

Java Platform, Standard Edition

Advanced Management Console User's Guide



2.18
F37469-01
January 2021

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

F37469-01

Copyright © 2014, 2021, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

| | | |
|----------|---|------|
| | Preface | |
| | Audience | vii |
| | Documentation Accessibility | vii |
| | Related Documents | vii |
| | Conventions | viii |
| 1 | What's New in the Advanced Management Console | |
| 2 | Introduction to Advanced Management Console | |
| | About Advanced Management Console | 2-1 |
| | Starting the Advanced Management Console User Interface | 2-2 |
| 3 | Desktop Management | |
| | About Desktops | 3-1 |
| | Desktops Tab | 3-1 |
| | Views for Desktops | 3-2 |
| | Filters for Desktop Properties | 3-2 |
| | Deployment Rule Set Distribution | 3-3 |
| | Generating Reports for Desktops | 3-3 |
| | Setting the Display Option for Desktop Reports | 3-3 |
| | Setting Filters for Desktop Reports | 3-4 |
| | Exporting Desktop Reports | 3-4 |
| | Pushing a Deployment Rule Set | 3-5 |
| | Enabling or Disabling Agent Auto Update | 3-6 |
| | Enabling or Disabling Java Auto Update | 3-7 |
| | Desktop Properties | 3-7 |
| | Web-Enabled JREs | 3-8 |
| | Desktop Properties Shared With Advanced Management Console Server | 3-9 |
| | Filter Criteria for Desktops | 3-9 |

4 Java Usage

| | |
|--|-----|
| About Tracking Java Usage | 4-1 |
| Java Usage Tab | 4-1 |
| Views for Java Usage | 4-2 |
| Filters for Usage Information | 4-2 |
| Generating Reports for Java Usage | 4-3 |
| Updating Application Names | 4-4 |
| Exporting Java Usage Reports | 4-4 |
| Java Usage Information | 4-5 |
| Filter Criteria for Java Usage Information | 4-6 |
| Java Usage Record Counters | 4-7 |
| Java Usage Tracker Configuration on Managed Desktops | 4-8 |
| Modifying Advanced Management Console Server Host Name | 4-8 |
| Tracking Managed JREs in Agents | 4-8 |

5 Java Runtime Environment Management

| | |
|---------------------------------------|-----|
| About the JRE Management Architecture | 5-1 |
| Installing JRE | 5-2 |
| Installing a Non-Enterprise JRE | 5-3 |
| Uninstalling JREs | 5-5 |
| Status | 5-6 |

6 Installer Configuration

| | |
|--|-----|
| About Installer Configurations | 6-1 |
| Adding a Java Version | 6-2 |
| Adding an Installer Configuration | 6-3 |
| Editing an Installer Configuration | 6-3 |
| Deleting an Installer Configuration | 6-4 |
| Applying a Configuration to an Installer File | 6-4 |
| Exporting an Installer Configuration to a File | 6-5 |
| Installer Configuration Attributes | 6-6 |
| Installer Configuration Properties | 6-6 |

7 User Management

| | |
|---------------------|-----|
| About User Accounts | 7-1 |
| Views for Users | 7-1 |

| | |
|--------------------------------------|-----|
| User Table Details | 7-2 |
| User Properties | 7-2 |
| Creating User Accounts | 7-2 |
| Editing User Accounts | 7-3 |
| Changing the Account Password | 7-3 |
| Resetting the Admin Account Password | 7-4 |
| Password Rules | 7-4 |
| Deleting User Accounts | 7-5 |
| User Permissions | 7-6 |

8 Agent Configuration

| | |
|--|-----|
| Configuring Advanced Management Console Agent Proxy Settings | 8-1 |
| Configuring Agent Intervals | 8-1 |
| Agent Update Initiation | 8-2 |

9 Other Settings

| | |
|---|-----|
| Customizing Java Usage Tracker Properties | 9-1 |
| Server Settings | 9-2 |

10 Rule Sets and Rules Management

| | |
|--|-------|
| About Deployment Rule Sets | 10-1 |
| Rule Sets Tab | 10-2 |
| Managing Rules and Rule Sets | 10-2 |
| Managing Rule Sets | 10-3 |
| Adding a Rule Set | 10-3 |
| Editing a Rule Set | 10-4 |
| Deleting a Rule Set | 10-7 |
| Exporting a Rule Set | 10-7 |
| Signing a Rule Set | 10-8 |
| Setting Default Deployment Rule Set | 10-9 |
| Viewing Relationships between Rule Sets and Applications | 10-9 |
| Managing Rules | 10-10 |
| Creating a Rule | 10-10 |
| Editing a Rule | 10-10 |
| Deleting a Rule | 10-11 |
| Rule Properties | 10-11 |
| Deploying Rule Sets | 10-12 |

11 Desktop Groups Configuration

| | |
|-------------------------------------|------|
| About Desktop Groups | 11-1 |
| About Mapping Files | 11-2 |
| Views for Desktop Groups | 11-2 |
| Desktop Group Table Details | 11-3 |
| Desktop Group Property Details | 11-3 |
| Creating a Desktop Group | 11-4 |
| Updating an Existing Desktop Group | 11-5 |
| Viewing Desktops in a Desktop Group | 11-5 |
| Deleting a Desktop Group | 11-6 |
| Desktop Group Properties | 11-6 |

12 Accessibility in Advanced Management Console

| | |
|---------------------|------|
| Screen Readers | 12-1 |
| Keyboard Access | 12-1 |
| Keyboard Activation | 12-1 |
| Keyboard Focus | 12-2 |
| Keyboard Navigation | 12-2 |
| List View | 12-2 |
| Tab Bars | 12-3 |

A Advanced Management Console Samples

Preface

The Advanced Management Console User's Guide provides information about using the Advanced Management Console to create deployment rules and rule sets, and to monitor the Java applications that are run in your enterprise.

The Advanced Management Console is available to enterprise customers within [My Oracle Support](#).

Note:

The Advanced Management Console requires a commercial license for use in production. To learn more about commercial features and how to enable them, see [Oracle Java SE Advanced & Suite Products](#).

Audience

This document is intended for system administrators who are responsible for managing the Java desktop environment in their enterprise. Readers are expected to know the process for distributing software to computers in their enterprise and have some knowledge of the Deployment Rule Set feature.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

- *Advanced Management Console Installation and Configuration Guide*
- Information about [Java Platform, Standard Edition \(Java SE\) 8](#)
- Information about the Deployment Rule Set feature is available at [Deployment Rule Set](#) in the *Java Platform, Standard Edition Deployment Guide*.

- Information about the Java Usage Tracker is available at [Java Platform, Standard Edition Usage Tracker Overview](#).

Conventions

The following text conventions are used in this document:

| Convention | Meaning |
|-----------------|--|
| boldface | Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary. |
| <i>italic</i> | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| monospace | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

1

What's New in the Advanced Management Console

The Advanced Management Console (AMC) offers system administrators greater control in managing Java version compatibility and security updates for desktops within their enterprise.

See [What's New In Advanced Management Console](#) for descriptions of changes and new features in this and other releases of the Advanced Management Console .

2

Introduction to Advanced Management Console

The Advanced Management Console is a feature of Oracle Java SE Advanced. The Advanced Management Console enables system administrators to monitor and manage the use of Java technology in their enterprise. The Introduction to Advanced Management Console topic includes the following sections:

- [About Advanced Management Console](#)
- [Starting the Advanced Management Console User Interface](#)

About Advanced Management Console

The Advanced Management Console provides system administrators with an insight into the Java applications that their users run and the versions of the Java Runtime Environment (JRE) that are used. Administrators can use the Advanced Management Console to provide some control over the use of Java technology on desktops in their enterprise.

The Advanced Management Console provides the following capabilities:

- Collection of information about Java applications that are run in the enterprise
- Automated discovery of all installed versions of Java on desktops that the Advanced Management Console manages
- Web-based analytics for data collected and for remote management
- Management and distribution of deployment rule sets
- Configuration of the MSI file for installing JREs

This guide contains the following topics that describe the capabilities of the Advanced Management Console :

- [Desktop Management](#)
- [Java Usage](#)
- [Java Runtime Environment Management](#)
- [Installer Configuration](#)
- [Rule Sets and Rules Management](#)
- [User Management](#)
- [Desktop Groups Configuration](#)
- [Advanced Management Console Samples](#)

Starting the Advanced Management Console User Interface

The Advanced Management Console provides a browser-based user interface (UI). You must have a valid user account to log in.

If the Advanced Management Console is not yet installed, then see *Installing and Configuring Advanced Management Console* in the *Advanced Management Console Installation and Configuration Guide*. At least one administrator account must exist.

To start the Advanced Management Console UI:

1. Enter `https://host-name:port-number/amcwebui/login.html` in the browser, where *host-name* is the DNS name of the WebLogic server that hosts Advanced Management Console and *port-number* is the listen port of the WebLogic Server.

The browser must be set to allow cookies.

If you are using the Internet Explorer, then make sure that **Display Intranet Sites in Compatibility View** is not selected in Compatibility View Settings.

2. Enter your login ID and password.

You must have an existing account to log in. The login ID is typically your email address.

3. Click **Login** to display the Home tab of the Advanced Management Console .



Note:

Users are automatically logged out after a preset interval of inactivity.

3

Desktop Management

The Advanced Management Console provides administrators with information about how Java technology is used in their enterprise. Through the Advanced Management Console , administrators can determine such things as how many computers are running an insecure version of Java, what versions of the JRE are installed on enterprise computers, and what deployment rule sets are active in the enterprise. The Advanced Management Console also enables administrators to push deployment rule sets to managed computers.

This topic includes the following sections:

- [About Desktops](#)
- [Desktops Tab](#)
- [Exporting Desktop Reports](#)
- [Pushing a Deployment Rule Set](#)
- [Enabling or Disabling of Agent Auto Update](#)
- [Enabling or Disabling Java Auto Update](#)
- [Desktop Properties](#)
- [Filter Criteria for Desktops](#)
- [JRE Security Baseline](#)

About Desktops

Desktops in the Advanced Management Console represent the client computers in an enterprise. Information about the desktops that are managed by the Advanced Management Console is shown in the Desktops tab and the Status tab.

For a desktop to be managed by the Advanced Management Console , the Advanced Management Console agent must be installed on the desktop. The agent gathers the information about the desktop and sends it to the central server. The agent also processes the requests to install a deployment rule set on the desktop. See *Advanced Management Console Agent Installation and Configuration* in the *Advanced Management Console Installation and Configuration Guide*.

A report of retired desktops and rule set failures is available from the Status tab.

Desktops Tab

The Desktops tab of the Advanced Management Console shows information about the desktops that are managed by the Advanced Management Console . Filters are available to get reports about selected desktop properties. The ability to push Deployment Rule Sets to desktops and export desktop information to an HTML file or comma-separated values (CSV) file is also provided.

Views for Desktops

The table in the Desktops tab shows the properties for desktops that are managed by the Advanced Management Console . The properties view provides more detailed information for each desktop. Depending on the display option selected, information can also be shown as a pie chart or a bar chart.

The table view is the default view. The table view is available for all display options. However the properties that are shown are dependent on the display option selected. Click the arrow that appears in the column heading to sort the data by the values in that column. Use the navigation bar below the table to view additional pages when the number of desktops exceeds the page size.

The properties view is available only when **Desktop** is selected as the display option. Click the column heading in the Installed JREs table or Command Queue table to sort the data by the values in that column. Use the navigation bar to scroll through the properties for other desktops that match the filter criteria.

The pie chart and bar chart are available when something other than **Desktop** is selected as the display option. Click a segment from the pie chart or a bar from the bar chart to see the desktops that match the selected value.

Filters for Desktop Properties

The display option and the filter criteria in the Desktops tab determine what information is shown for the desktops managed by Advanced Management Console .

The default display option is **Desktop**, which shows the properties for each managed desktop in a table. The other choices for the display option show the values for the selected option and the number of desktops that match each value. For example, selecting Java Runtime Environment (JRE) Major Version shows every major version of the JRE that is installed on at least one desktop and the number of desktops on which it is installed.

The filter criteria further refine the information shown. The choices available for the criteria are based on the properties of the desktops. For example, if the only major JRE versions found across all managed desktops are 1.7.0 and 1.8.0, then 1.6.0 is not shown as a choice for the JRE Major Version criterion.

You can use the display option and filter criteria together to get answers to questions similar to the ones in the following list:

- Which desktops are running insecure versions of the JRE?
Set **Display** to **Desktop**. Add the criterion **JRE Security**, and set it to **some JREs are insecure**. The table shows the list of desktops that have at least one insecure JRE installed.
- How many desktops are running versions of JRE 7?
Set **Display** to **JRE Major Version**. See the number in the Hosts column for the row showing JRE Major Version 1.6.0.
To show only the data for version 1.7.0, add the criterion **JRE Major Version** and set it to **1.7.0**. If 1.7.0 is not shown in the table or in the list of major versions available, then no desktops are running a version of JRE 7.
- Which deployment rule sets are desktops using?

Set **Display** to **Active Rule Set**. The table shows the list of rules sets that are active and the number of desktops for each rule set.

- Which desktops are using the rule set *rule-set-name*?

Set **Display** to **Desktop**. Add the criterion **Active Rule Set** and set it to the name of the rule set that you are interested in. The table shows the list of desktops that are using the selected rule set.

Deployment Rule Set Distribution

A deployment rule set helps you manage the applications that are allowed to run in your enterprise. The Desktops tab in Advanced Management Console contains an option for pushing a deployment rule set to selected desktops.

The Advanced Management Console agent is used to install the rule set on a desktop. Pushing a rule set sends a command to the agent. The next time the agent contacts the Advanced Management Console server, the agent processes the command. View the status of the rule set by selecting the **Rule Set Status** display option or setting the **Rule Set Status** filter criteria.

Generating Reports for Desktops

Reports are used to answer questions about desktops that are managed by Advanced Management Console and about the JRE versions and deployment rule sets installed on those desktops. Set the display option and filter criteria in the Desktops tab to generate the type of report that you want. Report data can be exported to an external file.

Depending on the filters that are used, reports are available as a table, pie chart, or bar chart. See [Views for Desktops](#).

Reports about retired desktops or desktops with rule set failures are available from the **Status** tab.

Setting the Display Option for Desktop Reports

Set the display option in the Desktops tab to show how many desktops managed by Advanced Management Console match each value for a specific property.

To set the display option:

1. In the Advanced Management Console, click the **Desktops** tab.
2. Select a property to see the report for that property.

The following examples show how the display option is used:

- To show the JRE versions installed on desktops and the number of desktops that have each version installed, set **Display** to **JRE Full Version**. The first column in the table shows the JRE versions that are found. The second column shows how many desktops have that version installed.
- To show the rule sets that are active on desktops and the number of desktops that have each rule set installed, set **Display** to **Active Rule Set**. The first column in the table shows the names of the active rule sets that are found. The second column shows how many desktops have that rule set installed.

- If a desktop group exists, then show the number of desktops associated with each value for a desktop group by setting **Display** to the name of a desktop group.

Setting Filters for Desktop Reports

Use filters in the Desktops tab to show only desktops managed by Advanced Management Console that match specific values for selected desktop properties.

To filter the information by a desktop property:

1. In Advanced Management Console , click the **Desktops** tab.
2. Click **Add Criteria** and select one or more filters from the list.
3. For each filter selected, select or enter the value to match.

Filters that provide a list of values show only values that are present in at least one desktop. For example, the JRE Major Version filter shows only major versions that are installed on at least one desktop. For filters that do not provide a list of values, such as First Name and Last Name, enter the string to match and press Enter. Wildcards are not currently supported.

Some filters require a secondary filter. The secondary filter is automatically shown when the primary filter is selected. For example, if the filter criterion **OS Version** is selected, then the **OS Family** filter is also displayed.

To see which desktops match the filter criteria, set **Display** to **Desktop**.

Exporting Desktop Reports

Data from the desktop reports that are generated by Advanced Management Console can be exported to an external file. Filter criteria is used to choose the desktops that are included in the exported data.

