editable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Category</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Full Name</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Email Address</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Phone Number</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Position</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Extension Attributes</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Site</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Mobile Devices Category</strong></td>
<td></td>
<td>Displays a list of mobile devices that the user is assigned to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Computers Category</strong></td>
<td></td>
<td>Displays a list of computers that the user is assigned to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>eBooks Category</strong></td>
<td></td>
<td>Displays a list of eBooks distributed to the user</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Peripherals Category</strong></td>
<td></td>
<td>Displays a list of peripherals that the user is assigned to, and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>peripherals assigned to computers that the user is assigned to</td>
</tr>
</tbody>
</table>
### Viewing Inventory Information from the Users Tab

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
   
   If the migration assistant is displayed on the pane, you must migrate your users before you proceed. (For more information and complete instructions, see the [Migrating Users Knowledge Base article.](#))
3. Perform a simple or advanced user search.
4. Click the user you want to view information for.
   
   The user's inventory information is displayed.
5. Use the categories to view information for the user.

### Editing Inventory Information from the Users Tab

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Perform a simple or advanced user search.
4. Click the user you want to edit information for.
   
   The user's inventory information is displayed.
5. Click **Edit**.
6. Make changes as needed.

*Note:* You cannot make changes to user and location information for peripherals that are assigned to a computer.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Editable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VPP Assignments Category</strong></td>
<td></td>
<td>Displays a list of content assigned to the user via VPP assignments</td>
</tr>
<tr>
<td><strong>VPP Codes Category</strong></td>
<td></td>
<td>Displays a list of VPP codes redeemed by the user</td>
</tr>
</tbody>
</table>
7. Click **Save**.

Changes to a user’s site are only applied in the Users tab. All other changes to a user’s inventory information are applied in the **Users** tab and also in the inventory information for computers, mobile devices, and peripherals that the user is assigned to.

**Note:** Removing a user from a site will remove the user assignment from all computers and mobile devices that belong to that site.
About User Groups

User groups allow you to organize users that share similar attributes. You can use these groups as a basis for configuring the scope of remote management tasks.

There are two kinds of user groups: smart user groups and static user groups. Smart user groups are based on criteria and have dynamic memberships. Static user groups have fixed memberships that you manually assign.
Smart User Groups

Smart user groups give you a way to organize users based on one or more attributes, such as username, full name, and email address. These groups have dynamic memberships that are updated whenever user information is edited.

Creating a Smart User Group

1. Log in to the JSS with a web browser.
2. Click Users at the top of the page.
3. Click Smart User Groups.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New.
5. Use the User Group pane to configure basic settings for the group. To enable email notifications, select the Send email notification on membership change checkbox.
6. Click the Criteria tab and add criteria to the group:
   a. Click Add .
   b. Click Choose for the criteria you want to add.
      To display additional criteria, click Choose for "Other Criteria".
   c. Choose an operator from the Operator pop-up menu.
   d. Enter a value in the Value field or browse for a value by clicking Browse .
   e. Repeat steps a through d to add criteria as needed.
7. Choose an operator from the And/Or pop-up menu(s) to specify the relationships between criteria.
8. To group criteria and join multiple operations, choose parentheses from the pop-up menus around the criteria you want to group.

<table>
<thead>
<tr>
<th>Smart Group</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td></td>
</tr>
<tr>
<td>And/Or</td>
<td>Criteria</td>
</tr>
<tr>
<td>Email Address</td>
<td>in</td>
</tr>
<tr>
<td>or</td>
<td>Full Name</td>
</tr>
<tr>
<td>and</td>
<td>Position</td>
</tr>
</tbody>
</table>
Operations in the group take place in the order they are listed (top to bottom).

Group memberships are updated each time user information is edited.

To view the group memberships, click View.

**Cloning, Editing, or Deleting a Smart User Group**

1. Log in to the JSS with a web browser.
2. Click Users at the top of the page.
3. Click Smart User Groups. On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the smart user group you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the group, click Clone and make changes as needed. Then click Save.
   - To edit the group, click Edit and make changes as needed. Then click Save.
   - To delete the group, click Delete. Then click Delete again to confirm.

