IBM Application Runtime Expert for i

Using The Console to Verify a System

Background

IMPORTANT: The console has been greatly enhanced in recent PTFs. To have access to all of the features discussed in this document, you must have IBM Application Runtime Expert for i PTF 5733ARE SI40302, or newer, installed on your system. PTF SI40302 upgrades the Web interface for Application Runtime Expert to version 1.4.0.

The IBM Application Runtime Expert for i, or ARE, allows users to build templates can be used to verify application and system attributes on an IBM i system. Once a template is built, there are two ways it can be used to verify a system:
1. Use the console Web user interface
2. Use a script that can be run from QShell

This document introduces you to the ARE console, or just console, which is the Web user interface where templates built using the Deployment Template Editor can be used to verify IBM i systems. The console provides a simple, yet powerful, interface where templates are used to verify remote systems. A system, whether local or remote, that is to be verified using a template is referred to as the *target system*. One of the primary benefits of using the console is that no templates need to be transferred to target systems; the console takes care of doing that. This means all you need to do is select a template to use, provide the target system name or IP address, user name, and password, and the console uses the selected template to verify the target system. The results of the verification are streamed from the target system back to the console, where you can review the ARE reports directly from your Web browser. The console can verify multiple partitions or systems simultaneously, making it very easy to verify your entire enterprise environment from a single place.

IMPORTANT: To verify an IBM i system using the console, there are a few, very common, products that must be installed on the target system, as well as recent levels of the HTTP and Java Group PTFs. For a full list of the required products and Group PTF levels for a target system, see
http://www.ibm.com/systems/power/software/i/are/ptfs.html

If a target system does not meet the minimum required product or PTF levels, an error

message **"*Remote system does not meet requirement*"** is displayed when you attempt to verify the target system. Detailed information about what required product or PTF is not installed on the target system can be found in the console runtime log file.

Console Overview

To access the console Web user interface, you must log into the ARE Web user interface. It is important to note that logging into the ARE Web user interface requires an IBM i user ID that has been given *ALLOBJ special authority. When you log into the ARE Web user interface, you are directed to the Deployment Template Editor home page. To access the console from this page, click on the 'Launch console' button below the 'Manage templates' table (see Figure 1 below).
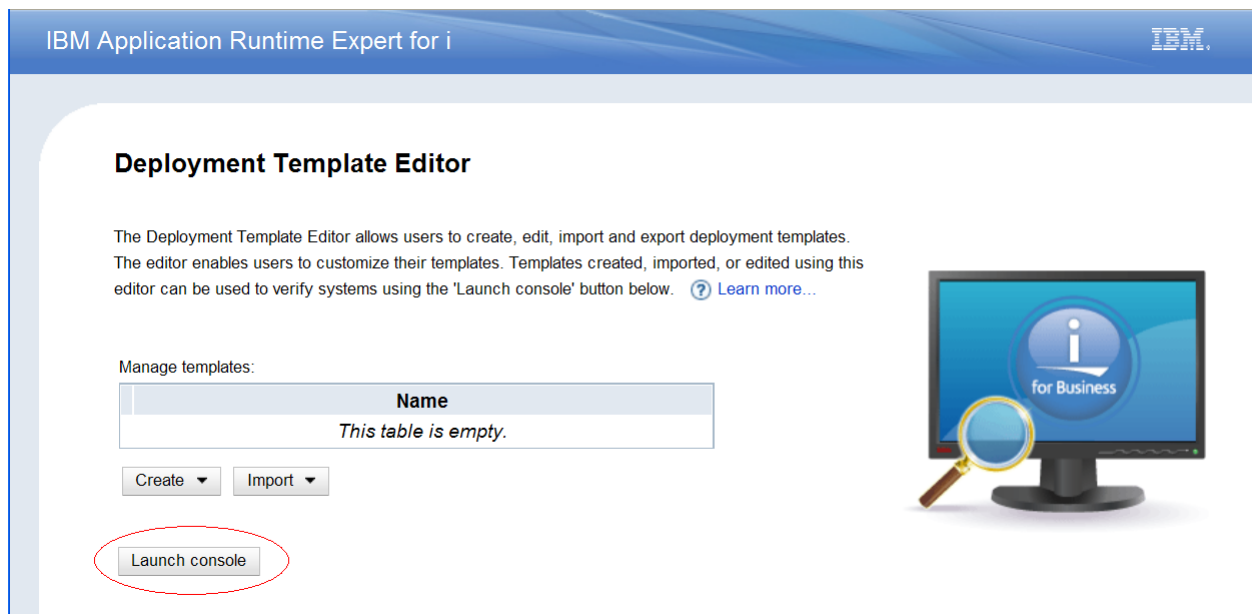