To export data for desktops:

1. In the Advanced Management Console , click the **Desktops** tab.
2. Make sure that **Display** is set to **Desktop**.
The **Other Actions** button is available only with the **Desktop** display option.
3. (Optional) Set the filter criteria to show only the desktops that you want included in the exported data.

Click **Add Criteria** and set the values for each filter that you select. Only information that matches the criteria is exported.

If no filters are set, then all desktops are included in the exported data.

4. Click **Other Actions** and then select **Export Data**.

The Export Data window is shown.

5. Choose the output format:
 - HTML: The generated file contains the data in a table with HTML formatting.
 - CSV: The generated file contains the data in text fields that are separated by the value separator that you select.
 - JSON: The generate file contains the data in machine-readable JSON format.

6. Click **Confirm**.

The browser prompts you to either save or view the data. Depending on the format selected, the default file name is `amc2-desktops_YYYY-MM-DD_HH-MM.csv` or `amc2-desktops_YYYY-MM-DD_HH-MM.html`, where `YYYY-MM-DD_HH-MM` is the server-side time stamp of when the file was created.

The following data is exported for each application that meets the filter criteria.

- Operating system name
- Operating system version
- Operating system architecture
- Owner name
- Owner email address
- Time stamp of last contact
- Host name
- IP address
- Name of active rule set
- Agent version
- Number of secure JRE versions installed on the desktop
- Number of insecure JRE versions installed on the desktop
- Desktop groups and the value of the group property for any group that includes the desktop
- Latest Usage column that indicates timestamp of most recent usage for the respective Java version

Pushing a Deployment Rule Set

A deployment rule set provides rules for allowing or blocking Java applications based on the criteria set in the rule. The Advanced Management Console enables you to distribute signed deployment rule sets to the desktops in your enterprise. When the Advanced Management Console pushes a signed `DeploymentRuleSet.jar` file to a desktop, the Advanced Management Console agent edits the `Java deployment.properties` on that desktop to point to a specific truststore that holds the certificates from this `DeploymentRuleSet.jar` file. By default, the `deployment.properties` file is located at: `C:\Windows\Sun\Java\Deployment\.`

If your desktop already contains a `deployment.properties` file with the `deployment.user.security.trusted.cacerts` property set to a specific location, then Advanced Management Console overwrites that property value.

Note:

A signed deployment rule set must be available in Advanced Management Console . Otherwise, the option to push a deployment rule set is not enabled.

To push a deployment rule set:

1. In Advanced Management Console , click the **Desktops** tab.
2. Make sure that **Display** is set to **Desktop**.
The **Push Deployment Rule Set** button is available only with the **Desktop** display option.
3. (Optional) Set the filter criteria to show the subset of desktops to which you want to push the rule set.
4. (Optional) Select the target desktops by selecting the check box for the desktop.
If no desktops are selected, then the target is all desktops that match the filter criteria that is set.
5. Click **Push Deployment Rule Set** to display the Push Deployment Rule Set dialog
6. Choose one rule set from the list provided.
Only signed rule sets can be distributed. If the rule set that you want to push is not in the list, then the rule set is currently unsigned.
7. Choose the target.
 - To push only to selected desktops, select **Selected Desktops**.
 - To push to all desktops matched by the filter criteria that is set, select **All Filtered Desktops**.
8. Click **Push**.

The next time the agent on the target desktops contacts the Advanced Management Console server, the agent downloads and installs the rule set. View the status of the rule set by selecting the **Rule Set Status** display option or setting the **Rule Set Status** filter criteria.



Note:

A rule set that is altered on a desktop after being deployed from the Advanced Management Console is no longer recognized by the Advanced Management Console . Properties for any desktop with an altered rule set are updated to indicate that the desktop does not have an active rule set.

Enabling or Disabling Agent Auto Update

The Advanced Management Console provides an option in the **Configuration** tab to enable or disable the agent auto update.

To enable or disable the agent auto update:

1. In the Advanced Management Console , click the **Configuration** tab.
2. Click the **Agent Settings** sub tab.
3. Click **Edit**.
4. Select or deselect the **Agent Auto Update** check box under Agent Action Intervals and Units to enable or disable agent auto update.
5. Click **Save**.

Enabling or Disabling Java Auto Update

Java has a mechanism which checks for and installs new versions of Java in the background. As the Advanced Management Console provides finer-grained control of Java Runtime Environment (JRE) management on desktops, an option is provided in the **Desktop** tab to enable or disable Java Auto Update on each desktop.

To enable or disable Java auto update:

1. In the Advanced Management Console , click the **Desktop** tab.
2. Ensure that the **Desktop** is selected in the **Display** drop-down list.
The **Other Actions** button is available only with the **Desktop** display option.
3. Ensure that the **Table** icon is selected.
4. (Optional) Set the filter criteria to show only the desktops for which you want to enable or disable the auto update.

- a. Click **Add Criteria** .
- b. Select the filters and set the values for each filter that you select.

The agent auto update is enabled or disabled only for the desktops that match the criteria. If no filters are set, then the agent auto update is enabled or disabled for all desktops.

5. Click **Other Actions** and then select **Set Java Auto Update for Desktop(s)** to display the Set Java Auto Update for Desktop(s) dialog.
6. Select the target desktops by selecting either of the following options:
 - **Selected Desktops**: Shows the number of desktops selected.
 - **All Filtered Desktops**: Shows the number of filtered desktops included.
7. Select **Enabled** to enable Java auto update or **Disabled** to disable it.
8. Click **Confirm**.

The Java Auto Update mechanism is now enabled (or disabled) on the selected desktops.

Desktop Properties

The Advanced Management Console agent collects information about the desktops managed by Advanced Management Console . The properties describe such things as the JRE versions, the operating system, and the deployment rule set for each desktop.

The following table describes the desktop properties that are shown when the display option is set to **Desktop**. Properties that are shown only in the properties view are indicated by an X in the Properties View Only column.

| Property | Description | Properties View Only | Optional |
|-----------------|--|----------------------|----------|
| Active Rule Set | Name of the active rule set, if any | | X |
| Architecture | Architecture of the JRE, for example, 32-bit | X | |

| Property | Description | Properties View Only | Optional |
|-----------------|--|----------------------|----------|
| Command Queue | List of commands executed for the desktop, the status of each command, and any additional details, such as the name of the deployment rule set that was pushed | X | |
| First Name | First name of the registered user of the desktop | X | X |
| Host Name | Host name of the desktop | X | |
| IP Address | IP address of the desktop | X | |
| Java Vendor | Name of the vendor that distributed the JRE | X | |
| Java Versions | List all web-enabled JREs found on the desktop. | | X |
| Last Contact | Time stamp of the last contact with the agent | | |
| Last Name | Last name of the registered user of the desktop | X | X |
| OS | Operating system that the desktop is running | | |
| OS Architecture | Architecture of the operating system that the desktop is running, for example, 64-bit | X | |
| OS Family | Operating system for the desktop | X | |
| Other JREs | Lists all other JREs (not web-enabled) found on the desktop. | | |
| Owner Email | Email for the registered user of the desktop | | X |
| Secure | Flag that indicates if the JRE is a secure version. A check mark means that it is secure. | X | |
| Path | Path to the location of the JRE. If the JRE is in more than one location, then all paths are shown, separated by semicolons (;). | X | |
| Version | Version of the Advanced Management Console agent installed on the desktop | | |

When the display option is set to something other than **Desktop**, the table shows the values for the selected [filter criteria for desktops](#) and the number of desktops that match each value.

Web-Enabled JREs

The Advanced Management Console agents can detect whether or not the Java Runtime Environments (JREs) are web enabled. If the JREs are web enabled, then they can be used to run applets and Java Web Start applications.

The Advanced Management Console can detect what JREs are actually used by Java Plugin or the Java Web Start to run Rich Internet Applications (RIAs). These web-enabled JREs are displayed in the **Java Versions** column of the [Desktop Properties](#) and in the Web Enabled JREs table in the Properties view. To view the Web Enabled JREs table, in the **Desktops** tab, select a Desktop, and click the **Properties** icon. Details of the selected desktop are displayed in the following tables: **Web Enabled JREs**, **Installed JREs**, and **Command Queue**. All the other JREs are listed in the **Other JREs** column of the **Desktop** tab.

You can also view the web-enabled JREs when you select either the JRE Full Version or the JRE Major Version from the **Display** drop-down list in the Desktop tab.

Desktop Properties Shared With Advanced Management Console Server

When the Advanced Management Console agent registers, it sends some information (Desktop Properties) to the Advanced Management Console server. This is information pertaining to both the Java Usage as well as the Java Runtime Environment (JRE).

The agent sends the following information about itself to the server:

- First Name (Optional)
- Last Name (Optional)
- Email (Optional)
- Heartbeat: Current time stamp of the agent trying to register.
- IP Address
- Host Name
- OS Architecture, for example 64-bit
- OS Version, for example, 10.9.5
- OS Name, for example, macOS

The values for First Name, Last Name, and the Email are the values entered in the `AMCUser.properties` file, which is the properties file of the Advanced Management Console agent. If the properties file is absent or the agent chooses to leave some of these values empty, then the values of the three properties are reported as null. Once the agent starts running, with the usage tracking record configured, details, such as the usage tracking records for webstart applications, applets — both jnlp and html, and the standalone applications are collected and shared periodically with the Advanced Management Console server.

The agent also periodically scans for JREs on the Desktop and shares the following information with the server:

- Java Version (both major and minor)
- Architecture
- Vendor
- Path where the JRE is installed
- Type of installation
- Whether the JRE is web enabled

Filter Criteria for Desktops

The filter criteria available in the Desktops tab is used to generate reports about the desktops managed by Advanced Management Console . The filters and the values chosen provide administrators with specific information about the desktops and JRE versions in use in the enterprise.

The following table describes the filters that are available for desktops, and indicates if the criteria is set as the display option or as a filter. For filters, the valid values are provided in the drop-down list, except where noted in the description.

| Criteria | Description | Display Option | Filter Criteria |
|-----------------------|---|----------------|-----------------|
| Desktop | List of desktops managed by Advanced Management Console | X | |
| JRE Major Version | Major version of the JRE, such as 1.7.0 or 1.8.0. | X | X |
| JRE Minor Version | Version number of the update release for a major release. The JRE major version filter is also shown when this filter is selected. | | X |
| JRE Full Version | Major and minor version of the JRE, such as 1.7.0_67 or 1.8.0_40 | X | |
| JRE Architecture | Architecture of the JRE, such as 32 for the 32-bit JRE | X | X |
| JRE Security | Security status based on the JRE security baseline . Set the filter to show desktops where all installed JREs are secure, all installed JREs are insecure, or some installed JREs are insecure. | | X |
| OS Family | Operating system for the desktop | X | X |
| OS Version | Version of the operating system. The OS family filter is also shown when this filter is selected. | | X |
| OS (Family + Version) | Family and version of the operating system | X | |
| OS Architecture | Architecture of the operating system | X | X |

| Criteria | Description | Display Option | Filter Criteria |
|------------------|--|----------------|-----------------|
| Last Contact | <p>The following types of desktops listed in this drop-down list: Retired, Online, and Offline. Set the filter to display the desktop type:</p> <ul style="list-style-type: none"> Retired: a desktop that hasn't contacted the Advanced Management Console server for more than a month. It is a desktop that contacts the Advanced Management Consoleagent and not the server. It may happen that a desktop is actually on, but for some reason the agent can't contact the server, and such a desktop is shown either as retired, or as offline. See Unregistering Advanced Management Console Agents and Usage Tracker Properties in the <i>Advanced Management Console Installation and Configuration Guide</i> for instructions used in removing "Retired" desktops. Offline: a desktop that hasn't contacted the Advanced Management Console server for more than a day but less than a month. Online: desktops that have contacted the server in the last 24 hours. | | X |
| | <div style="border-left: 2px solid #0070C0; border-right: 2px solid #0070C0; border-bottom: 2px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>In the future releases of the Advanced Management Console, the values (1 month or 1 day) can be changed, or a way to configure them may be provided in the Advanced Management Console UI.</p> </div> | | |
| Owner First Name | First name of the registered user of the desktop. Enter the name to match. | | X |
| Owner Last Name | Last name of the registered user of the desktop. Enter the name to match. | | X |
| Owner Email | Email of the registered user of the desktop. Enter the email address to match. | | X |
| Active Rule Set | Name of the active rule set installed on the desktop | X | X |
| Rule Set Status | Status of the request to push a rule set to the desktop | X | X |

| Criteria | Description | Display Option | Filter Criteria |
|----------------------|---|----------------|-----------------|
| Agent Version | Version of the Advanced Management Console agent that is running on the desktop | | X |
| <i>Desktop-group</i> | Filter for each desktop group that is defined, if any. <i>Desktop-group</i> is the name of the group. | X | X |

JRE Security Baseline

The JRE security baseline identifies the latest version of the JRE that contains security-related changes. A baseline is identified for each JRE family. The Status tab of Advanced Management Console shows the current security baseline.

The Java Security Baseline section of the Status tab shows the following information:

- **URL:** Location from which Advanced Management Console downloads information about the security baseline version
- **Baseline Date:** Date and time that the security baseline at the location identified by the **URL** field was last updated
- **Baseline:** The security baseline version for each JRE family
- **Last Check:** Date and time that information about the security baseline was last checked by the Advanced Management Console

4

Java Usage

The Advanced Management Console provides administrators with information about the Java applications that are run in their enterprise and the versions of the Java Runtime Environment (JRE) that are used to run them. Through the Advanced Management Console, administrators can determine such things as which version of the JRE is used to run corporate applications and how many browser-based applets are being run in the enterprise.

This topic contains the following sections:

- [About Tracking Java Usage](#)
- [Java Usage Tab](#)
- [Generating Reports for Java Usage](#)
- [Updating Application Names](#)
- [Exporting Java Usage Reports](#)
- [Java Usage Information](#)
- [Filter Criteria for Java Usage Information](#)
- [Java Usage Record Counters](#)
- [Java Usage Tracker Configuration on Managed Desktops](#)

About Tracking Java Usage

Java Usage Tracker is a feature of the JRE. When enabled on a computer, Java Usage Tracker (JUT) tracks the use of applications and JREs on that computer. Advanced Management Console collects the information from the Usage Tracker and presents it in reports.

For the Advanced Management Console to collect information, the Java Usage Tracker must be enabled on desktops in the enterprise. When you install the Advanced Management Console Agent on a desktop, the Java Usage Tracker is enabled. You can also manually enable the Java Usage Tracker on desktops that do not support the Advanced Management Console Agent.

See *Java Usage Tracker Setup for Advanced Management Console* in the *Advanced Management Console Installation and Configuration Guide*.

The Status tab of the Advanced Management Console shows the number of records that were processed successfully or unsuccessfully. See [Java Usage Record Counters](#).

Java Usage Tab

The Java Usage tab of Advanced Management Console shows the applications that are running on desktops in your enterprise and the versions of the Java Runtime

Environment (JRE) that are being used. Filters are available to get reports about the applications and JREs.

The information is shown in the format of a table, pie chart, or bar chart. See [Views for Java Usage](#).

The [filters](#) determine what information is shown.

From this tab, Java Usage Tracker data can be exported to an HTML file or a comma-separated values (CSV) file.

Views for Java Usage

Information in the Java Usage tab of the Advanced Management Console is available in table format, as a pie chart, and as a bar chart, as depicted by table, pie chart, and bar chart icons respectively. The display option and filter criterion are used to choose the type of information shown.

The table view is the default view. Click the arrow that appears in the column heading to sort the data by the values in that column. Use the navigation bar below the table to view additional pages when the number of entries exceeds the page size. The **Details** and **Properties** icons are enabled when you select an application in the Display table. These two icons are grayed out if no application is selected. The **Properties** icon gets enabled when you select a non-web application and the both the icons are enabled only when you select a web-based application.

The categories shown for the pie chart and the horizontal axis of the bar chart are based on the option selected for **Display**. For example, if **Application Security** is selected, then the categories are **Sandbox** and **All permissions**. The count shown in the pie chart segments and the vertical axis of the bar chart is based on the option selected for **Counter**. If **Counter** is set to **Hosts**, then the charts show the number of hosts in each category.