**Viewing Smart User Group Memberships**

1. Log in to the JSS with a web browser.
2. Click Users at the top of the page.
3. Click Smart User Groups. On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the smart user group you want to view memberships for.
5. Click View.

A list of group memberships is displayed.
Static User Groups

Static user groups give you a way to organize users by assigning them to a group. These groups have fixed memberships that must be changed manually.

After creating a static user group, you can view its memberships.

Creating a Static User Group

1. Log in to the JSS with a web browser.
2. Click Users at the top of the page.
3. Click Static User Groups.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click New.
5. Use the User Group pane to configure basic settings for the group.
6. Click the Assignments tab and select the checkbox for each user you want to add.
7. Click Save.

To view the group memberships, click View.

Cloning, Editing, or Deleting a Static User Group

1. Log in to the JSS with a web browser.
2. Click Users at the top of the page.
3. Click Static User Groups.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the group you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the group, click Clone and make changes as needed. Then click Save.
   - To edit the group, click Edit and make changes as needed. Then click Save.
   - To delete the group, click Delete. Then click Delete again to confirm.
Viewing Static User Group Memberships

1. Log in to the JSS with a web browser.
2. Click Users at the top of the page.
3. Click Static User Groups.
   On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click the user group you want to view memberships for.
5. Click View.

A list of group memberships is displayed.
Appendix I
Helpful Links
JAMF Resources

For more information on Casper Suite-related topics, see the following resources:

- **Casper Suite Release Notes**
  
The release notes include a list of new features, bug fixes, and known issues. They also explain how to upgrade the JSS, and what you need to do to take advantage of new features. Release notes for the most recent version of the Casper Suite are available in the Casper Suite DMG, and at:
  

- **JAMF Software Server installation and configuration guides**
  
  These guides provide information on installing and setting up the JSS on supported Mac, Linux, and Windows platforms. They also explain how to perform advanced configuration and troubleshooting tasks. They are available at:
  

- **Manually Installing the JAMF Software Server**
  
  This technical paper explains how to manually install the JSS on Linux and Windows platforms. You can download it from:
  

- **QuickStart Guides**
  
  The *QuickStart Guide for Managing Computers* and the *QuickStart Guide for Managing Mobile Devices* serve as a starting point for new Casper Suite administrators. They provide simplified workflows for performing basic administrative tasks, such as inventory and software distribution, and they reference related sections in the *Casper Suite Administrator’s Guide*. Both QuickStart Guides are available in the Casper Suite DMG, and at:
  

- **Technical papers**
  
  JAMF Software technical papers provide best-practice, step-by-step workflows for using the Casper Suite to administer third-party software, such as Adobe Creative Suite or FileVault 2. They are available at:
  
  [http://www.jamfsoftware.com/technical-papers](http://www.jamfsoftware.com/technical-papers)

- **JAMF Nation**
  
  The JAMF Nation community website contains several different types of resources related to the Casper Suite. It allows you communicate with other Casper Suite administrators via discussions, submit feature requests, and access the Knowledge Base. The Knowledge Base contains hundreds of articles that address frequently asked questions and common issues. You can access JAMF Nation at:
  
  [https://jamfnation.jamfsoftware.com](https://jamfnation.jamfsoftware.com)
IS&T Resources

Test Casper Server:
https://casper1-test.mit.edu:8443

Production Casper Server:
https://casper1.mit.edu:8443

Apple Volume Purchasing Program:
http://ist.mit.edu/iosapps/vpp

Casper Client & Other Resources:
https://www.dropbox.com/sh/t2fpvk7d85bekze/AAAbUJTdji9byY4OsLfwrLoOa?dl=0

Casper KB Article:
http://kb.mit.edu/confluence/display/istcontrib/Casper+Suite

Mac Imaging & Tools:
https://wikis.mit.edu/confluence/x/_o7zB

Contact support by emailing:
endpointmanagement@mit.edu
Overview of Technologies
Applications and Utilities

This section provides an overview of the applications and utilities that make up the Casper Suite.

Casper Admin

The Casper Admin application is a repository that allows you to add and manage packages, scripts, printers, and Dock items. It also allows you to create configurations (images) using these items and replicate files to distribution points.

Composer

The Composer application allows you to build packages (PKG or DMG) of software, applications, preference files, or documents. Composer also allows you to build a DMG of an operating system.

jamf agent

The jamf agent collects application usage data and restricts software on managed computers.