Figure 1 – Launch console button on the Deployment Template Editor home page

After clicking the 'Launch console' button, you are brought to a page where you can use your templates to verify remote systems. If you need to return to the template editor, simply click the 'Launch deployment template editor' button at the bottom of the page (see figure 2 below).
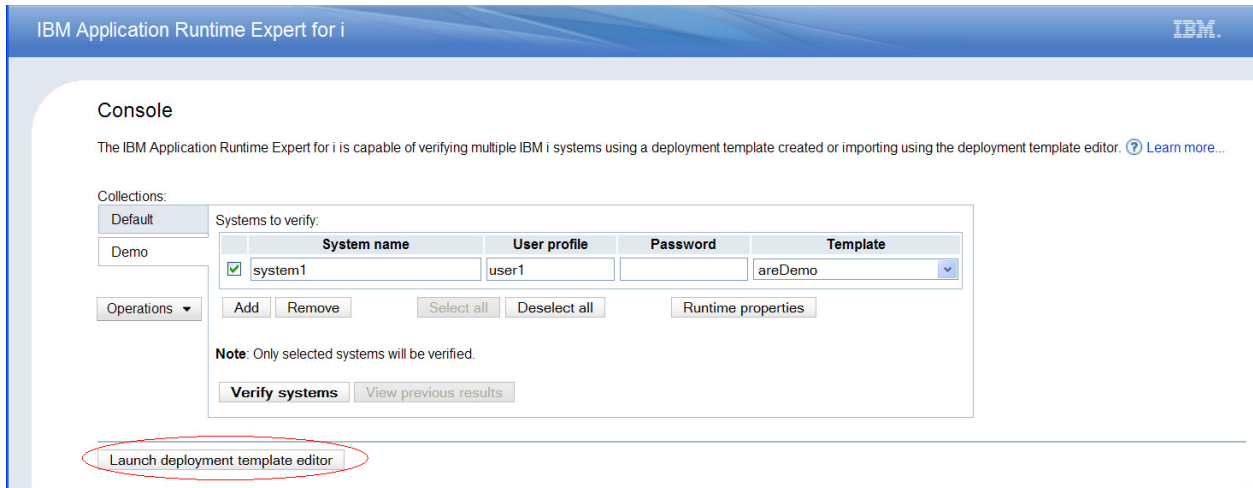
Figure 2 – Launch deployment template editor button on the console main page

Managing systems and groups

The console provides the ability to create groups of systems that you wish to verify. System groups provide a simple way to use different templates to verify groups of systems. You can set up your system groups once, and then toggle between them depending on what systems you want to verify or what template you would like to use for verification.

By default, the console has one system group named 'Default'. Each system group allows you to mange system information for that group, as well as select the template that is used to verify the systems.
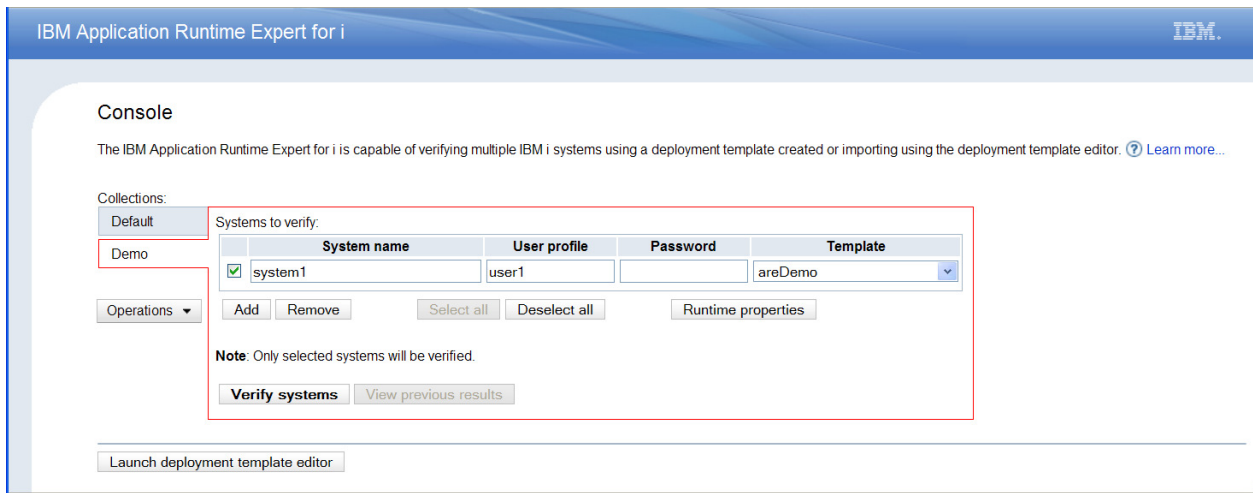