Filters for Usage Information

The display option and filter criteria in the Java Usage tab of the Advanced Management Console determine what type of information is shown.

The default display option is **JRE Full Version**. This option shows statistics for the applications that were run with the JRE versions that are shown. The display option sets the type of information that is shown in the first column of the table view and the categories for the pie chart and bar chart.

The [filter criteria](#) further refine the information shown. The choices available for each criterion are based on the values reported by Java Usage Tracker. For example, if the only major JRE versions used for all applications that are tracked are 1.7.0 and 1.8.0, then 1.6.0 is not shown as a choice for the JRE Major Version criteria.

You can use the display option and filter criteria together to get answers to questions similar to the ones in the following list:

- Which applications are running with an insecure version of the JRE?
Set **Display** to **Application**. Add the criterion **JRE Security Baseline** and set it to **some JREs are insecure**.
- How many Java Web Start applications require access to the user's system?

Set **Display** to **Application Type**. Add the criterion **Application Security** and set it to **All Permissions**. Add the criteria **Application Type** and set it to **WebStart Application**.

The next example shows how to see which applications require access.

- Which Java Web Start applications require access to the user's system?

Set **Display** to **Application**. Add the criterion **Application Security** and set it to **All Permissions**. Add the criterion **Application Type** and set it to **WebStart Application**.

- What operating systems are being used to run applications?

Set **Display** to **OS Family**. No additional filters are needed.

- What are the applications, types of applications, and the JRE versions discovered after a specified date?

Add the criterion **First Use After** and set the required date and time to view all the applications or JREs that were discovered after the date and time selected.

- How to list the applications that use Java Commercial features?

Set **Display** to **Application**. Add the criterion **Java Commercial Feature**. Select the required filter option **FlightRecorder**, **UseAppCDS**, or both to display relevant applications that use Java Commercial features.

Generating Reports for Java Usage

Reports are used to answer questions about how Java is used in your enterprise. These reports use the information generated by Java Usage Tracker and collected by the Advanced Management Console Agent. Report data can be exported to an external file.

To generate a report:

1. In the Advanced Management Console , click the **Java Usage** tab.
2. Set **Display** to the type of information that you want.

The values for the type of information selected are shown as the first column of the table view, the categories for the pie chart, or the horizontal axis of the bar chart.

3. To further filter the information, click **Add Criteria** and select one or more filters from the list.
4. For each filter selected, select or enter the value to match.

Filters that provide a list of values show only values that are present for at least one application. For filters that do not provide a list of values, such as Application, type the string to match and press Enter.

Some filters require a secondary filter. The secondary filter is automatically shown when the primary filter is selected. For example, if the filter criterion **JRE Minor Version** is selected, then the **JRE Major Version** filter is also shown.

5. Choose the format in which you want to view the information.

Updating Application Names

In the **Java Usage** tab of the Advanced Management Console , you can select an application and set a name (an alias) for it. Applications are uniquely identified by locations, which are different for various application types. They can be, for example, class names, web page URLs, JNLP URLs, or jar file names. However, location names are often long and/or less understandable. In addition, it is also possible for a single application to have multiple locations that look similar or share a common pattern. For this reason, setting an alias makes an application appear more readable and also enables the merging of multiple locations into a single application. More specifically, for every application in the Java Usage tab, you can set an alias to simplify the application name. For example, `com.sun.deploy.panel.ControlPanel` can be named `Java Control Panel`.

To update (or simplify) application names:

1. In the Advanced Management Console , click the **Java Usage** tab.
2. Set **Display** to the type of information that you want. To update application names, ensure to set the **Display** type to Applications.

The **Update Name** button is displayed only when the Display type is set to Applications.

3. Select an Application that you want to update in the **Application** table.

The **Update Name** button becomes enabled.

4. Click **Update Name** to display the Update Application Name dialog box.
5. Enter the new application name in the **Application Name** field.
6. Enter a pattern in the **Location Pattern** field. You can use wild cards for the pattern: an asterisk (*) substitutes zero or any characters; an underscore (_) substitutes a single character.

Note that the merging is enabled for standalone applications only.

7. Click **Next** to review the details under **Review and Submit**.

At this step, you can review the new name of the application, and in case of standalone applications, a list of locations that are going to be merged into a single application.

8. Click **Submit**.

The application name gets updated and message is displayed indicating that the application was successfully updated.

Exporting Java Usage Reports

Data from the Java usage reports that are generated by Advanced Management Console can be exported to an external file. Filter criteria is used to choose the applications that are included in the exported data.

To export Java usage data:

1. In Advanced Management Console , click the **Java Usage** tab.

2. (Optional) Set the filter criteria to show only the applications that you want included in the exported data.

Click **Add Criteria** and set the values for each filter that you select. Only information that matches the criteria is exported. The **Display** option does not affect what information is exported.

If no filters are set, all applications are included in the exported data.

3. Click **Export Data**.

The Export Data window is shown.

4. Choose the output format.

- HTML: The generated file contains the data in a table with HTML formatting.
- CSV: The generated file contains the data in text fields that are separated by the value separator that you select.
- JSON: The generated file contains the data in machine-readable JSON format.

5. Click **Confirm**.

The browser prompts you to either save or view the data. Depending on the format selected, the default file name is `amc2-java-usage_YYYY-MM-DD_HH-MM.csv` or `amc2-java-usage_YYYY-MM-DD_HH-MM.html`, where `YYYY-MM-DD_HH-MM` is the server-side timestamp of when the file was created.

The following data is exported for each application that meets the filter criteria. See [Filter Criteria for Java Usage Information](#) for a description of the properties:

- Location
- Type of application
- Application security
- Java version
- Java architecture
- Host name/IP address
- Operating system name
- Operating system version
- Run count
- Timestamp of last run

Java Usage Information

The Java Usage Information is about applications and their Java Runtime Environment (JRE) versions that are used to run them is collected from desktops that have the Advanced Management Console agent installed. This information is shown in the Java Usage tab of Advanced Management Console .

The following table describes the statistics that are shown. All of the statistics, except Path are available in the table view. Select one row (depends on the selected Display, one row can be an application, or an application type, or an OS family) in table view and click the **Properties** icon, the Path information for the table row is shown. The path details for the JRE are displayed immediately below the Hosts details, and

appear in the same place for all display types. Latest usage is not available for the pie chart or bar chart.

| Statistic | Description |
|--------------|---|
| # Apps | Number of applications that meet the filter criteria |
| # Runs | Cumulative number of times that the applications that meet the filter criteria have been run |
| # Hosts | Number of hosts on which the applications that meet the filter criteria are installed |
| # JREs | Number of JREs associated with this row for the chosen display type. For example, if the display type is Applications, then it's the number of JREs used to run the application; similarly, if the display type is OS family, then it's the number of JREs run on that OS family. |
| First Usage | The first time an application or a JRE version was discovered. |
| Latest Usage | The most recent time that an application that meets the filter criteria was run. |
| Path | Full path of the JRE in Java Usage reports. For example: /Library/Application Support/Oracle/Java_AMC/versions/AMC-2.7-b04/java. |

Filter Criteria for Java Usage Information

The filter criteria available in the Java Usage tab of Advanced Management Console are used to generate reports about how Java is used. The filters and the values chosen provide administrators with specific information about the applications in use in the enterprise.

The following table describes the filters that are available, and indicates if each criterion is available as the display option or as a filter. For filters, valid values are provided in the drop-down list, except where noted in the description.

| Criteria | Description | Display Option | Filter Criteria |
|----------------------|--|----------------|-----------------|
| Application Type | Type of application, such as HTML applet or Java Web Start application. | X | X |
| Application | Name or location of the main class, JAR file, or JNLP file, depending on the type of application. Enter the string to match. | X | X |
| Application Security | Type of access required by the application, such as sandbox or all-permissions | X | X |
| JRE Major Version | Major version of the JRE, such as 1.7.0 or 1.8.0 | X | X |
| JRE Minor Version | Version number of the update release for a major release | | X |
| JRE Full Version | Major and minor version of the JRE, such as 1.7.0_67 or 1.8.0_40 | X | |

| Criteria | Description | Display Option | Filter Criteria |
|-------------------------|---|----------------|-----------------|
| JRE Security Baseline | Security status based on the JRE security baseline. See JRE Security Baseline . Set the filter to show statistics for applications that were run with only secure JREs, only insecure JREs, or a mixture of secure and insecure JREs. | | X |
| JRE Architecture | Architecture of the JRE, such as 32 for the 32-bit JRE | X | X |
| OS Family | Operating system on which the application and JRE run | X | X |
| OS Version | Version of the operating system | | X |
| OS Family + Version | Family and version of the operating system | X | |
| Java Commercial Feature | The commercial features such as FlightRecorder and UseAppsCDS that the applications use. | | X |

Java Usage Record Counters

The Advanced Management Console collects Java usage records and processes them to extract the information needed. The Status tab shows the number of records that are processed.

The Java Usage section of the Status tab shows the following information:

- **Accepted Records:** Number of usage records that were processed successfully.
- **Rejected Records:** Number of usage records that couldn't be processed. Possible reasons for rejecting a record can either include a discrepancy between the Java Usage Tracker configuration in the Advanced Management Console and the Java Usage Tracker configuration for a desktop, or a new Java application is using an argument value that conflicts with the existing Java Usage Tracker configuration.

To display details of records:

1. Click **Rejected Records** to display rejected record details, such as IP address, Rejection Reason, and Truncated Java Usage Tracker Record in the JUT Record Rejection Details dialog.
2. Click the **Rejected Records Table** icon to display all the records in a tabular format.
3. Select a record and click the **Rejected Record details** icon to display the details of the selected record. The display of records in the Rejected Records Table can be further refined with filters. You can toggle the checkboxes against each of the filters to select or deselect the filters.
4. If you want to remove all filters, then click **Remove All**.
5. Click **Download Rejected Records File** to open or save the list of rejected records as a CSV file.

 **Note:**

The maximum number of records that gets downloaded in a file is 100,000.

Clear Counters resets the record counters to zero. If records are being rejected, then clearing the counters after attempting to resolve the issue shows if records are no longer being rejected.

Java Usage Tracker Configuration on Managed Desktops

Managed desktops are those desktops, where the Advanced Management Console agents are running and installed. The Advanced Management Console agents configure Java Usage Tracker on managed desktops. This helps you in handling the Java Usage Tracker configuration issues, if in case you have Java Usage Tracker configured with one server and want to switch to Advanced Management Console for Java tracking.

To achieve this configuration, the Advanced Management Console agent places the `usagetracker.properties` file (Java Usage Tracker configuration file) in the appropriate JRE sub directory. For JREs prior to JDK 9, the file is placed in the `lib/management` folder, and for JDK 9, it's the `conf/management` folder. In the Advanced Management Console UI, you can download the `usagetracker.properties` file in the **Settings** sub tab of the **Configurations** tab.

When you modify any of the Java Usage Tracker properties, for example Java Usage Tracker separator, Java Usage Tracker listener port, or Quote Character, and then the Advanced Management Console automatically updates such configuration on all the managed desktops.

Modifying Advanced Management Console Server Host Name

You can modify the hostname that you had specified during the initialization of Advanced Management Console , in case you had entered the host name incorrectly.

To change the server host name:

1. In the Advanced Management Console UI, click the **Configuration** tab.
2. Click **Settings** sub tab, and then click **Edit**.

You can now edit the Hostname. The **Edit** button is replaced by the **Save** and **Cancel** buttons.

3. Enter a new Hostname, and then click **Save**.

The new host name applies to new agents and not to the agents that already exist.

Tracking Managed JREs in Agents

In the **Configurations** tab of the Advanced Management Console UI, you can select the type of managed Java Runtime Environments (JREs), such as standard, private,

installed, enterprise, or web-enabled JREs that you want to track on the agent side, and to exclude specific folders from JRE scanning and tracking.

Based on what you select in the **Configurations** tab, only those JREs are tracked on the agents, which effectively means that the Java Usage Tracker configuration is enabled only on those tracked JREs.

To track managed JREs:

1. In the Advanced Management Console UI, click the **Configuration** tab.
2. Click the **Agent Settings** tab, and then click **Edit**.

The check boxes in the Other Agent Settings section are now enabled, the Exclude Paths list becomes editable. The **Edit** button is replaced by the **Save** and **Cancel** buttons.

3. Select all or any of the following JREs to track:

 **Note:**

By default, all of the check boxes are selected.

- **Installed:** JRE that is currently installed on the agent.
 - **Web Enabled:** Helps in running applets and Java Web Start applications.
 - **Enterprise:** Allows system administrators to quickly and consistently roll out pre-configured Oracle **JRE** updates to Windows systems by using the automation tools.
 - **Standalone:** JRE that doesn't contains tools, such as `tools.jar` or `javac` that are specific to a JDK. The Standalone JRE is sometimes also referred to as a public JRE. It is available to all Java programs, browsers, and libs in this JRE.
 - **Private:** JRE that is installed in the system but is not referred to by default. This could be a copy of either the JRE or the JDK folder from another installed directory.
4. Add or Remove paths from the list.
 - a. To exclude specific folders from the JRE scan and consequently from tracking with the AMC Agent, enter the path for the folder and click **Add**.

The path is added to the list. The maximum number of paths that can be added is 10. The maximum length of a path is 2000 characters. You can enter either Windows or Linux/macOS paths.

When the AMC agent scans a system for a JRE, it will skip the excluded paths and all subdirectories. In particular, the `usagetracker.properties` file will not be put into the JRE directory. If an application is launched using a JRE from an excluded path, the application that is launched will not be recorded.

- b. To re-enable scanning for JREs in specific folders, click the **Remove** link beside the path in the list.

 **Note:**

In macOS Catalina, there is a change in the file system due to which the set of files and folders present in the user directory is displayed in another path as well, such as `/System/Volumes/⟨⟨path⟩⟩`. To avoid reporting duplicates, the path `/System/Volumes/` is excluded from JRE tracking by default on macOS. To include this path, remove the `/System/Volumes/` entry from the **Paths To Exclude From JRE Tracking** field.

5. Click **Save** to save the changes.

The **Save** and **Cancel** buttons disappear and the **Edit** button comes back on the **Agent Settings** tab.

5

Java Runtime Environment Management

The Advanced Management Console agents enables you to install or uninstall the Java Runtime Environment (JRE) — both Enterprise and Non Enterprise from managed desktops. You can also customize a JRE version on Installers tab and select it for installing on targeted desktops. The installed JREs from managed desktops can also be uninstalled for targeted desktops.

Note:

This feature is currently not supported for desktops or servers on Linux platform.

The JRE Management topic consists of the following sections:

- [About the JRE Management Architecture](#)
- [Installing JRE](#)
- [Uninstalling JREs](#)
- [Status](#)

About the JRE Management Architecture

The Java Runtime Environment (JRE) management workflow consists of the following components: User Interface (UI), Server, and agents.

This topic describes the JRE architecture:

- **UI:** The user interface for JRE Management is facilitated through the Desktop and the Status tabs in the Advanced Management Console
 - **Desktops:** In the Desktops tab, select required desktops, where a JRE should be installed or uninstalled, and click **Install JRE** or **Uninstall JRE** respectively.
 - **Status:** In the **Status Tab**, you can see view the details of all the scheduled actions (commands) with information about the number of desktops, where each action is completed, failed, or in progress.
 - **Installer:** In the Installers tab, you can add Java versions and configure them for both enterprise and non-enterprise JREs. Enterprise JREs are similar to .msi packages, which contain both JRE packages and configuration files, while non-enterprise JREs don't contain any configuration files. Non-Enterprise JREs cannot be configured. They are used without configuration.
- **Server/Database:** The information about each [install JRE](#) or [uninstall JRE](#) action is stored. Each action contains information about all desktops, where it is targeted to, as well as status on each desktop
- **Agents:** The agent actions perform the JRE installation and uninstallation processes.