The jamf agent is installed and updated on managed computers automatically. It is installed in the following location:

/usr/sbin/jamfAgent

jamf binary

Most tasks in the Casper Suite are executed using the “jamf“ command-line application (also known as the jamf binary). Although you are free to use this application at will, it is installed, updated, and run on managed computers automatically. It is stored in the following location on managed computers:

/usr/sbin/jamf

JAMF Helper

The JAMF Helper displays messages to users. It is stored in the following location on managed computers:

/Library/Application Support/JAMF/bin/
JAMF Software Server

The JAMF Software Server (JSS) is a web application that functions as the administrative core of the Casper Suite. The JSS allows you to perform inventory and remote management and configuration tasks on managed computers and mobile devices. All other administrative applications in the Casper Suite communicate with the JSS.

Management Action

The Management Action application displays User Interaction messages in the OS X Notification Center. It is stored in the following location on managed computers:

/Library/Application Support/JAMF/bin/

Self Service for OS X

The Self Service application allows users to browse and run policies, install configuration profiles, Mac App Store apps and eBooks, access webpages, and utilize plug-ins developed with the Self Service API. Users can point and click their way through Self Service using an intuitive interface similar to iTunes.

You can make any policy, configuration profile, Mac App Store app, or eBook available in Self Service and customize how it is displayed to users. You can also make two types of plug-ins available in Self Service: URL plug-ins and Self Service Plug-in bundles. URL plug-ins give users easy access to webpages right from the application. Self Service Plug-in bundles are custom plug-ins developed with the Self Service API.
Security

This section explains the primary security measures in the Casper Suite:

- Passwords
- Communication protocols
- Public key infrastructure
- Signed applications

Passwords

The Casper Suite allows you to store individual accounts for managed computers and reset the passwords if necessary.

Passwords stored in the database are encrypted using a standard 256-bit AES encryption algorithm.

Communication Protocols

The Casper Suite has security built into its design. Connections between the JAMF Software Server (JSS), the other applications in the Casper Suite, and mobile devices take place over Secure Sockets Layer (SSL) using Transport Layer Security (TLS). The Casper Remote application and the network scanner in the Recon application connect to computers over Secure Shell (SSH), or Remote Login.

Secure Shell (SSH)

SSH is a network security protocol built into OS X. For more information, go to:
http://openssh.com/

Transport Layer Security (TLS)

TLS is a security protocol for Internet communication. For more information, go to:

Public Key Infrastructure

A public key infrastructure (PKI) is the design by which digital certificates are obtained, managed, stored, and distributed to ensure a secure exchange of data over a public network.
Certificate Authority

A certificate authority (CA) is a trusted entity that signs and issues the certificates required for certificate-based authentication. It is the central component of the PKI.

The JSS includes a preconfigured PKI that uses a built-in CA. The built-in CA is used by default to issue certificates to both computers and mobile devices.

You can also configure your own PKI if you have access to an external CA that supports SCEP. The external CA can be a CA hosted by your organization or by a trusted third-party vendor. If you integrate an external CA with the JSS, this CA will be used to issue certificates to both computers and mobile devices.

Simple Certificate Enrollment Protocol

Simple Certificate Enrollment Protocol (SCEP) obtains certificates from the CA and distributes them to managed mobile devices, providing a simplified way of handling large-scale certificate distribution.

The CA hosted by the JSS (the “built-in CA”) supports SCEP. If you plan to use an external CA hosted by your organization or by a third-party vendor, this CA must support SCEP as well.

Certificates

The Casper Suite uses the following certificates to ensure security:

- **SSL Certificate**—The JSS requires a valid SSL certificate to ensure that computers and mobile devices communicate with the JSS and not an imposter server. The SSL certificate that you can create from the built-in CA secures communication using a 2048-bit RSA encryption.

- **Device Certificates**—Device certificates allow the JSS to verify the identity of OS X computers and mobile devices each time they communicate with the JSS.

- **CA Certificate**—This certificate establishes trust between the CA and OS X computers, and between the CA and mobile devices.

- **Signing Certificate**—This certificate is used to sign messages passed between the JSS and OS X computers, and between the JSS and mobile devices.