Figure 3 – System groups in the console

The console provides a set of options for managing system groups. The options are accessible via the 'Operations' menu, which is located directly below the 'Default' system group tab on the left side of the page.
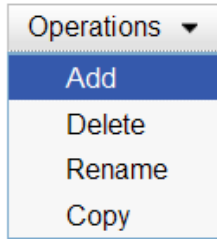

Figure 4 – Operations menu for managing system groups

The system group management options are:
- **Add** – Adds a new, empty system group. You must provide a name for the new system group. Group names are limited to a maximum of 40 characters, and cannot include spaces or certain special characters.
- **Delete** – Deletes the currently selected system group. All of the systems included in the group are removed as well.
- **Rename** – Renames the currently selected system group.
- **Copy** – Creates a copy of the currently selected system group. The copied group includes all of the systems from the original group.

Within each system group is a table of systems to verify, as shown in figure 5 below:
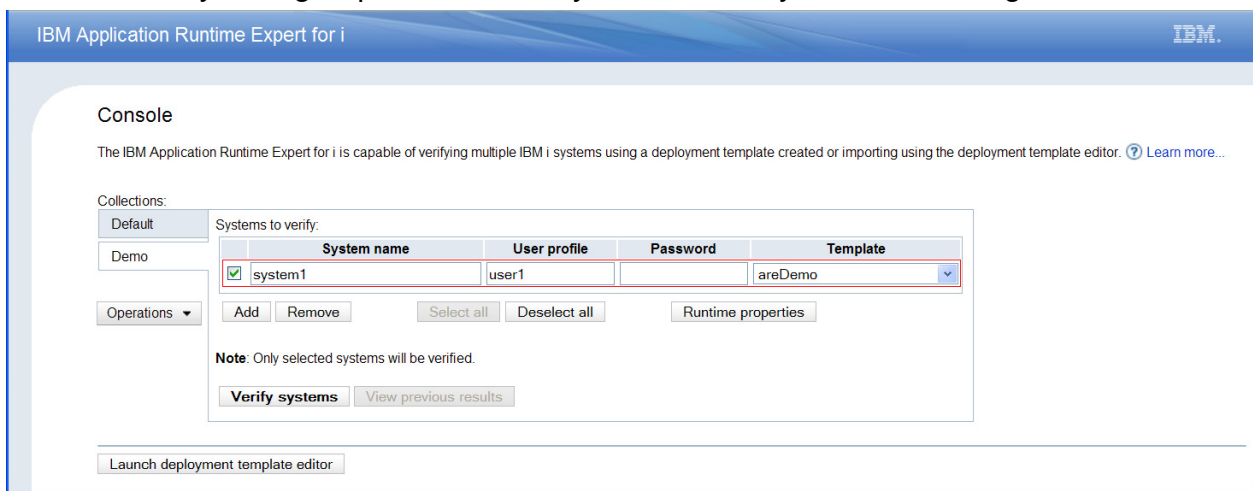

Figure 5 – Specify information about a system to verify

Each row in the table represents one system to verify, and requires the following information:
- **System name** – Often referred to as the 'target' system, this is the name of the

system to verify. Either a system name or an IP address can be specified.
- **User ID** – An IBM i user ID for the target system. This user ID is used to run the verification job on the target system. Must be a valid, enabled user ID on the target system.
- **Password** – The password on the target system for the supplied user ID.
- **Template** – The template that is used to verify the target system.

IMPORTANT: The specified user ID is used to run the verification job on the target system. In order for the verification to run successfully, the user ID must have sufficient authority to access all of the resources that need to be verified.

Within each group you can add and remove systems. Note that when removing systems, all selected rows (the check box to the left of the system name field) are removed. The results of the most recent verification can be seen using the 'View previous results' button. Previous verification results are only available as long as your browser session with ARE remains active.

For some templates, runtime information may need to be passed to the ARE core so that the verification can work correctly (the ARE core is the ARE component that verifies a system using templates built using the deployment template editor). For example, if a replacement variable is used by the template, the value for the replacement variable may need to be provided as an input property to the ARE core. To address this need, the console provides a way to configure the runtime attributes of the verification. The 'Runtime properties' button provides a way to configure how many systems are verified at the same time, the logging level used by the ARE core during the verification, and a free form input box where you can specify properties, such as replacement variable values, to be passed to the ARE core on each system that is verified.