Installing JRE

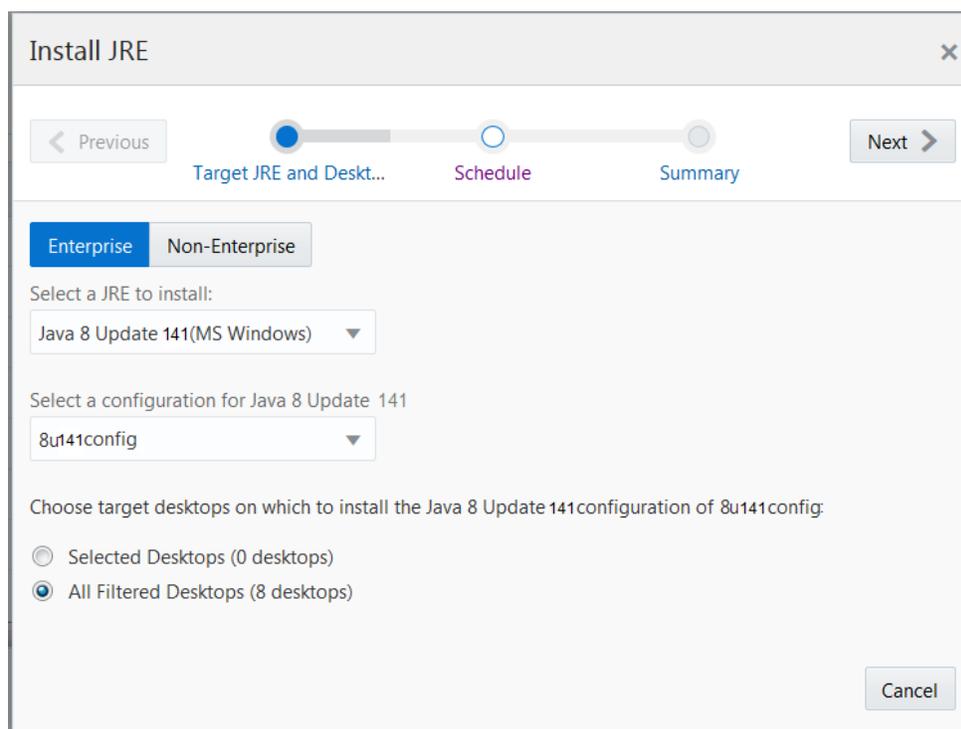
In the **Desktop** tab of `/amcwebui`, click **Install JRE** to install a configured Java Runtime Environment (JRE).

As a prerequisite, in the **Installer** tab of the Advanced Management Console, click **Add Java Version** to add and configure a Java version before you start with the JRE installation process:

To install JRE:

1. In the Advanced Management Console, click the **Desktops** tab. Ensure that you have selected the targeted Desktop from the **Display** drop-down list.
2. Click **Install JRE** to display the Install JRE dialog.
The **Enterprise** button is highlighted, by default.
3. Select a JRE from the **Select JRE to install** drop-down list.

You can select an available JRE version added to Installers tab. Once you select a JRE, the corresponding Configuration is displayed in the **Select a Configuration for JRE** drop-down list. For example, if you select Java 8 Update 141 JRE, then in the **Select a Configuration for Java 8 Update 141** drop-down list, `8u141config` is displayed.



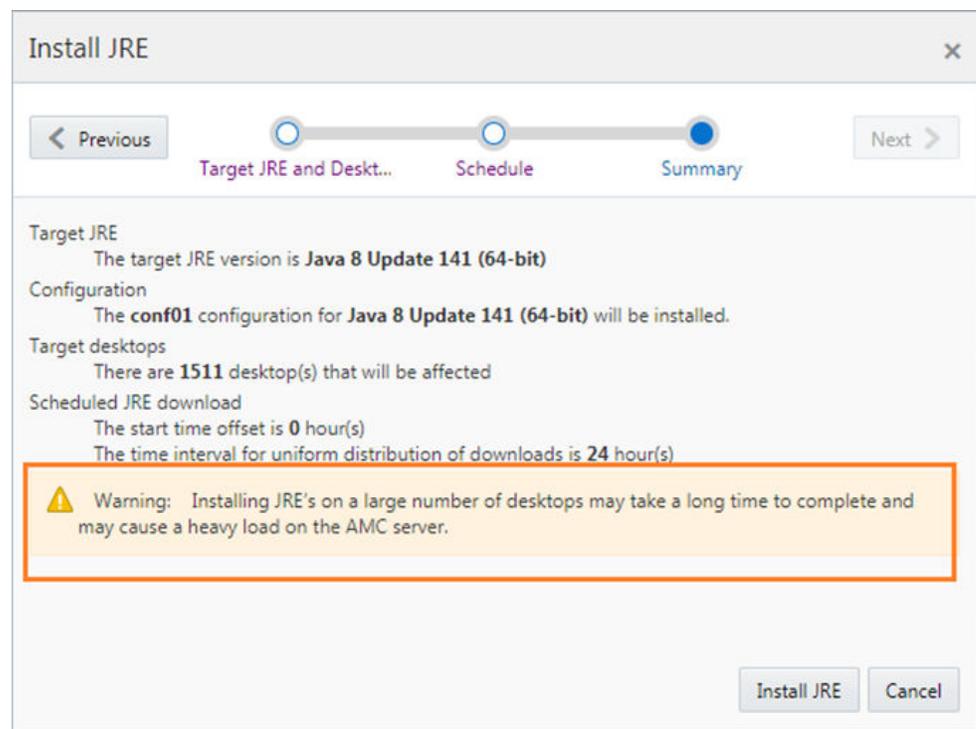
4. Select target desktops on which to install the selected JRE. You can either select the **Selected Desktop** or **All Filtered Desktops**. Ensure that you have selected at least one desktop.

Once you select either of these options, **Next** is enabled. If you haven't selected at least one desktop, the **Next** button is not enabled.

Note:

In case you have selected more than 1000 desktops, then a warning message is displayed under **Summary**.

5. Click **Next** to display the **Schedule** screen and select the following (Optional step):
 - a. **Postpone JRE downloads, hours**: Select a value if you want to postpone the time taken to download the JRE.
 - b. **Time interval to spread JRE downloads uniformly, hours**: Select a value to spread the time taken to download the JRE.
6. Click **Next** to display the summary of the selected JRE. The selected schedule is shown under Summary.



7. Click **Install JRE** to schedule Install JRE command.

Installing a Non-Enterprise JRE

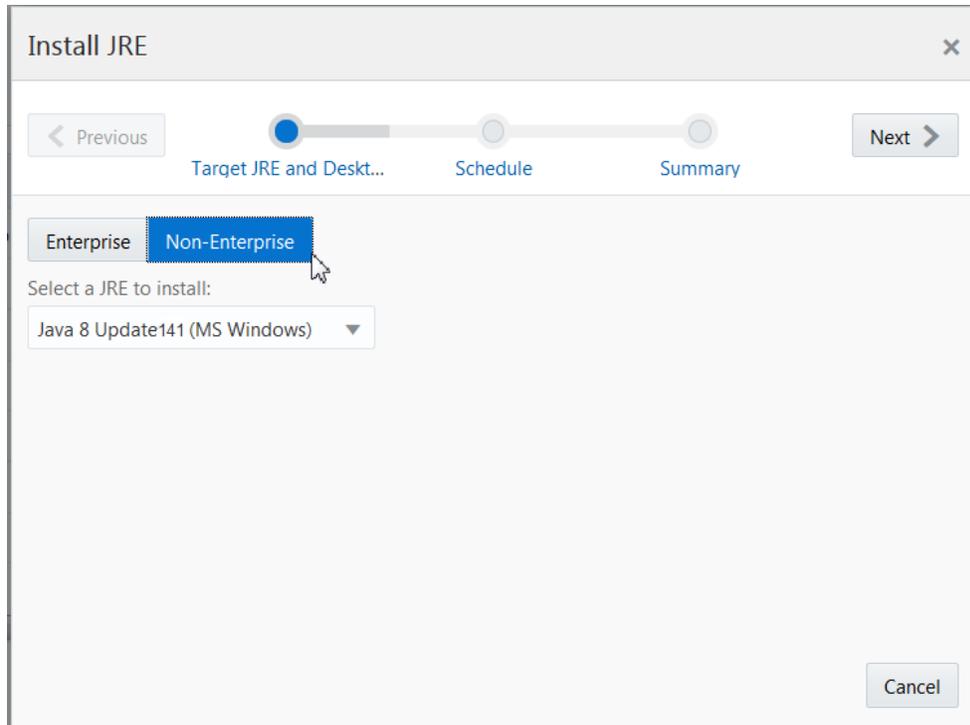
You can install non-enterprise JREs for Windows and on macOS. However, the non-enterprise don't have the ability to define customization, but can be installed by using **Install JRE** from the **Desktops** tab.

As a prerequisite, in the **Installer** tab of the Advanced Management Console, click **Add Java Version** to add and configure a Java version before you start with the JRE installation process:

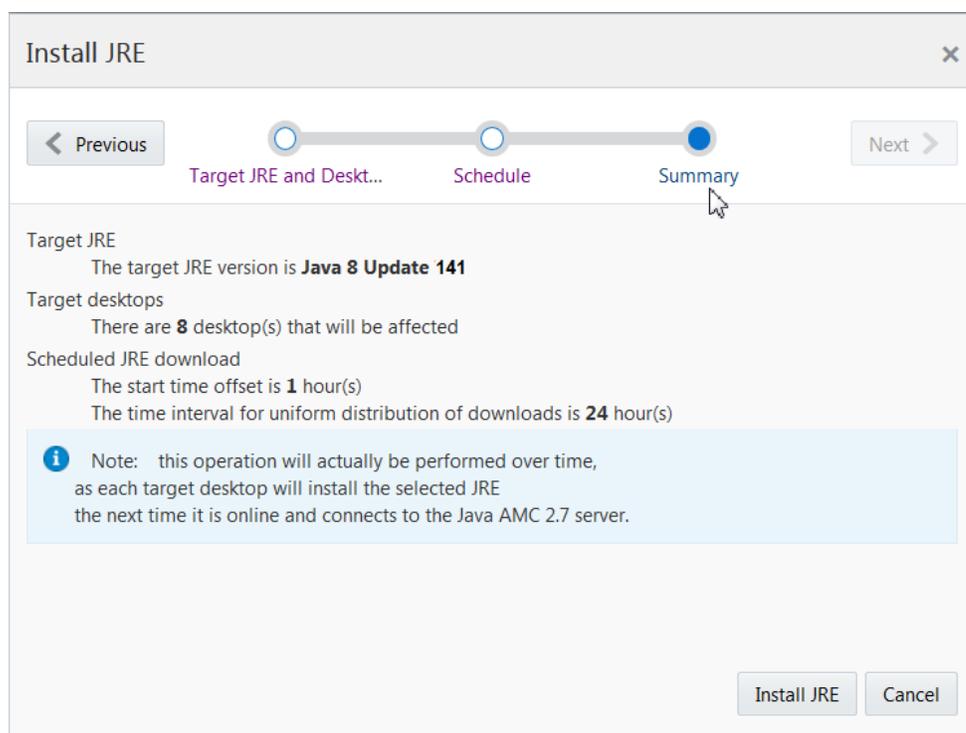
To install a non-enterprise JRE:

1. In the Advanced Management Console, click the **Desktops** tab. Ensure that you have selected the targeted Desktop from the **Display** drop-down list.

2. Click **Install JRE** to display the Install JRE dialog.
The Enterprise tab is highlighted, by default.
3. Select target desktops on which to install the selected JRE. You can either select the **Selected Desktop** or **All Filtered Desktops**.
Once you select either of these options, **Next** is enabled.
4. Click **Non-Enterprise** tab.
5. Select a JRE from the **Select JRE to install** drop-down list.



6. Click **Next** to display the **Schedule** screen and select the following (Optional step):
 - a. **Postpone JRE downloads, hours:** Select a value if you want to postpone the time taken to download the JRE.
 - b. **Time interval to spread JRE downloads uniformly, hours:** Select a value to spread the time taken to download the JRE.
7. Click **Next** to display the summary of the selected JRE:



8. Click **Install JRE** to schedule Install JRE command.

Uninstalling JREs

You can uninstall detected Oracle JREs on managed desktops, which are installed using Oracle Java Runtime Environment (JRE) installers or Enterprise Microsoft Windows Installer (MSI). The Advanced Management Console doesn't uninstall privately-installed JREs or JREs that are present on the desktops but are not actually installed.

To uninstall JREs:

1. In the Advanced Management Console, click the **Desktops** tab. Ensure that you have selected targeted Desktops from the **Display** drop-down list.
2. Click **Uninstall JRE** to display the Uninstall JRE dialog.
3. Select the target desktops from which you want to uninstall the JREs. Select either of the following target options: **Selected Desktops** or **All Filtered Desktops**.
4. Click **Next**.
5. Select how you would like to uninstall JRE versions.. You can select either of the following options: **Uninstall JRE versions below the security baseline** or **Uninstall specific JRE versions**.

The **Next** button is enabled only when you select either of these options. If you select **Uninstall specific JRE versions**, then a list of JRE versions are displayed as shown:

Uninstall JRE [X]

← Previous Target desktops **Uninstall Options** Summary Next →

Choose how you would like to uninstall JRE versions:

Uninstall JRE versions below the security baseline

Uninstall specific JRE versions

1.4.2_14

1.4.2_18

1.4.2_19

1.5.0_06

Cancel

- Click **Next** to display the Summary of the JREs selected to be uninstalled.

Uninstall JRE [X]

← Previous Target desktops Uninstall Options **Summary** Next →

The following JRE versions will be uninstalled:

1.4.2_14

1.4.2_18

Note: this operation will actually be performed over time, as each target desktop will uninstall the selected JRE the next time it is online and connects to the Java AMC 2.7 server.

Uninstall JRE Cancel

- Click **Uninstall JRE** to uninstall the selected JREs.

Status

The Status tab forms a major User Interface (UI) component of the Java Runtime Engine (JRE) management architecture. This tab further comprises the following tabs: **Commands**, **Desktop**, **Java**, and **Java Releases** tabs.

- **Commands:** In the **Commands** tab, you can view the details of the agent actions, such as Install JRE and Uninstall JRE, along with their status: whether Scheduled, In Progress, Completed, Failed, or Cancelled. For each of these command status, you can click on the counter to see all the desktops, where the command is in the specified state. To cancel any of the actions, click the **Cancel** icon.
- **Desktops:** In the **Desktops** tab, you can view the details of the rule sets that have failed and retired desktops. Click **Display data in Desktops tab** to go to the Desktop tab.
- **Java:** In the **Java** tab, you can view the details of the number of processed and failed Java Usage Tracker records, as well as information about Java Security Baseline.
- **Java Releases:** In the **Java Releases** tab, information about the upcoming and released CPUs are displayed. The Java Versions, Type (CPU/LU/PSU), and Date are displayed in a tabular format in this tab. Also, a warning appears as a number next to the **Java Releases** tab that indicates the number of new releases that you may not be aware of. For example, (4), where (4) indicates that 4 new releases have happened since you last visited the **Java Releases** tab.

6

Installer Configuration

The Advanced Management Console enables administrators to add Java installer packages for Windows and macOS.

 **Note:**

Adding Java installer packages for Linux platform is currently not supported.

AMC supports Java Runtime (JRE) installers for Enterprise (MSI/PKG) as well as Non-Enterprise (EXE/DMG). The customized installer package contains the installation options that are set according to the needs of the enterprise.

This topic includes the following sections:

- [About Installer Configurations](#)
- [Adding a Java Version](#)
- [Adding an Installer Configuration](#)
- [Editing an Installer Configuration](#)
- [Deleting an Installer Configuration](#)
- [Applying a Configuration to an Installer File](#)
- [Exporting an Installer Configuration to a File](#)
- [Installer Configuration Attributes](#)
- [Installer Configuration Properties](#)

About Installer Configurations

The Installers tab of the Advanced Management Console is divided into Enterprise and Non Enterprise sub tabs. Each of these sub tabs comprises the Windows tab and the macOS tabs that show the installer configurations that have been created on Windows and macOS respectively. Information about each installer is also shown, such as the date it was last modified and the number of properties that have been customized. Commercial customers have access to MSI (Windows installer) and PKG (macOS installer) for the JRE. These files contain installer properties that you can set to customize the installation of the JRE. The Advanced Management Console enables you to create configuration files and custom installer files to use when deploying a JRE to desktops that run on these operating systems.