- **Push Certificate**—The JSS requires a valid push certificate to communicate with Apple Push Notification service (APNs).

- **Anchor Certificate**—This certificate allows mobile devices and computers to trust the SSL certificate.
Global Management Settings
Recurring Check-in Frequency

The recurring check-in frequency is the interval at which computers check in with the JSS for available policies. The recurring check-in frequency is set to “Every 30 Minutes”.

Startup Script

The Startup Script settings in the JAMF Software Server (JSS) allow you to create a startup script on computers and use it to perform the following actions at startup:

- Check for policies triggered at startup.
- Enable computer-level Managed Preferences.

Login and Logout Hooks

The Login/Logout Hooks settings in the JAMF Software Server (JSS) allow you to create login and logout hooks on computers and use them to perform the following actions:

- Check for policies triggered at login or logout.
- Enable user-level and user-level enforced Managed Preferences at login.
- Hide the Restore partition at login.

Warning: Creating login and logout hooks with the Casper Suite can disable existing login and logout hooks.
Security Settings

The Security settings in the JAMF Software Server (JSS) allow you to do the following:

- Enable certificate-based authentication.
- Enable push notifications.
- Enable SSL certificate verification.
- Specify the condition under which the checksum will be used to validate packages.
- Specify a maximum clock skew between managed computers and the JSS host server.

When an OS X computer attempts to communicate with the JSS and the security requirements specified in the JSS are not met, communication is blocked.
Appendix II
Composer

About Composer

Composer allows you to build packages of software, applications, preference files, or documents. A package is a self-contained group of files that can be deployed to remote computers or as part of the imaging process.

The first step to building a package is creating a package source. Depending on the files you want to package, Composer allows you to monitor the installation of your software or use files that already exist on the drive to create the package source.

After you create a package source, you can build a PKG or a DMG from the package source.

Composer also allows you to build a DMG of an operating system.
Creating Package Sources

A package source allows you to view and edit attributes of a package (such as files, scripts, privileges, and localizations) before it is built. Once a package source exists for a group of files, you can make modifications and build the package as many times as necessary.

There are several ways to create a package source:

- **Take snapshots**—Composer takes before and after snapshots of the file system and creates a package source based on the changes. This method allows you to monitor installations in all locations on the drive. If necessary, you can also quit Composer or log out/reboot during the installation process.

- **Monitor the file system**—Composer uses the File System Events (FSEvents) framework to monitor any changes that are made to the file system during the installation process. Next, Composer creates a package source based on the changes. This method does not allow you to quit Composer or log in/reboot during the installation process. In addition, an excess of file system activity can cause FSEvents to miss changes.

- **Use pre-installed software**—You can use software that is pre-installed on your computer to create a package source based on package manifests. This method allows you to create package sources without monitoring the installation process.

- **Use user environment settings**—Package manifests can also be used to capture settings configured on your computer, such as Dashboard, Display, and Global Preference settings.

- **Drag contents from the Finder**—A simple drag-and-drop process allows you to create a package source from files already installed on your computer.

- **Use an existing package**—Composer allows you to make modifications to an existing package or convert between the PKG and DMG package formats.

Taking Snapshots

If the files you want to package are not already installed on the drive, Composer can take a snapshot of the file system before and after the files have been installed and create a package source based on the changes.

Composer can take two kinds of snapshots:

- **Normal snapshots**—These snapshots capture any new files on the drive. These snapshots can take anywhere from ten seconds to several minutes depending on your hardware and the number of files on the drive.

- **New and modified snapshots**—These snapshots capture any new files on the drive, as well as any files that have been modified. These snapshots can take longer than normal snapshots, since Composer records the modifications date of each file while performing the snapshot.
There are several benefits to using the snapshot approach:

- Composer monitors installations in all locations on the drive.
- You can quit Composer during the installation process.
- You can log out or reboot during the installation process.
- If you delete a file while making modifications to a package source, it may be possible to restore the deleted file.

1. Open Composer and authenticate locally.
2. In the toolbar, click **New**.
3. Under the Monitor Installation heading in the sidebar, select **Snapshot**.
4. Select **Normal Snapshot** or **New & Modified Snapshot** and click **Next**.
5. Enter a name for the package and click **Next**.
6. Install and configure your software, and then click **Create Package Source** to initiate the “after” snapshot.