Additional configurations can be created as needed. For example, if the organizations in your enterprise have different requirements for installing the JRE, then you can create a custom configuration for each organization. A custom installer file can be generated for each configuration, or the configuration can be exported to a file, which is then passed to the installer when the installer is invoked.

**Note:**

Any kind of installer configuration is applicable to Enterprise installers only.

The initial configuration is created when the Java version is added to the Advanced Management Console . This configuration shows the default settings for the installer properties.

Adding a Java Version

If you have an installer file for a Java Runtime Environment (JRE) version that is used in your enterprise, then add this Java version to the Advanced Management Console . As new versions of Java are released, add the installer files for each version. A default configuration is created for each version based on the settings in the installer file. You can also add non-enterprise JREs (EXE/DMG) to Advanced Management Console , but customization is not supported.

To add a Java version:

1. In the Advanced Management Console , click the **Installers** tab.

The **Enterprises** sub tab is highlighted by default.

The **Windows** tab is displayed by default. Start the Advanced Management Console UI as described in [Starting the Advanced Management Console User Interface](#), in case the user interface is not running. If you want to add a Java version in a macOS environment, then click the **macOS** tab.

2. Click **Add Java Version**.

A Java Web Start application is downloaded to your system and started. If you are prompted to allow the application to run, then click **Run**.

3. In the Select installer for Configuration window, select installer file for the JRE that you want to add, and click **Open**.

After the installer file is uploaded to the Advanced Management Console , refresh the browser page to see added Java version and installer file.

The installer file shown next to the Java version contains the default settings for the installer properties. This is the base version, which is never changed in the Advanced Management Console .

**Note:**

Click the **Non Enterprise** sub tab, and repeat the steps to add a Java version to non-enterprise JREs.

Adding an Installer Configuration

After you add a Java version to Advanced Management Console , you can add more configurations for that version as needed. Different configurations enable you to customize the installation for the different groups that you support.

Note:

The configuration-related topics are applicable only to Enterprise JREs only. Non-Enterprise JREs cannot be configured. They are used without configuration.

To add an installer configuration:

1. In the Advanced Management Console , click the **Installers** tab. The **Enterprise** sub tab is highlighted by default.

In the **Windows** tab, the list of Java versions and existing configurations is shown. See [Adding a Java Version](#). If you want to add a configuration in a macOS environment, then click the **macOS** tab.
2. Add a configuration.
 - To add a configuration using the default settings, click **Add New Configuration** in the table for the Java version of interest.

Enter the name for the configuration when prompted. The page of properties is then shown.
 - To add a configuration using the settings from an existing configuration, click **Duplicate** in the Actions column for that configuration.

The page of properties is shown. The name of the configuration defaults to the name of the configuration that was duplicated followed by `-copy`. Edit the **Configuration** field to change the name.
3. Set the properties as needed.

If you change a property from its default setting, then the **Reset** option is shown in the Set Default column. To restore the default value for a property, click **Reset**. If you duplicate an existing configuration and change a property, then reset sets the property to the default value, not to the value in the configuration that was duplicated.
4. Click **Save** to save the configuration.

Editing an Installer Configuration

You can modify existing installer configurations in Advanced Management Console as needed.

To edit an installer configuration:

1. In the Advanced Management Console , click the **Installers** tab. The **Enterprise** sub tab is highlighted by default.

In the **Windows** tab, the list of Java versions and existing configurations is shown.

If you want to edit a configuration in a macOS environment, then click the **macOS** tab.

2. Click **Edit** in the Actions column for the configuration that you want to edit.

The page of properties is shown.

3. Change the settings as needed.

If you change a property from its default setting, then the **Reset** option is shown in the Set Default column. To restore the default value for a property, click **Reset**.

4. Click **Save** to save the configuration.

Any customized MSI files and exported configuration files that were created before the configuration was edited are not changed.

Deleting an Installer Configuration

When a configuration is no longer needed, you can delete this installer configuration from Advanced Management Console .

To delete an installer configuration:

1. In the Advanced Management Console , click the **Installers** tab. The **Enterprise** sub tab is highlighted by default.

In the **Windows** tab, the list of Java versions and existing configurations is shown. If you want to delete a configuration from a macOS environment, then click the **macOS** tab.

2. Click **Delete** in the Actions column for the configuration that you want to remove.
3. Confirm the deletion when prompted.

The page automatically refreshes and shows that the installer configuration has been deleted.

4. (Optional) Manually delete any customized MSI files and exported configuration files that you created from the deleted configuration.

Applying a Configuration to an Installer File

To create a custom installer file, apply an installer configuration in Advanced Management Console to the base installer file for a Java version. The custom installer file then contains the settings needed to install the Java Runtime Environment (JRE) in your enterprise.

To apply a configuration to an installer file:

1. In the Advanced Management Console , click the **Installers** tab. The **Enterprise** sub tab is highlighted by default.

In the **Windows** tab, the list of Java versions and existing configurations is shown.

Note:

You cannot apply a configuration to an installer file in the macOS environment.

2. Click **Apply to MSI** in the Actions column for the configuration that you want to use to create the custom MSI file.

A Java Web Start application is downloaded to your system and started. If you are prompted to allow the application to run, then click **Run**.

3. In the **Save Configured MSI File As** window, go to the location where you want to save the custom MSI file and provide a name for the file.

4. Click **Save** to start downloading the base MSI and applying the configuration.

The message "File *file-name* patched successfully" is shown when the customized MSI file is successfully saved.

Use this installer (MSI) file with system management software to distribute the JRE and ensure that it is installed with the settings required by your enterprise. If needed, settings in the MSI file can be overridden by settings passed from the command line or a configuration file.

Exporting an Installer Configuration to a File

A configuration file for installer can be exported using the **Export to File** option. This configuration contains customized setting applicable to related Java version installer and can be used to run a customized installations.

To export an installer configuration to a file:

1. In the Advanced Management Console , click the **Installers** tab. The **Enterprise** sub tab is highlighted by default.

In the **Windows** tab, the list of Java versions and existing configurations is shown. If you want to export an installer configuration in a macOS environment, then click the **macOS** tab.

2. Click **Export to File** in the Actions column for the configuration that you want to export.

You are prompted to either open the file with a text editor or save the file.

- To save the file, select **Save File**.

Navigate to the location where you want to save the file and enter a name of your choice. Click **Save**.

- To view the file in an editor, select **Open With** and choose the editor to use.

Make any changes that you want and then save the file to the location of your choice.

When you install a JRE, pass the file that you created while installing an MSI file. This step is required to provide custom settings to the file that is created during MSI installation. Ensure that the version of the JRE you are installing matches the version of the JRE for which the configuration file was created. Make sure that the Settings in the configuration file override the settings in the MSI file. Settings from the command line override both the configuration file and the MSI file.

You can use this configuration file to test configurations without needing to create multiple MSI files. Also, if most settings are the same for all organizations, then you can create a custom MSI file for most settings and then pass in a configuration file for the few settings that are different.

Installer Configuration Attributes

The Installers tab of Advanced Management Console provides information about the available installer configurations and the attributes. Configurations for each Java version that was added to Advanced Management Console are grouped by Java version.

The following table describes the information shown for each configuration:

| Attribute | Description |
|-------------------------|---|
| Configuration | Name of the configuration |
| Created On | Date and time that the configuration was created |
| Last Modified On | Date and time of the most recent modification |
| # Customized Properties | Number of properties that have a value different than the default value |
| Actions | Actions that are available for the configuration |

Installer Configuration Properties

Property settings are used to manage the installation of the Java Runtime Environment (JRE). These settings control such things as the location of the deployment rule set, where the JRE is installed, and if Java applications are allowed to run in the browser.

The properties that are available differ by the version of the JRE. See [Installer Configuration File Options](#) in *MSI Enterprise JRE Installer Guide for Windows*.

7

User Management

Access to the Advanced Management Console is managed with user accounts. When a user is added, the permissions that are given to the user determine the functions that the user can access. Users are managed in the Configuration tab of the Advanced Management Console .

The User Management topic includes the following sections:

- [About User Accounts](#)
- [Views for Users](#)
- [Creating User Accounts](#)
- [Editing User Accounts](#)
- [Changing the Account Password](#)
- [Resetting the Admin Account Password](#)
- [Password Rules](#)
- [Deleting User Accounts](#)
- [User Permissions](#)

About User Accounts

Users of the Advanced Management Console are the enterprise administrators who are responsible for managing desktops in an enterprise. A user must have an account to log in to the Advanced Management Console . Access to the different functions is controlled by the permissions given to the account.

The first time the Advanced Management Console is started, the user is prompted to create a user account. That account is then used to create additional users from the Configuration tab of the Advanced Management Console . See [Creating User Accounts](#).

Users can change the password and edit the properties for their own account. If they do not have Administrator permission, then they cannot change their permissions. See [User Permissions](#).

Only users with Administrator permission can [create](#) and delete users. These users can also edit the accounts of other users, including changing the permissions for the account.

Views for Users

The table view for Users in the Configuration tab of Advanced Management Console shows the user accounts that are defined. The properties view shows the properties for the selected account.

In the table view, click the arrow that appears in the Users column heading to sort the data by the values in that column. Use the navigation bar below the table to view additional pages when the number of user accounts exceeds the page size. Use the navigation bar below the properties to view the properties for other user accounts.

User Table Details

The table view for Users in the Configuration tab of Advanced Management Console provides information about the user accounts and the permissions associated with each account.

The following table describes the information that is shown in the table view for user accounts:

| Column Name | Description |
|-----------------------|---|
| Users | Name of the user account |
| Admin Permission | If a check mark is shown, then the account has administrator permission |
| Installers Permission | If a check mark is shown, then the account has installers permission |
| Rule Sets Permission | If a check mark is shown, then the account has rule sets permission |
| Java Usage Permission | If a check mark is shown, then the account has Java usage permission |

User Properties

The properties view for Users in the Configuration tab of the Advanced Management Console provides information about user account.

The following table describes the information that is shown in the properties view for a user account.

| Property | Description |
|------------|---|
| Email | Name of the account. The string entered is used to log in to the account. |
| First Name | First name of the owner of the account |
| Last Name | Last name of the owner of the account |
| Phone | Phone number for the owner of the account |
| Role | Permissions given to the account |

Creating User Accounts

User accounts enable administrators to access the Advanced Management Console . Create the accounts for your organization and use the permissions to limit access to only the functions needed by each user.

To create a user account:

1. In the Advanced Management Console UI, click the **Configuration** tab.
2. Click **Users**.

The table of existing user accounts is shown.

3. Click **Create**.

The form for providing information needed for the account is shown.

4. Enter the information for the account that you are creating.

The email address is used as the name of the account and the string that the user enters to log in. The email address must be unique.

Required fields are marked with an asterisk (*). See [Password Rules](#) for the guidelines on setting passwords.

5. Click **Save** to create the account.

The account is shown in the table of accounts.

Editing User Accounts

Edit a user account when a user's information changes or you need to change the permissions for the account. Users with `Admin` permission can edit any user account. Users without `Admin` permission can edit only their own account.

To edit a user account:

1. In the Advanced Management Console UI, click the **Configuration** tab.

2. Click **Users**.

The table of existing user accounts is shown.

3. Double-click the account that you want to edit.

The properties view for the account is shown.

4. Click **Edit**.

5. Change the information for the account that you are editing.

You must have `Admin` permission to change the permissions for an account. You cannot remove `Admin` permission from your own account.

6. Click **Save** to save the changes.

Changing the Account Password

You can change the account password for your Advanced Management Console as needed, regardless of the permissions given to the account.

To change the password for a user account:

1. In the Advanced Management Console UI, click the **Configuration** tab.

2. Click **Users**.

The table of existing user accounts is shown.

3. Double-click the account for the password that you want to change.

The properties view for the account is shown.

4. Click **Update Password**.

The Update Password dialog is shown.

5. Enter the new password in both fields. Refer to [Password Rules](#) for the guidelines on setting passwords.
6. Click **Save** to change the password.

Resetting the Admin Account Password

You can reset the admin account password of Advanced Management Console .

To reset the admin account password:

1. In the Advanced Management Console login page, click **Forgot Password**.
2. Enter your email address and click **Reset password**.

A link will be sent to the specified email ID to reset the password.

 **Note:**

Ensure that you have the mail configuration in the WebLogic server.

3. Click the link and enter the new password in both fields. Refer to [Password Rules](#) for the guidelines on setting passwords.
4. Click **Save**.
5. Login to your account with the new password.

 **Note:**

The password reset functionality does not support LDAP accounts.

Password Rules

Requirements for Passwords

The default length for passwords is initially set by the administrator when initializing the AMC console. The length of all passwords must be between 8 and 128 characters. After the AMC console is initialized, the password length can be edited under Users in the Configuration tab. When the length is edited by changing the value in the Password Policy section of Users settings, all user accounts must use the new password length.

In addition to meeting the minimum character length requirement, all passwords must contain at least one character from each of the following groups:

- Numbers
- Special characters: See the following table for a list and description of the special characters that can be used in passwords
- Lowercase letters
- Uppercase letters

Table 7-1 Special Characters Allowed in Passwords

| Name of the Character | Characters |
|--|------------|
| question mark | ? |
| at sign | @ |
| exclamation point | ! |
| number sign | # |
| dollar sign | \$ |
| percent sign | % |
| plus sign | + |
| hyphen | - |
| slash | / |
| period | . |
| backslash | \ |
| single quotation mark | ' |
| comma | , |
| colon | : |
| caret | ^ |
| underscore | _ |
| grave accent | ` |
| This character is also known as the backquote character. | |
| tilde | ~ |
| left parenthesis | (|
| right parenthesis |) |
| left brace | { |
| right brace | } |
| left bracket | [|
| right bracket |] |

Deleting User Accounts

When a user account is no longer needed for the Advanced Management Console , you can delete it. Administrator permissions are required to delete a user account.

To delete a user account:

1. In the Advanced Management Console UI, click the **Configuration** tab.
2. Click **Users**.
The table of existing user accounts is shown.
3. Select the user that you want to delete.
You cannot delete the account that you used to log in.
4. Click **Delete**.

5. Confirm the deletion in the Confirm Delete dialog box.
The account is removed from the table of accounts.

User Permissions

Access to the functions of Advanced Management Console is controlled by user accounts and the permissions given to the accounts.

The following table describes the permissions that are available:

| Permission | Description |
|------------|--|
| Admin | Permission for managing users and desktop groups, view permission for other tabs |
| Installers | Permission for installer configuration |
| Rule Sets | Permission for desktop management, rule set management, and status |
| Java Usage | Permission for Java usage reports |

8

Agent Configuration

This topic includes the following sections

- [Configuring Agent Proxy Settings](#)
- [Customizing Agent Intervals](#)
- [Initiating Agent Update](#)

Configuring Advanced Management Console Agent Proxy Settings

You can set the Advanced Management Console agent proxy host name and port in the **Agents Download** sub tab of the **Configuration** tab. The **Agents Download** sub tab consists of downloadable agent bundle files (zip files).

To configure the agent proxy setting:

1. In the Advanced Management Console UI, click the **Configuration** tab.
2. Click **Agents Download**.
3. Click **Edit** to display the **Configure AMC Agent Proxy Settings** dialog.
4. Enter the following details for the agent to connect to the Advanced Management Console server:
 - **Agent Proxy Host Name:** Specify a proxy server host name.
 - **Agent Proxy Port:** Specify a proxy server port number.

 **Note:**

Clearing both the Agent Proxy host name and port deletes an existing proxy setting. If there is no proxy, then the proxy host name and port details are not needed.