---

### Monitoring the File System

When creating a package source using file system monitoring, Composer uses the File System Events (FSEvents) framework that is built into OS X to monitor any changes that are made to the file system. Each time a change is made, FSEvents receives a notification. After your software is installed, Composer analyzes the changes and creates a package source based on the results.

The following limitations should be taken into consideration when monitoring the file system to create a package source:

- You cannot quit Composer during the installation process.
- You cannot log in or restart during the installation process.
- It is possible for FSEvents to miss events if there is too much file system activity.

1. Open Composer and authenticate locally.
2. In the toolbar, click **New**.
3. Under the Monitor Installation heading in the sidebar, select **Snapshot**.
4. Select **Monitor File System Changes** and click **Next**.

5. Enter a name for the package and click **Next**.

6. Install and configure your software, and then click **Create Package Source**.
Creating Package Sources From Pre-Installed Software

You can create a package source from software that is currently installed on your computer if Composer contains a package manifest for the software.

**Note:** If there is software you would like added to the package manifest options in Composer, email your recommendations to diffs@jamfsoftware.com.

1. Open Composer and authenticate locally.
2. In the toolbar, click **New**.
3. Under the Package Manifests heading in the sidebar, select **Pre-Installed Software**.
   Composer scans the file system and displays icons for the software it can package.
   **Note:** To view package manifests for software that is not installed on the computer, click the disclosure triangle next to **Pre-Installed Software** and select **Not Installed**.
4. Select the item(s) you want to create a package source from and click **Next**.

Creating Package Sources from the User Environment Settings

You can create a package source that captures the look and feel of your computer’s interface, such as Dashboard, Display, and Global Preference settings. If Composer contains a package manifest for the setting you want to capture, you can create a package source from it.

To determine which of your current settings Composer can package, select **User Environment** under the Package Manifests heading. Composer scans the file system and displays icons for the settings that it has package manifests for.

**Note:** If there is a setting you would like added to the package manifest options in Composer, email your recommendations to diffs@jamfsoftware.com.
1. Open Composer and authenticate locally.
2. In the toolbar, click **New**.
3. Under the Package Manifests heading in the sidebar, select **User Environment**.
4. Select the item(s) you want to create a package source from and click **Next**.

**Creating Package Sources by Dragging Contents from the Finder**

If you already know which item you want to package, you can bypass the snapshot or monitoring process by dragging items from the Finder to the Sources list in Composer.

There are a few ways Composer handles these items:

- If the item is a package (DMG, PKG, or MPKG), it is listed in the sidebar under the Packages heading.
- If the item is a folder, the root of the folder is used as the root of the package if it is one of the following directories:
  
  /Applications/
  /Developer/
  /Library/
  /System/
  /Users/
  /bin/
  /private/
  /sbin/
  /usr/

- Any other items are copied to their current location.

**Note:** This is the equivalent of a PreBuilt package in earlier versions of Composer.
Creating Package Sources from Existing Packages

Composer allows you to rebuild an existing package (PKG, DMG, or MPKG) by converting it to a package source. After converting it to a package source, you can make changes to its contents and save a new copy of the package.

1. Open Composer and authenticate locally.

2. Drag the package you want to convert from the Finder to the sidebar in Composer. The package appears under the Packages heading.

3. Select the package and click **Convert to Source**.

When the conversion is complete, a new package source is listed in the sidebar under the Sources heading.
### Package Manifests

Package manifests are .composer files that can be used to create package sources from the software installed on your computer. They can also be used to capture settings configured on your computer, such as Dashboard, Display, and Global Preference settings.

Composer comes with over 100 package manifests. You can use the update feature in Composer to add new package manifests as they become available. You can also create your own package manifests and import package manifests that are stored on your computer.

### Creating Package Manifests

1. Open Composer and authenticate locally.
2. Click the disclosure triangle next to an existing package source.
3. Click the disclosure triangle next to Snapshots.
4. Control-click (or right-click) Files For Package and select Export Package Manifest.
5. Enter a name for the package manifest.

6. Enter a description of the package manifest and the name of the person who is creating it.

7. Select the checkbox next to each file that must be present on a computer for the package manifest to appear under the Pre-Installed Software heading or the User Environment heading in Composer.

8. If desired, select the **Custom Icon** checkbox and choose an icon for the package manifest. The icon is displayed when viewing the package manifest in Composer.

9. If you want to upload the package manifest to JAMF Nation:
   a. Click **Upload to JAMF Nation**.
   b. Enter the username and password for your JAMF Nation account.
   c. Choose a third-party product to associate the package manifest with. For example, if you are creating a package manifest for Adobe Reader 10, associate it with the "Adobe Reader" third-party product.
   d. Click **Upload**.

10. Click **Save As**.

11. Choose a location to save the package manifest and click **Save**.
### Updating Package Manifests

Periodically, new package manifests become available for Composer. To ensure that you have the latest package manifests, choose **File > Update Package Manifests** from the menu bar in Composer.

Composer downloads the latest package manifests from JAMF Nation and any new package manifests that JAMF Software has added to the application, and stores them in the following location:

/Library/Application Support/JAMF/Composer/ImportedPackageManifests/

### Importing Package Manifests

If you do not want to add all package manifests from JAMF Nation to Composer, you can download one or more specific package manifests from JAMF Nation and import them to Composer. You can also import package manifests that you created.

To import package manifests that are saved to your computer, choose **File > Import Package Manifests** from the menu bar in Composer and then choose the package manifest you want to import.

Composer imports the package manifests and stores them in the following location:

/Library/Application Support/JAMF/Composer/ImportedPackageManifests/
Viewing and Editing the Contents of Package Sources

Once a package source exists for the files you want to package, Composer allows you to do the following:

- Delete files that should not be included in the package.
- Add files by dragging them into Composer from the Finder.
- Change privileges on a file or folder.
- Restore files that were deleted from the package source.

In addition to viewing files or folders through the Composer interface, you can view this information in the Finder or using Quick Look.

Deleting Files or Folders from a Package Source

In the Package Contents pane, select the item(s) you want to delete from the package source and choose File > Delete from the menu bar.

Adding Files to a Package Source

Drag the file(s) you want to add to your package source from the Finder into the Package Contents pane in Composer.

Changing Privileges on Files or Folders in a Package Source

Select a file or folder in the Package Contents pane in Composer to display its privileges in the bottom of the window. You can change the privileges using this display. Changes are saved automatically. If the selected item is a folder, you can apply the privileges that exist on the folder to each enclosed item by clicking the Action button to the right of the X-column.

Restoring Deleted Files or Folders to a Package Source

If you delete a file or folder from the Package Contents pane, it may be possible to restore the item. When you restore a deleted file or folder, Composer copies the item from its original location on the drive.

**Note:** Deleted files and folders can only be restored if a snapshot was used to create the package source.

1. Open Composer and authenticate locally.
2. Click the disclosure triangle next to the package source in the sidebar.
3. Click the disclosure triangle next to Snapshots.
4. Select **Files for Package** to display a list of files, folders, and directories from the snapshot.
5. Select the item you want to restore.
6. Control-click (or right-click) the selected item and choose **Restore**.

**Viewing Files or Folders in a Package Source Using the Finder**

In the Package Contents pane, select the item(s) you want to preview, and then choose **File > Reveal in Finder** from the menu bar.

**Viewing Files or Folders in a Package Source Using Quick Look**

In the Package Contents pane, select the item(s) you want to preview, and then choose **File > Quick Look** from the menu bar or press the Space bar.
Adding Scripts to Package Sources

Composer allows you to manage scripts for PKGs. The following default scripts are available in shell and perl:

- InstallationCheck
- Postflight
- Postinstall
- Postupgrade
- Preflight
- Preinstall
- Preupgrade
- VolumeCheck

**Note:** Flat PKGs support Preinstall and Postinstall scripts only. To build a PKG that contains other scripts, you can deselect the **Build Flat PKGs** option in Composer preferences, or you can disable this preference for a single package.

These scripts read in the available parameters that are received from the installer and give descriptions for the supported exit codes.

Composer also attempts to verify that the script syntax is valid. If a script appears to have invalid syntax, a warning icon appears.