Configuring Agent Intervals

In the Advanced Management Console web user interface, you can set the time between regular agent actions to different values. The Advanced Management Console checks for updates to these values. When you modify the agent intervals in the Advanced Management Console UI and save the changes, a command is created with the information of the new intervals. Agents then fetch this command the next time they check for new commands and update themselves with new interval values and the new values replace the old interval values.

To configure the agent intervals:

1. In the Advanced Management Console UI, click the **Configuration** tab.
2. Click **Agent Settings**.
3. Click **Edit** to display the **Agent Actions Interval** dialog.
4. Edit any of the following values. You can either edit all of them or just the ones that you want to:

JUT Processing Interval

Interval for the agents to report Java Usage Tracker records to the server

Check Command Interval

Interval to check if the server has any commands for the agent

Standard JRE Scan Interval

Interval to scan Java Runtime Environment (JRE) in the standard location (For example, on Windows it is C:\Program Files\Java) and report to server

Application JRE Scan Interval

Interval to scan JRE under the application location (For example, on Windows it is C:\Program Files) and report to server

LocalStorage JRE Scan Interval

Interval to scan JREs in the entire local storage system (not targeting any particular directory) and report to server

Agent Auto Update

Enable or disable the agent auto update

Agent Log File Max Size (Kb)

Maximum agent log file size in Kb

Number of Agent Log Files

Maximum agent log file number during agent log rotation

Randomize Interval

Enable or disable randomize interval

5. Click **Save**.

Agent Update Initiation

The agent update initiation setting provides you with a way to influence the frequency at which agent updates are initiated or retried. This frequency can affect the load on servers and the network.

To manage the agent update initiation window:

1. In the Advanced Management Console UI, click the **Configuration** tab.
2. Click **Agent Settings**.
3. Click **Edit** to be able to update values under the **Agent Actions Interval** or **Agent Update Initiation** sections of the **Agent Settings** sub tab.
4. In the **Agent Update Initiation** section, enter a time period in the **Agent Update Initiation Period in Hours** field. The Advanced Management Console uses this time period to calculate the frequency at which the agent updates are initiated. The **Example** gives an estimation of how frequently the initiations occurs. The values

in the **Example** get updated dynamically, as you update **Agent Update Initiation Period in Hours**. The interval between update attempts is never greater than 1 second, regardless of the period selected.

The calculation doesn't include agents that have been offline for approximately 60 days or more.

9

Other Settings

The Advanced Management Console enables administrators to specify the parameters in the Java Usage Tracker properties file. Administrators can also configure the server parameters that the agent uses.

This topic includes the following sections:

- [Customizing Java Usage Tracker Properties](#)
- [Server Settings](#)

Customizing Java Usage Tracker Properties

The Advanced Management Console agent automatically enables the Usage Tracker on agent-managed Windows and macOS desktops. However, you need to manually configure the Java Usage Tracker on the Linux operating system.

To customize the Java Usage Tracking settings:

1. In the Advanced Management Console UI, click the **Configuration** tab.
2. Click **Settings**.
3. Configure the parameters as described in the following table:

| Parameter | Description |
|-----------------------|---|
| Port Number | The port number of the host. The default value is 19870. |
| Separator | The character or string that separates entries in the log file. The default is <SEP>. |
| Quote Character | The character or string used to quote fields. The default is <QT>. |
| Inner Quote Character | The character or string that is used to quote an item containing a space in JVM argument and additional properties field, which are space-separated lists. The default is <IQT>. |

4. Click **Save**.

Note:

For Linux desktops, download the `usagetracker.properties` file and place it in the `<JRE directory/lib/management` folder.

Server Settings

You can edit the default values for server settings as follows:

1. In the Advanced Management Console UI, click the **Configuration** tab.
2. Click **Settings**.
3. Enter the **Hostname** of the server.
4. Enter the **Port Number** of the server.
5. Customize the browser **Session Timeout** for the AMC UI. A notification is displayed informing the user about the timeout and an option to extend the session. The value should be set in the range of 5 minutes to 480 minutes(8 hours).The default value is 60 minutes.
6. Click **Save**.

10

Rule Sets and Rules Management

The Advanced Management Console enables administrators to create and distribute deployment rule sets, which provide control over the browser-based Java applications that are run on desktops in their enterprise. Usage information collected from Java Usage Tracker reports can be used to create rules and rule sets. Existing rule sets can be imported and managed by Advanced Management Console .

This topic includes the following sections:

- [About Deployment Rule Sets](#)
- [Rule Sets Tab](#)
- [Managing Rule Sets and Rules](#)
- [Deploying Rule Sets](#)
- [Generating a Self-Signing Certificate](#)

About Deployment Rule Sets

A deployment rule set enables enterprises to continue using legacy business applications in an environment of ever-tightening application security policies. You can use a deployment rule set to manage which web-based Java applications, such as Java applets or Java Web Start applications, are allowed to run in an enterprise. You can also use a deployment rule set to control the version of the Java Runtime Environment (JRE) that is used for an application. The Advanced Management Console provides administrators with a tool for creating and managing deployment rules sets, which can then be distributed throughout the enterprise.

Deployment rule sets contain deployment rules. These rules are used in the deployment process to determine if a browser-based Java application is allowed to run, if the application is automatically blocked, or if default processing is used. Applications are compared to the rules based on criteria such as location, title, JAR file checksum, and certificate used to sign the application. Rules are compared in the order in which they appear in the rule set. The first rule that an application matches determines the action taken for that application.

Although multiple rule sets can be defined, only one rule set can be active on a user's system. That rule set must be a signed JAR file. The export feature of the in the **Rule Sets** tab generates the necessary JAR file. If JAR signing is enabled, then signing is done as part of the export process; otherwise, the JAR file must be signed manually. After the JAR file is signed, it must be imported into the Advanced Management Console to be available for distribution. See [Exporting a Rule Set](#). In the Rule Sets tab, you can also set a rule set as the default deployment rule set. See [Setting Default Deployment Rule Set](#),

See [Deployment Rule Set](#) in the *Java Platform, Standard Edition Deployment Guide*.

Rule Sets Tab

The Rule Sets tab of the Advanced Management Console shows a list of rule sets and corresponding lists of all rules. The tab also displays an artificial rule set called All Rules, which is not a rule set, but is a collection of all rules in the Advanced Management Console. For each rule set, the name and its title, action of the rule, rule version, and the location of the rule are displayed.

In the **Display Rule As** table, click the arrow that appears in the column heading to sort the data by the values in that column. Use the navigation bar below the table to view additional pages when the number of entries exceeds the page size. Click the **Properties** icon next to **Display Rule As** to view the properties of the selected Rule. The following figure displays the Display Rule As table and its properties:

| ID | Rule Name | Title | Action | Run Version | Location |
|----|-------------------|---------------------|--------|-------------|---|
| 61 | Allow-DryRun-Rule | JNLP application | RUN | SECURE-1.8+ | http://parovoz.ru.oracle.com/~aananiev/jem/applets/UnlpApplication.jnlp |
| 45 | Allow-Rule | AMC Webstart Sample | RUN | SECURE-1.8 | https://slc08mcc.us.oracle.com:8088/amcwebui/amcsamples/webstart/Red/version-webstart.jnlp |
| 63 | Allow-Sample-Rule | AMC Webstart Sample | RUN | SECURE-1.8+ | https://slc08mcc.us.oracle.com:8088/amcwebui/amcsamples/webstart/Yellow/version-webstart.jnlp |

In **Display Rule Set As**, click the **Table** icon, and then click the **Rule Set Action** icon to do the following to manage the rule sets:

- Create a rule set
- Delete the selected rule set
- Sign the selected rule set
- Import a rule set
- Export a rule set
- Assign a default rule set
- Move the selected rule up or down by clicking the **Up** and **Down** arrow icons

Under **Display Rule Set As**, select a Rule Set and click the **Rule Set Details** icon to view the Rule Set details, and then manage the rule sets (create, delete, sign, import, export, and assign a default rule set).

In the **Rule Set Details** pane, click the **Edit** icon to edit the selected rule set. Click the **Rule Set Details** (search) icon to view the details of the rule set both in tabular as well as properties view.

Managing Rules and Rule Sets

Use the Rule Set tab in the Advanced Management Console to manage rule sets and view the relationship between rule sets and applications.

The following table under **Rule Set Details** describes the information that is shown for each rule set. To view the details, click the **Rule Set Details icon** :



| Property | Description |
|---------------|---|
| Rule Set Name | Name of the rule set. This name is not part of the exported rule set. Double-click the rule set name to show and hide the names of the rules that are in the rule set. |
| # of Rules | Number of rules in the rule set |
| Signed | Indicator that the rule set is signed. Rule sets that show a check mark in this column are signed. Only signed rule sets can be distributed to desktops in your enterprise. |

This topic contains the following sections:

- [Managing Rule Sets](#)
- [Managing Rules](#)

Managing Rule Sets

You can manage rule sets in the Rule Sets tab of the Advanced Management Console .

This topic contains the following sections:

- [Adding Rules to a Rule Set](#)
- [Editing a Rule Set](#)
- [Deleting a Rule Set](#)
- [Exporting a Rule Set](#)
- [Signing a Rule Set](#)
- [Setting Default Deployment Rule Set](#)

Adding a Rule Set

Only one deployment rule set can be active on a desktop. However, you can have more than one rule set in Advanced Management Console . You can also create rule sets for different purposes, such as providing a customized rule set for each department in your enterprise. Working with multiple rule sets also enables you to try out different combinations of rules.

Adding a Rule Set includes the following:

- [Importing an Existing Rule Set](#)
- [Creating a Rule Set](#)

Importing an Existing Rule Set

If you have an existing rule set, then you can import it into Advanced Management Console from the Rule Set tab.

To import a rule set:

1. In the Advanced Management Console , click **Rule Set**.

2. In the **Display Rule Set As**, click the **Rule Set Actions** drop-down arrow icon and select **Import** to display the Import New Rule Set dialog.
3. Enter or browse to the location of the file that you want to import.
You can import a signed or unsigned rule set JAR file named `DeploymentRuleSet.jar`, or a rule set definition file named `ruleset.xml`.
4. Enter a name in **Rule Set Name**.
Advanced Management Console uses this name is used to manage the rule set. The name is not included when a rule set is exported.
5. Click **Import** to import the rule set.
The rule set is added to the Rule Sets table, and the rules included in the rule set are added to the Rules table. Expand the rule set to see the rules that were imported. The names for the rules in the imported rule set default to the name of the rule set followed by a rule number. See [Editing a Rule](#).

Creating a Rule Set

To create new Rule Sets for managing web-based Java applications in your enterprise, go to the Rule Set tab in the Advanced Management Console .

To create a rule set:

1. In the Advanced Management Console , click **Rule Set**.
2. In **Display Rule Set As**, click the **Rule Set Actions** icon to display the **New Rule Set** dialog.
3. Enter a Name for the rule set.
4. (Optional) Enter the **Customer Data** for the rule set.

The Custom Data information is added to the Java Usage Tracker record when no rules in the rule set match the application.

Add valid XML in the Customer Data field. A block of data must begin with the `<customer>` element and end with the `</customer>` element. Multiple `<customer>` blocks are valid and all XML elements must be within a `<customer>` block. If the data is invalid, then the rule cannot be saved.

5. Click **Create** to create the rule set.

The rule set is added to the Rule Sets table. If you added rules when you created the rule set, then you can expand the rule set to see the rules. See [Adding a Rule to a Rule Set](#).

Editing a Rule Set

After a deployment rule set is created, you can add more deployment rules and delete rules that are not needed in the **Rule Sets** tab in the Advanced Management Console . You can also reorder the rules. The order of the rules in the rule set is important, because the action taken for a web-based Java application is determined by the first rule that the application matches.

The Editing a Rule Set topic includes the following sections:

- [Adding a Rule to a Rule Set](#)
- [Reordering Rules in a Rule Set](#)

- [Removing Rules from a Rule Set](#)
- [Editing Customer Data in a Rule Set](#)
- [Editing a Signed Rule Set](#)

Adding a Rule to a Rule Set

You can add deployment rules to the rule set to define the action that you to be applied for a web-based Java application in the Rule Sets tab. The order of the rules matters.

To add rules to a rule set:

1. Click the **Rule Sets** tab in the Advanced Management Console .
2. Under **Display Rule As**, select a rule in the Rules table.
3. Use one of the following methods to add the selected rule to a rule set:
 - Use the mouse to drag the selected rule from the Rules table to the target rule set in the Rule Sets table.
 - Click **Add to Rule Set**. In the Add a Rule to a Rule Set dialog, select a target rule sets, and click **Add**.
 - In the Rule Sets table, select a rule in a rule set. Use the mouse to drag the rule to a different rule set. The rule is added to the target rule set and also remains in the source rule set.

See [Editing a Signed Rule Set](#) for actions that are needed if you edit a signed rule set.

Reordering Rules in a Rule Set

The order of the deployment rules in a deployment rule set matters. The first rule to match an application is used to determine the action for that application. You can reorder rules using the Up and Down arrows in the Rule Sets tab. For best results, place rules with the most restrictive matching criteria ahead of rules with less restrictive matching criteria.

To reorder rules in a rule set:

1. Click the **Rule Sets** tab in the Advanced Management Console .
2. Under **Display Rule Set As**, select a Rule Set from the Rule Set table.
The associated rules are displayed in the Rules table under **Display Rule As**.
3. Select a rule that you want to reorder and use **Up** or **Down** buttons accordingly to move the selected rule.

If the rule set is a signed rule set, then when you reorder the rules, a warning message is displayed indicating that you are about to modify a signed rule set. Typically, if rules are reordered in a signed rule set, then the rule set becomes unsigned and you need to sign the rule set to make your changes effective. See [Editing a Signed Rule Set](#).

Removing Rules from a Rule Set

When you no longer need a deployment rule, remove it from the Rule Sets tab in the Advanced Management Console .

To remove rules from a rule set:

1. Click the **Rule Sets** tab in the Advanced Management Console .
2. Under **Display Rule As**, select a rule in the Rules table.
3. Select the rule that you want to remove.
4. Click **Remove from Rule Set**.

The rule gets deleted from the rule set. If the rule set is a signed rule set, then when you try to remove a rule, a warning message is displayed in the **Remove Rule From Rule Set** dialog indicating that you are about to modify a signed rule set. Typically, if rules are removed from a signed rule set, then the rule set becomes unsigned and you need to sign the rule set to make your changes effective. See [Editing a Signed Rule Set](#).

The selected rules are removed from the rule set, but remain in the Rules table for future use. See [Deleting a Rule](#).

Editing Customer Data in a Rule Set

Add custom data to a rule set or modify that data in the **Rule Sets** tab of the Advanced Management Console . This data is added to the Java Usage Tracker record when no rules in the rule set match the application.

To edit customer data:

1. Click the **Rule Sets** tab in the Advanced Management Console .
2. Under **Display Rule As**, select a rule in the Rules table and click **Edit** to display the Edit Rule dialog.
3. In the Customer Data section, make the changes that you want.

Add valid XML in the Customer Data field. A block of data must begin with the `<customer>` element and end with the `</customer>` element. Multiple `<customer>` blocks are valid and all XML elements must be within a `<customer>` block. If the data is invalid, then the rule cannot be saved.

4. Click **Apply** to save the changes.

Editing a Signed Rule Set

A signed deployment rule set is locked and is ready to be distributed in Advanced Management Console . When you edit a signed rule set, a warning message is displayed indicating that the rule set is locked. If you proceed to edit the rule set, then the rule set gets unlocked and is no longer considered signed.

The following tasks provides information about editing a signed deployment rule set:

- [Adding Rules to a Rule Set](#)
- [Reordering Rules in a Rule Set](#)
- [Removing Rules from a Rule Set](#)
- [Editing Customer Data in a Rule Set](#)

To use the rule set after it is edited, you must export and sign the rule set. To sign the rule set, you can do either of the following:

- Select the option to sign the rule set internally in the Advanced Management Console when you export: In this case, you need not import the signed rule set

back into Advanced Management Console , because the import is automatically done. See [Exporting a Rule Set](#).

- Sign the rule set externally after you have exported it. Typically, you can do this when you have your own corporate code signing group or service that signs artifacts for you: In this scenario, when you export the rule set and sign externally, you must import the signed rule set back to Advanced Management Console. See [Importing an Existing Rule Set](#).

 **Note:**

After an existing rule set is signed, it is redeployed to all the managed desktops, to which the rule set was originally deployed. For example, if the rule set was the most recent rule set deployed to desktop A, then desktop A gets an automatic update with a new version of the rule set after it is signed again.

Deleting a Rule Set

When you no longer need one of the deployment rule sets that you created, you can delete the rule set in the Rule Sets tab of the Advanced Management Console .

To delete a rule set:

1. In the Advanced Management Console , click **Rule Set**.
2. Under **Display Rule Set As**, select a Rule Set that you want to delete.
3. Click the **Rule Set Actions** icon and select **Delete**.
4. In the Delete Rule Set confirmation dialog, click **Delete** to delete the selected rule set.

Exporting a Rule Set

When you have a deployment rule set ready for production, you can export that rule set and create the file that can be distributed to desktops. The file is signed if the tool is configured to supporting signing the rule set as part of the export process.

To export a rule set:

1. In the Advanced Management Console , click the **Rule Sets** tab.
2. Under **Display Rule Set As** select a Rule Set that you want to export.
3. Click the **Rule Set Actions** icon and select **Export** to display the Export Rule Set dialog
4. Provide the following information:
 - **DRS Version:** Select the deployment rule set version for the rule set. Rules might contain information that is not supported in earlier versions. Select **Auto** to have the version set automatically based on the rules in the rule set.
 - **Sign Rule Set:** Select this option to sign the rule set as part of the export process.
5. Click **Export** to export the rule set.

If you have selected the JAR option, then the **Opening Deployment RuleSet.Jar** dialog is displayed indicating that the `DeploymentRuleSet.jar` file is created in the output directory specified. Click **Save** to save the JAR file to your system.

If you have selected the XML option, then the **Opening ruleset.xml** dialog is displayed indicating that the `ruleset.xml` file is created in the output directory specified. See [Package and Install the Rule Set](#) in the *Java Platform, Standard Edition Deployment Guide*.

A signed rule set is ready to be distributed to your users. To use Advanced Management Console for distribution, you must import the signed rule set from the Rule Sets tab. See [Importing an Existing Rule Set](#).

Signing a Rule Set

To sign a rule set:

1. In the Advanced Management Console, click the **Rule Sets** tab.
2. In the Rule Set table, select the Rule set you want to sign.
3. Click the **Rule Sets Action** icon and then click **Sign...** to display the Sign Rule Set JAR File dialog.

If the selected Rule has already been signed, then a warning message is displayed in the dialog indicating that the rule set has already been signed.

4. Select one of the following options in the Sign Rule Set JAR File dialog:
 - **Sign with self-signed certificate**
 - **Sign with local keystore and private key provided by user**
 - **Import a signed JAR**
5. Click **Next**. The Signing Details are as shown as shown:

The screenshot shows the "Sign Rule Set JAR File" dialog box with the "Signing Details" tab selected. The dialog has a progress bar at the top with three steps: "Signing Options", "Signing Details", and "Summary". The "Signing Details" section displays the following information:

| | |
|----------------------|---|
| Certificate Alias: | amcselfsign |
| Certificate Details: | CN=amc2u5-parovoz,OU=Java,O=FMW,L=Saint-Petersburg,ST=Saint-Petersbur |
| Valid Starting On: | 9/21/2016, 3:44:06 AM |
| Invalid After: | 9/21/2017, 3:44:06 AM |

At the bottom, there is a "Default Deployment Rule Set" dropdown menu with a checkmark icon, and a "DRS Version:" dropdown menu set to "Auto". A "Cancel" button is located at the bottom right.

6. Select **Default Deployment Rule Set** to set the Deployment Rule Set as the default.

There can be only one default Default Deployment Rule Set. If you select a signed ruleset as the default one, then this selection overrides any previous default Default Deployment Rule setting.

7. Click **Sign**.

If the Rule Set has been signed, then it is indicated with a success message in the Summary page of the Sign Rule Set Jar File dialog box.

Setting Default Deployment Rule Set

In the **Rule Sets** tab of the Advanced Management Console , you can set a rule set as the default deployment rule set. If a default deployment rule set exists, then Advanced Management Console automatically deploys that default rule set to target systems during the Advanced Management Console agent registration.

To set a default deployment rule set:

1. In the Advanced Management Console , click the **Rule Sets** tab.
2. In the Rule Set table, select the rule set that you want to set as the default rule set.
3. Click the **Rule Sets Action** icon and then click **Set as Default** to display the Default Deployment Rule Set dialog.
4. Click **Apply** to set the selected Rule set as the default deployment rule set.

The default deployment rule set is indicated by **D**.

If you want to mark any other rule set as a default one, then you can just select a different, signed rule set as the default option. This new selection overrides the old selection. The **Set as Default** option is available only for signed rule sets.

Note:

If you select a rule set that is already marked as the default, then use the **Set as Default** option to remove the default status from the deleted rule set.

Viewing Relationships between Rule Sets and Applications

Identify the deployment rule sets that match a specific application from the **Rule Sets** tab. Viewing rule set relationships enables you to verify that you have defined a deployment rule to provide the desired action for a web-based Java application.

To view the relationships for a specific application:

1. In the Advanced Management Console , click the **Rule Sets** tab.
2. Under **Display Rule Set As** select a rule set from the rule set table.
3. Click the **Rule Set — App Relationship** icon to display a tree view of all rule sets and their related applications.
4. Expand the **All Rule Sets** tree and select a rule set to display the relationship in the **Related Applications** panel.

The **Related Applications** panel shows the web-based Java applications that you selected and the JAR file and extensions for that application.

5. Click the **Table** icon to go back to the rule sets table view.

Managing Rules

In the Advanced Management Console , click the **Rule Sets** tab to create, edit, and delete deployment rules. The rules that you create can then be added to deployment rule sets to manage the web-based Java applications that are being run in your enterprise.

The following actions are available for managing rules:

- [Creating a Rule](#)
- [Editing a Rule](#)
- [Deleting a Rule](#)
- [Rule Properties](#)

Creating a Rule

Create deployment rules from both the Java Usage tab and the Rule Set tab of the Advanced Management Console . A rule is used to define the action taken when a web-based Java application that matches the rule is started.

To create a rule from the Rule Sets tab:

1. In the Advanced Management Console click the **Rule Sets** tab.
2. Click **New** on the **Display Rule As** panel to display the Create a New Rule dialog.
3. Enter a name for the rule, and provide information for the remaining fields.
4. Click **Create** to save the rule.

Editing a Rule

You can modify existing deployment rules by using the **Edit** button in the **Rule Sets** tab of the Advanced Management Console .

To edit a rule:

1. In the Advanced Management Console click the **Rule Sets** tab.
2. Under **Display Rules As**, select a Rule from the Rules table.
3. Click **Edit** to display the Edit Rule dialog.
4. Edit the rule details.

If you edit a rule that is associated with a signed rule set, then the respective rule set becomes unsigned and out of date. You need to sign the rule sets again to make them effective.

5. Click **Apply** to apply your changes to the rule.

Deleting a Rule

You can delete existing deployment rules by using the **Delete** button in the **Rule Sets** tab of the Advanced Management Console .

To delete a rule:

1. In the Advanced Management Console click the **Rule Sets** tab.
2. Under **Display Rules As**, select a Rule from the Rules table.
3. Click **Delete** to display the Delete Rule confirmation dialog.
4. Click **Delete** to delete the rule.

The rule gets deleted from the Rules table.

Rule Properties

Each deployment rule contains information that is used to determine if a web-based Java application matches the rule. When an application is run, the application properties are compared with the rule properties to determine if the application is allowed to run.

The following table describes the rule properties:

| Property | Description |
|-------------|---|
| Name | Name given to the rule. This name is required for identification purposes within Advanced Management Console . The name is not exported with the rule set. |
| Title | Title of the application. If no title is provided, then all applications are considered a match to the title property. If a title is provided and Rule Action is set to either <code>default</code> or <code>run</code> , then information must be provided for Location, Certificate, or both. |
| Location | URL for the source of the application. If no URL is provided, then all applications are considered a match to the URL field. For applications that use JNLP, this is the location of the JNLP file. For applications embedded in a web page, this is the location of the web page. |
| Certificate | Hash value for the certificate that was used to sign the application and the algorithm used to create the hash value. Certificate hash values are typically used to identify signed applications. |
| Checksum | Hash value for the checksum for the JAR file and the algorithm used to create the hash value. Checksum hash values are typically used to identify unsigned JAR files. |
| Rule Action | Action taken for any application that matches the rule. Select one of the following options: <ul style="list-style-type: none">• <code>default</code>: Use default processing to determine if the application is allowed to run.• <code>block</code>: Always block the application.• <code>run</code>: Allow the application to run. If this option is selected, then you must also specify a JRE version and at least one of the following properties: Title, Location, Hash value.• <code>force-run</code>: Override the JRE requested by the application, if any, and run the application with the JRE specified in the rule. If this option is selected, then you must also specify a JRE version. |

| Property | Description |
|---------------|--|
| Version | <p>JRE version to use to run the application. This property is enabled only if the Rule Action is set to <code>run</code> or <code>force-run</code>.</p> <p>The version specified for the rule must match the version specified by the application; otherwise, the application is blocked. The versions don't need to be an exact match, for example, <code>1.7+</code> and <code>1.8*</code> are considered a match. For Version, choose one of the following options and select a release or enter a version number:</p> <ul style="list-style-type: none"> • SECURE: Any secure version. This option matches the secure version from any API level. • SECURE + API level: A secure version from the API level selected from the list. Select Or Later to allow secure versions newer than the selected API level to be used. For example, <code>SECURE-1.7</code> matches any secure version from the 1.7 release only, and <code>SECURE-1.7+</code> matches any secure version from the 1.7 release and later releases. • API level: Any version from the API level selected from the list. Select Or Later to allow versions newer than the selected API level to be used. For example, <code>1.7*</code> matches any version of the 1.7 release only, and <code>1.7+</code> matches any version of the 1.7 release and later releases. An asterisk is added to the API level when the rule is saved if Or Later is not selected. • Product: The specific version entered in the field for versions. Enter the version that you want, or select a release from the list. Select Or Later to allow versions newer than the specified version to be used. For example, <code>1.8.0_05</code> matches only the 1.8.0_05 version of the 1.8 release, and <code>1.8.0_05+</code> matches the 1.8.0_05 version and later versions in the 1.8 release as well as versions in later releases. • Latest available JRE: The latest version that is available on the user's system. |
| Message | <p>Message shown to the user. If no message is provided, then a default message is shown when an application is blocked, and no message is shown when an application matches a run rule.</p> <p>To add a message, right click in the message table and select Add Message. A new row is added to the table.</p> <p>In the Locale column, enter the locale for the message and Enter. In the Message column, enter the message to show the user and press the Enter key. If the Locale field is set to <code><default></code>, then the message is used when no message is provided for the user's locale.</p> <p>If multiple messages are provided, then all messages are compared with the user's locale in the order shown. If more than one message matches the locale, then the last message matched is used. To reorder the messages in the table, delete and reenter the messages as needed.</p> |
| Customer Data | <p>Custom information that is included in a rule. This information is added to the Java Usage Tracker record when an application that matches the rule is run.</p> <p>Add valid XML in the Customer Data field. Each block of data must begin with the <code><customer></code> element and end with the <code></customer></code> element. Multiple <code><customer></code> blocks can be entered. All XML elements must be within a <code><customer></code> block. If the data is invalid, the rule cannot be saved.</p> |

Deploying Rule Sets

The Advanced Management Console provides administrators with a way to distribute a deployment rule set to desktops in their enterprise. The desktops must be registered with the Advanced Management Console .

Generating a Self-Signed Certificate

In the Configuration tab of the Advanced Management Console , you can generate a self-signed certificate on the server to sign rule set jars.

To generate a self-signed certificate:

1. In the Advanced Management Console click the **Configuration** tab.
2. Click **Jar Signing**.

If a generated certificate already exists, the corresponding data is displayed, and the **Generate** button is disabled.

3. Enter the following details in the **Create Certificate** dialog:

- Common Name
- Organizational Unit
- Organization
- City
- State/Region
- Country
- Days Valid: Optional field. By default, the value in the **Days Valid** field is set to 365 days.

4. Click **Generate**.

The details of the self-signed certificate are displayed under **Generated certificate for signing deployment rule set JARs**. Click **Export Certificate** to download the generated certificate in PEM (Privacy-Enhanced Mail) format .

11

Desktop Groups Configuration

The Advanced Management Console enables enterprise administrators to define desktop groups and associate desktops with one or more groups based on desktop properties. Desktop groups are added in the Configuration tab of the Advanced Management Console . Existing desktop groups are available as filters in the Desktops tab.

This topic includes the following sections:

- [About Desktop Groups](#)
- [About Mapping Files](#)
- [Views for Desktop Groups](#)
- [Creating a Desktop Group](#)
- [Updating an Existing Desktop Group](#)
- [Viewing Desktops in a Desktop Group](#)
- [Deleting a Desktop Group](#)
- [Desktop Group Properties](#)

About Desktop Groups

Desktop groups in the Advanced Management Console provide a way to filter desktops based on the values for a group. The group name is treated as an additional property for desktops and a mapping file defines the values for that property.

As an example, consider a group named `Country`, which has the values `China`, `France`, `Russia`, and `United States`. When the group is created, existing desktops are mapped to the appropriate group value. To view desktops that are associated with the group value `France`, the filter criterion `Country` is added in the Desktops tab and set to `France`.

Desktops are associated with a group based on one of the following desktop properties:

- IP address
- Email
- Host name

When the group is created, the desktop property to use is selected. A mapping file is provided, which contains a list of values for the selected desktop property and the group value to associate with the desktop.

If the desktop properties for a desktop are changed, then the new values are compared with the group mapping files. Group associations are automatically adjusted based on the new values for the desktop properties. For desktops that are added after a group is created, the desktop properties are compared with the mapping file for the group. If a match is found, then the new desktop is associated with the group.

About Mapping Files

A desktop group in the Advanced Management Console is generated from a mapping file, which is used to map desktops to the group. The mapping file can be any comma-separated values (CSV) file that contains information about the desktops in the enterprise.

Each entry in the mapping file must contain a column for the desktop property on which the mapping is based and a column for the group value that is associated with the desktop. For example, if the mapping is based on host names and the group is based on countries, then each entry must contain a host name and country name. If a mapping file contains additional columns, then that information is ignored.

The character that is used to separate columns is specified when the group is created. The default is a semicolon (;). The column indexes for the desktop property and the group value are also specified when the group is created. The index is zero-based, so the first index for the first column is 0.

The following example shows a sample mapping file named `country-mapping.txt`, which can be used to create a group named `Country` that contains the group values `China`, `France`, `Russia`, and `United States`. The mapping between group values and desktops is based on the host name. The file contains the host names of desktops in column 0 and the country for each desktop in column 2. The file also contains business unit information in column 1, which is ignored.

```
hostname1;Marketing;France
hostname2;Marketing;France
hostname3;Marketing;United States
hostname4;Engineering;Russia
hostname5;Finance;France
hostname6;Finance;United States
hostname7;Sales;China
hostname8;Sales;Russia
```

When a group is created, the mapping file is processed. Desktops that are matched to an entry in the file are associated with the group value that is specified for the desktop. Using the sample mapping file above, the desktop with host name `hostname4` is associated with the group `Country` and the group value `Russia`. Desktops that do not match any entry in the file are not associated with the group. Entries in the file that do not match any desktop are ignored. The number of desktops that are matched and the number that are ignored are reported in the Configuration tab of Advanced Management Console .

To change a mapping file, you must delete the group and create it again using the edited mapping file.

Views for Desktop Groups

The table view for Desktop Groups in the Configuration tab of the Advanced Management Console shows the groups that are defined. The properties view shows the property values for the selected group.