To view the error that occurred while Composer was verifying the script, Control-click (or right-click) the script and choose **Compile Script**.

**Note:** InstallationCheck and VolumeCheck scripts have warning and failure messages that can be localized according to the needs of the user. To localize these messages, the corresponding .strings file (InstallationCheck.strings or VolumeCheck.strings) must be created for each localization.

Adding a postflight script to a package source allows you to remove deprecated or unneeded files from computers as they install the package.

1. Open Composer and authenticate locally.
2. Click the disclosure triangle next to the package source in the sidebar.
3. Do one of the following:
   - To add a postflight script that removes deleted files from computers, click the disclosure triangle next to Snapshots. Then Control-click (or right-click) the Deleted Files heading and choose Add postflight Shell Script.
     
     **Note:** This function is only available if a snapshot was used to create the package source.
   - To add another type of script, Control-click (or right-click) Scripts and choose the script you want to add.

The script is displayed under the Scripts heading in the sidebar.

4. (Optional) Select the script in the sidebar to view or change its contents.

**Adding a Postflight Script that Removes Deleted Files from Computers**

Adding a postflight script to a package source allows you to remove deprecated or unneeded files from computers as they install the package.

**Note:** This function is only available if a snapshot was used to create the package source.
4. Select the Deleted Files heading to view the deleted files captured by the snapshot.

5. Control-click (or right-click) the Deleted Files heading and choose **Add postflight Shell Script**.

   ![Postflight Shell Script](image)

   The script is displayed under the Scripts heading in the sidebar.

6. (Optional) Select the script in the sidebar to view or change its contents.
Localizations

Localizations allow you to customize the language used when displaying package information to a user. By default, a package source only includes an English localization.

Composer includes defaults for the following localizations supported by the PKG format:
- `da.lproj`
- `Dutch.lproj`
- `English.lproj`
- `Fi.lproj`
- `French.lproj`
- `German.lproj`
- `Italian.lproj`
- `Japanese.lproj`
- `ko.lproj`
- `no.lproj`
- `pl.lproj`
- `pt_PT.lproj`
- `pt.lproj`
- `ru.lproj`
- `Spanish.lproj`
- `sv.lproj`
- `zh_CN.lproj`
- `zh_TW.lproj`

Adding Localizations to Package Sources

1. Open Composer and authenticate locally.
2. Click the disclosure triangle next to the package source in the sidebar.
3. Control-click (or right-click) Settings and choose the localization that you want to add.
Adding and Editing Files for a Localization

You can include two kinds of files in a localization:

- **Description.plist files**—These files display the title of a package and its description in the Installer application. Each localization contains a description.plist file by default.
- **Strings files**—VolumeCheck.strings and InstallationCheck.strings files are used to localize warning and error messages. These files are only effective when used in conjunction with their corresponding scripts (VolumeCheck and InstallationCheck).

1. Open Composer and authenticate locally.
2. Click the disclosure triangle next to the package source in the sidebar.
3. Click the disclosure triangle next to **Settings**.
4. Control-click (or right-click) the language folder you want to add the .strings file to, and select **Create InstallationCheck.strings** or **Create VolumeCheck.strings**.
5. Click the .strings file to change its contents in the Package Contents pane.
Building Packages from Package Sources

After you have verified the contents of a package source, Composer allows you to build two different kinds of packages: PKGs and DMGs. Each format has advantages depending on the intended use of the package and the tool you use to deploy it.

Once a package source exists in Composer, you can build a PKG or DMG package from the source at any time. You also have the ability to convert from one format to another after a package has been built.

Building a PKG

PKGs can be deployed using almost any deployment tool, such as Apple Remote Desktop (ARD), the Casper Suite, and other client management systems.

The PKG format allows for easy installation by the user. Double-clicking the package opens the Installer application and guides the user through the installation process.

**Note:** PKGs cannot dynamically deploy files in the user’s home directory to user templates when used with the Casper Suite.

By default, Composer builds flat PKGs.

1. Open Composer and authenticate locally.
2. Select the package source you want to build as a PKG from the Sources list in the sidebar.
3. In the toolbar, click **Build as PKG**.
   **Note:** If the **Build flat PKGs** preference is enabled and the package source contains scripts that are not supported by flat PKGs, a dialog will appear. To disable this preference for this package only, click **Build as non-flat PKG**. To build a flat PKG that ignores unsupported scripts, click **Build as flat PKG**.
4. Select a location to save the package and click **Save**.
Building a DMG

When used in conjunction with the Casper Suite, the DMG format allows you to dynamically deploy files and folders to each user that has an account on a computer, as well as the network home directories of currently logged-in users. There is also an option to deploy files and folders to the user template directories, ensuring that any new user receives the correct default environment.

1. Open Composer and authenticate locally.
2. Select the package source you want to build as a DMG from the Sources list in the sidebar.
3. In the toolbar, click Build as DMG.
4. Select a location to save the package and click Save.
Composer Preferences

Composer allows you to manage the following settings:
- Toolbar preferences
- Package preferences
- Cleanup options for OS packages
- Excluded files
- Location of the work directory
- Default bundle identifier

You can access Composer preferences by choosing Composer > Preferences from the menu bar.

This section provides a detailed explanation of Composer preferences.

Toolbar Preferences

Composer allows you to customize the toolbar by adding and removing items.

To add items to the toolbar, Control-click (or right-click) the toolbar and select Customize toolbar, and then drag desired items to the toolbar.

To remove an item from the toolbar, simply drag the item off of the toolbar.
Package Preferences

Composer allows you to manage Package preferences from the pane in the screen shot below.

This pane includes the following preference settings:

**Build flat PKGs**
By default, Composer builds flat PKGs. Flat PKGs consist of a single file and allow for easier and more reliable deployment than non-flat PKGs. You cannot view or change the contents of a flat PKG after it is built.

**Sign flat PKGs**
This option allows you to sign flat PKGs with an installer certificate (.p12) obtained from Apple. Signing PKGs with an installer certificate makes it possible to verify that the PKG was created by an identified developer. It also allows users to install PKGs on computers that have Apple's Gatekeeper feature set to only allow applications downloaded from the Mac App Store and identified developers.

To sign flat PKGs, Composer must be running on OS X v10.7 or later.

Select the **Sign with** option and choose an installer certificate from the pop-up menu. Installer certificates that are located in the login keychain in Keychain Access are displayed in the pop-up menu.

**Note:** The pop-up menu also displays application certificates that are located in the login keychain in Keychain Access. It is important that you use an installer certificate, not an application certificate, to sign flat PKGs.
Remove .DS_Store Files in Common Locations
Enabling this option ensures the removal of any files that disturb the way Finder windows are presented on a user’s computer. Any .DS_Store files necessary to configure views of deployed files and folders will not be removed.

This feature removes .DS_Store files in the following locations:
/ .DS_Store
/Applications/ .DS_Store
/Applications/Utilities/ .DS_Store
/Developer/ .DS_Store
/Library/ .DS_Store
/System/ .DS_Store
/Users/ .DS_Store
/Users/<username>/ .DS_Store
/Users/<username>/<first_level_directory>/ .DS_Store

Scan Images When Building DMGs
Scanning images when building a DMG calculates the checksum and stores it in the DMG.

The checksum is used to ensure proper installation of the DMG package.

Play Sounds
Composer plays a sound each time a package source is created or deleted.

Reveal in Finder when done
When this option is enabled, Composer reveals newly built packages in a Finder window.

Exclusion List
The exclusion list allows you to specify files and folders that should be ignored when creating a package using a snapshot or file system monitoring.

To view the exclusion list, click Exclusion List in the toolbar. A list of common files and folders is specified by default.
To add and remove files, use the **Add (+)** and **Delete (–)** buttons at the bottom of the list.

**Advanced Preferences**

Composer allows you to manage some advanced preferences from the pane in the screen shot below.

This pane includes the following preference settings:

**Work Directory**

When Composer creates a package source, it copies files to a work directory. This work directory must have privileges enabled.

To change this directory, click **Change**, or hold down the Option key when you open Composer.

**Default Bundle Identifier**

The default bundle identifier is used when creating the `info.plist` file for a new package source. For example, if the default bundle identifier is “com.jamfsoftware”, and you create a package source named “Composer”, the bundle identifier for the package source is “com.jamfsoftware.composer”.

![Advanced Preferences](image.png)