In both views, click the arrow that appears in the column heading to sort the data by the values in that column. Use the navigation bar below the table to view additional

pages when the number of desktop groups exceeds the page size. Use the navigation bar below the properties to view the properties for other desktop groups.

Desktop Group Table Details

The table view for Desktop Groups in the Configuration tab of Advanced Management Console provides information about the number of entries in the mapping file and the number of entries that do not match a desktop.

The following table describes the information that is shown in the table view for desktop groups:

| Column Name | Description |
|---|---|
| Group Name | Name of the group |
| Desktop Property | Desktop property that is used to match desktops to the group |
| Desktop Property Value Count | Number of entries in the mapping file that contain the desktop property to be matched. One entry in the mapping file could match more than one desktop. For example, an email address could be associated with multiple desktops. |
| Unassigned Desktop Property Value Count | Number of entries in the mapping file that do not match any desktops. Click the unassigned desktop count value to download the CSV file. The file contains the list of desktops that don't have an agent associated with them. |

Desktop Group Property Details

The properties view for Desktop Groups in the Configuration tab of Advanced Management Console provides information about the values associated with the group and the number of desktops that match each value.

The following table describes the information that is shown in the properties view for a desktop group:

| Column Name | Description |
|--|--|
| <i>desktop-group-name</i> | Name of the desktop group. The entries in this column are the group values found in the mapping file for this group. |
| <i>number-of-desktop-property-values</i> | Number of entries in the mapping file that contain a value for the desktop property on which the mapping is based. The column name shows the total number of entries in the mapping file. For each row, the column shows the number of entries in the mapping file that match the group value shown in the first column. |
| <i>number-of-values-not-assigned</i> | Number of entries in the mapping file that do not match any desktop. The column name shows the total number of entries that are not matched. For each row, the column shows the number of entries in the mapping file that match the group value shown in the first column, but don't match any desktop. Click the count value to download the CSV file. The file contains the list of desktops that don't have an agent associated with them. |

Creating a Desktop Group

Desktop groups in Advanced Management Console add properties for searching and organizing the desktops in an enterprise.

To create a desktop group:

1. In the Advanced Management Console , select the **Configuration** tab.
2. Click **Desktop Groups**.

The table of existing desktop groups is shown.

3. Click **Create**.

The Create Desktop Group dialog box is shown.

4. Enter the information for the group that you are creating.

If you use the `country-mapping.txt` sample mapping file described in [About Mapping Files](#), then you can use the following values:

- **Group Name:** Country
- **CSV Input File:** `country-mapping.txt`
- **Group Value Column Index:** 2
- **Desktop Property Index:** 0

Note:

Instead of an IP address, such as 192.0.2.254, you can also provide an IP range in a Classless inter-domain routing (CIDR) format, for example, 192.0.2.1/24 similar to providing an IP address. In case of an IP range, for example 192.0.2.157/24, the network address (192.0.2.157) and the broadcast address (192.0.2.254) are automatically excluded by the Advanced Management Console server. Therefore, the actual IP addresses that get stored are 192.0.2.1, 192.0.2.2, ..., 192.0.2.253.

- **Desktop Property:** Hostname
- **Separator in CSV File:** ;

Although the Advanced Management Console doesn't fully support all the rules for CSV, the following usages are supported:

- If a value contains the separator, or in other words, the CSV separator character itself is part of a value, then ensure that the value is enclosed within double quotes. For example, if comma is the separator used in the CSV file, then the value, such as "California, USA", which contains a comma, is enclosed within double quotes.
 - A double-quote appearing inside a field must be escaped by preceding it with another double quote. For example: "California " "USA".
 - Lines starting with a # are comments and are ignored.
5. Click **Create** to create the group.

The mapping file is processed and the group is created. Processing of the mapping file might take a while.

To see the new group in the list of filters for the Desktops tab, go to the Desktops tab and refresh the page in the browser.

Updating an Existing Desktop Group

A desktop group in the Advanced Management Console organizes or groups a number of desktops together based on their properties, such as IP Address. For example, a desktop group called Country has values, such as Canada, US, and there are 100 entries that have desktop group value called Canada. You can update an existing group, by removing desktops from it, adding new desktops to it, or reassigning some desktops to a different group.

To update an existing desktop group:

1. In the Advanced Management Console , select the **Configuration** tab.
2. Click **Desktop Groups** to display the existing desktop group.
3. Select a desktop group in the table. The **Update** button becomes enabled.
4. Click **Update** to display the Update Desktop Group dialog box.

You can choose to do one of the following:

- a batch update (which is updating multiple entries at once)
- a point update (which is updating a single entry)
- schedule automatic update by providing the data required in the Update Desktop Group dialog box

A batch update requires an input file in the CSV format. During an automatic update, the Advanced Management Console fetches the Desktop group mapping file (the CSV file) from the host (the URL parameter in the Update Desktop Group dialog box), and updates the selected group automatically. The CSV format is same as detailed in [Creating a Desktop Group](#). Depending on the selection of the update type, an appropriate section for that update is toggled to show up for you to enter data and submit an update.

Viewing Desktops in a Desktop Group

The properties view for desktop groups in the Advanced Management Console provides links to the list of desktops that are associated with each group value. Also, desktops in the Desktops tab can be filtered by group name to see which desktops are associated with the group.

To view the desktops that are in a desktop group:

1. In the Advanced Management Console , select the **Configuration** tab.
2. Click **Desktop Groups**.

The table of existing desktop groups is shown.

3. Double-click the desktop group that you want to view.

The properties view for that desktop group is shown. The first column shows the values for the group. Each value is a link to the list of desktops that are associated with that value.

- Click the link for one of the group values.

The list of desktops that are associated with that value is shown in the Desktops tab. If a value does not provide a list, then no desktops are associated with that value.

You can also use the filters in the Desktops tab to view the desktops in a group. Select the group name from the filter criteria.

Deleting a Desktop Group

When a desktop group is no longer needed, you can delete it. To change a desktop group, you must delete it and then re-create it with the edited mapping file.

To delete a desktop group:

- In the Advanced Management Console , select the **Configuration** tab.
- Click **Desktop Groups**.

The table of existing desktop groups is shown.

- Select the desktop group that you want to delete.
- Click **Delete**.

Confirm that you want to delete the group.

Desktop Group Properties

Properties for desktop groups describe the mapping file that is used to create the group. The properties also identify the desktop property on which the mapping for the group is based.

The following table describes the properties for desktop groups:

| Property | Description |
|--------------------------|---|
| Group name | Name of the group. The group name is used as the filter name for the filter criteria and display option in the Desktops tab. |
| CSV Input File | Location of the mapping file. Click Browse to go to the file. |
| Group Value Column Index | Index of the column in the mapping file that contains the value for the group. For example, if the group identifies the country for each desktop, then this index is the column in which the country name appears. The columns are zero based, which makes the first column in the file column 0. |
| Desktop Property Index | Index of the column in the mapping file that contains the value for the desktop property that is used to determine if a desktop is part of the group. For example, if the mapping is based on the host name of desktops, then this index is the column in which the host name appears. The columns are zero based, which makes the first column in the file column 0. |
| Desktop Property | Desktop property that is used to determine if a desktop is part of the group. Select a property from the list provided. |
| Separator in CSV File | Character or string that is used to separate the values in the mapping file. The default is a semicolon (;). |

12

Accessibility in Advanced Management Console

Oracle is committed to creating products, services, and supporting documentation that is accessible to the disabled community.

Oracle's goal is to ensure that disabled users of our products can perform the same tasks, and access the same functionality as other users.

This topic describes the accessibility features supported by Advanced Management Console.

Screen Readers

Oracle supports screen readers that translate screen-based information into spoken words to assist vision-impaired users.

For instance, configuration options are currently available for the JAWS screen reader produced by Freedom Scientific, Inc. For information on configuring this product, refer to the [Freedom Scientific](#) screen reader website.

Keyboard Access

Advanced Management Console support keyboard access to several menu and toolbar functionality for users to navigate between windows and work with them, or invoke resources.

The following sections provide details on the keyboard activation and focus operations that are present in Advanced Management Console.

Keyboard Activation

After navigating to a component, you can then use the keyboard to activate the component.

The following table lists the key that are used to activate GUI components.

| Activation Keys | GUI Action |
|-----------------|--|
| Enter or Return | Activates the default command button. |
| Escape | Dismisses a menu or dialog box without changes. |
| Space Bar | Activates the tool bar button that has keyboard focus. |

Keyboard Focus

When a component has focus, it generally displays the colored border or changes the color.

However, some components in the GUI can't be displayed with a focus indicator. In this case, you must continue to use the keyboard to traverse the GUI until the focus is displayed.

Keyboard Navigation

Keyboard navigation enables you to move keyboard focus from one GUI component to another by using the keyboard without activating the component.

The following table lists the keys used for keyboard navigation.

| Navigation Key | GUI Action |
|-----------------|---|
| Tab | Navigates to the next component in the GUI. The tab traversal order is generally left to right and top to bottom. |
| Shift+Tab | Navigates to the previous component. |
| Left arrow | Moves the keyboard focus to the left by one character or component. |
| Right arrow | Moves the keyboard focus to the right by one character or component. |
| Up arrow | Moves the keyboard focus up by one line or component. |
| Down arrow | Moves the keyboard focus down by one line or component. |
| PGUP | Navigates up one pane of information within a scroll pane. |
| PGDN | Navigates down one pane of information within a scroll pane. |
| Home | Moves to the beginning of the data. In a table, the focus moves to the beginning of a row. |
| End | Moves to the end of the data. In a table, the focus moves to the last cell in a row. |
| Control+T | Shifts focus to the next link in a topic or in a report. |
| Control+Shift+T | Shifts focus to the previous link in a topic or in a report. |

List View

List view describes how to navigate within tables appearing on a page.

The following table lists the keys used for navigation within a table.

| Navigation Key | GUI Action |
|----------------|--|
| F2 | Enters Actionable mode. This enables keyboard action on elements inside the item, including navigation between focusable elements inside the item. |
| Esc | Exits Actionable mode. |

| Navigation Key | GUI Action |
|----------------|---|
| Tab | When in Actionable Mode, navigates to next focusable element within the item. If the last focusable element is reached, shift focus back to the first focusable element. When not in Actionable Mode, navigates to next focusable element on page (outside ListView). |
| Shift+Tab | When in Actionable Mode, navigates to previous focusable element within the item. If the first focusable element is reached, shift focus back to the last focusable element. When not in Actionable Mode, navigates to previous focusable element on page (outside ListView). |
| Left arrow | Move focus to the item on the left. |
| Right arrow | Move focus to the item on the right. |
| Up arrow | Move focus to the item above. |
| Down arrow | Move focus to the item below. |
| Enter | Selects the current item. No operation if the item is already selected. |

Tab Bars

This section describes how to use the keyboard to work with tab bars.

The following table lists the keys used for tab bar navigation.

| Navigation Key | GUI Action |
|----------------|--|
| Enter or Space | Selects list item. |
| Up Arrow | Moves focus to the previous visible list item. |
| Down Arrow | Moves focus to the next visible list item. |
| Right arrow | For horizontal tab bar, focus will be moved to next visible item. |
| Left arrow | For horizontal tab bar, focus will be moved to previous visible item. |
| Home | Moves focus to the first visible list item. |
| End | Moves focus to the last visible list item. |
| F2 | If focus is on a list item, pressing F2 will make its contents accessible using Tab. |
| Esc | When F2 mode is enabled, press Esc to exit F2 mode. |
| Ctrl + X | Marks the current item to move if reorderable is enabled. |
| Ctrl + V | Paste the item that are marked to directly before the current item. |
| DELETE | Delete the current item. |

A

Advanced Management Console Samples

The Advanced Management Console provides sample applet and web start applications similar to those found in organizations running Java. Administrators can use these sample applications as a diagnostic tool to verify known results. The URL for the sample application is `https://hostname:port/amcwebui/amcsamples.html`. For example, `https://localhost:7002/amcwebui/amcsamples.html`.

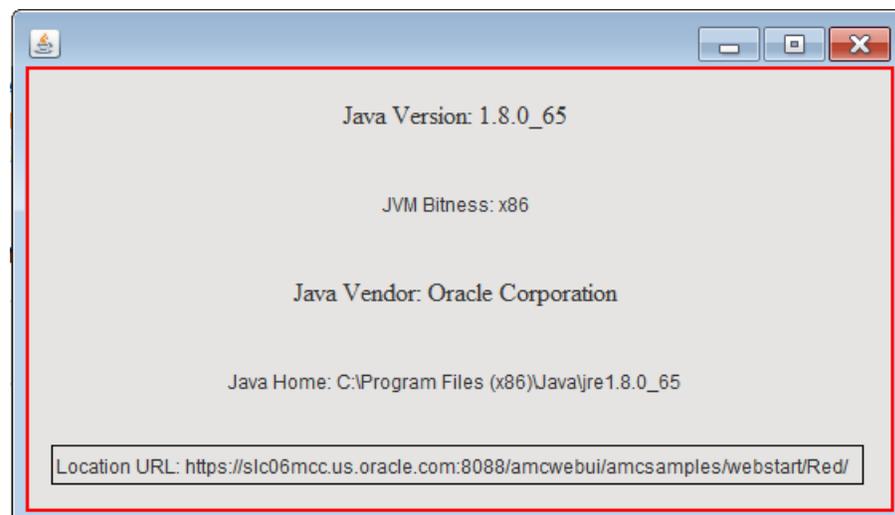
Each program lists the Java version used for the launch.

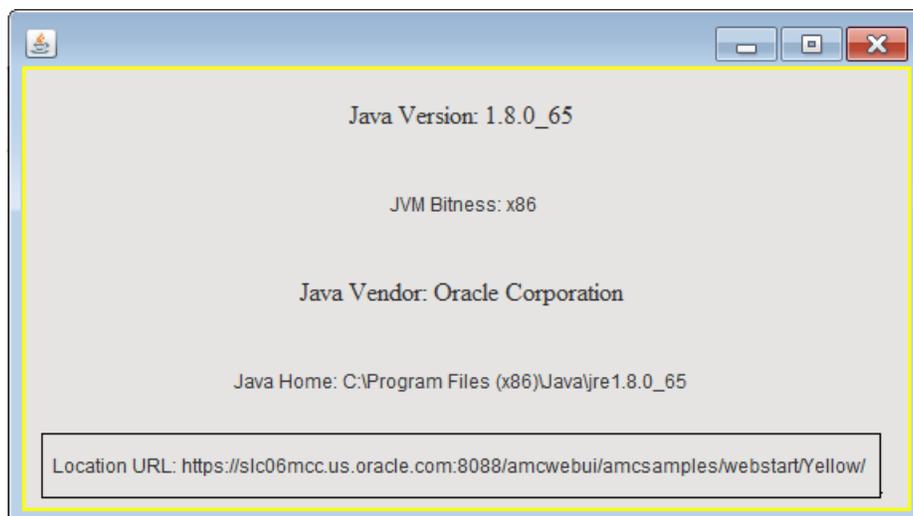
In general, in the Samples Web Start Applications and HTML Applets for Advanced Management Console page, you can do the following:

- Verify that Java works correctly in the browser, by seeing the program.
- Verify that usage tracking is configured, by looking for records of this launch. Go to the **Java Usage** tab to view these records.
- Verify that Deployment Rule Sets are configured correctly, by targeting samples to run on different Java versions.

The two html applets and two webstart applications are color coded (red and yellow) so that the application URL that appears in Java Usage tab includes the corresponding color to differentiate between one another. To test more applications, change the color in the Location URL of the launched program.

For example, click either **Launch Red Web Start Application** or **Launch Yellow Web Start Application** to view the Java Usage:





To verify the sample applets or webstart applications with different Java versions, you can create rules that can be launched with specific Java versions. A sample rule (for a red application) is as follows:

```
<rule>  
<location="https://hostname:port/amcwebui/amcsamples/webstart/Red"  
action="run" version="1.8.0_65"/>  
</rule>
```