It is important to understand that Runtime Properties settings are applied to all systems in the system group. If you require different runtime property settings for different systems, you can do this by creating multiple system groups, with each group having its own set of runtime properties.
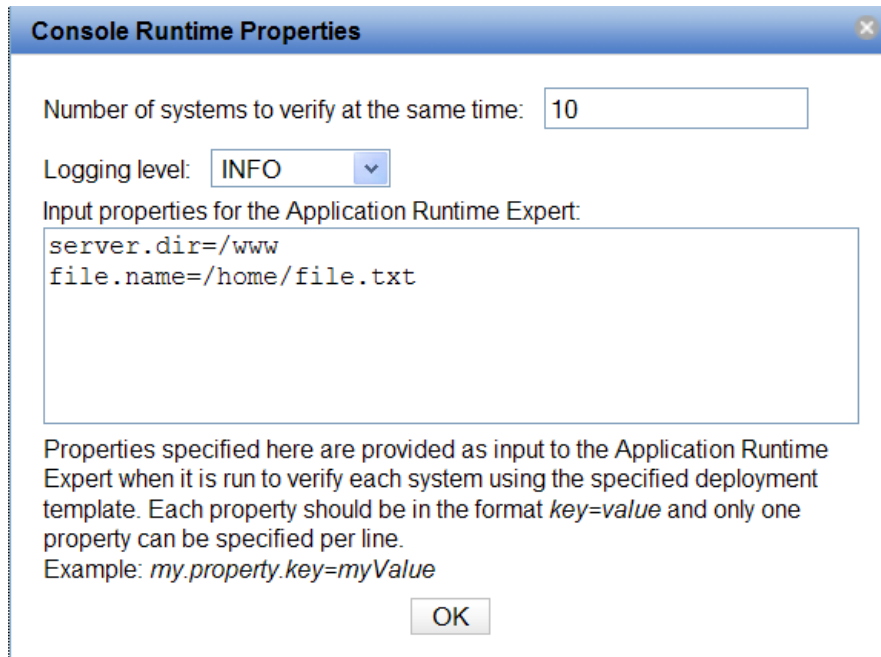
Figure 6 – Console Runtime Properties dialog box

Verifying systems

Once you have specified all of the systems to verify, you can begin the verification process by clicking the 'Verify systems' button.

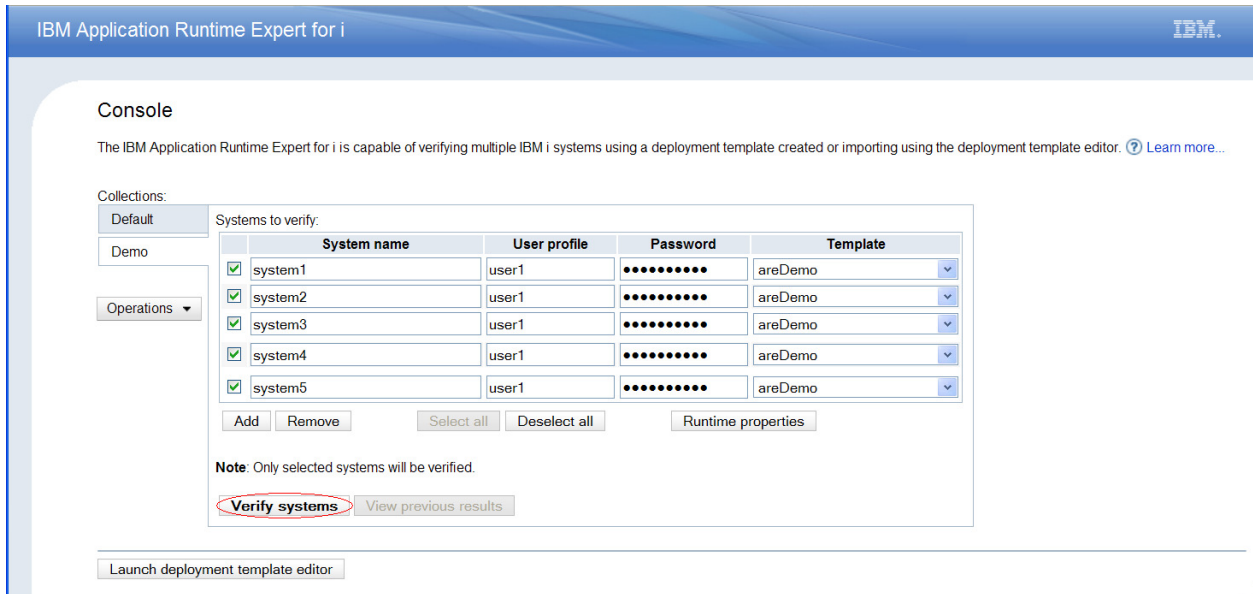**IMPORTANT:** Only selected systems (the check box to the left of the system name field) are verified.

Figure 7 – Starting the verification for the selected systems

After clicking the 'Verify systems' button, you are taken to a page that shows the current system verification status. The system verification status refreshes periodically. You can manually refresh the status by clicking the 'Refresh' link in the upper right corner of the verification status table.
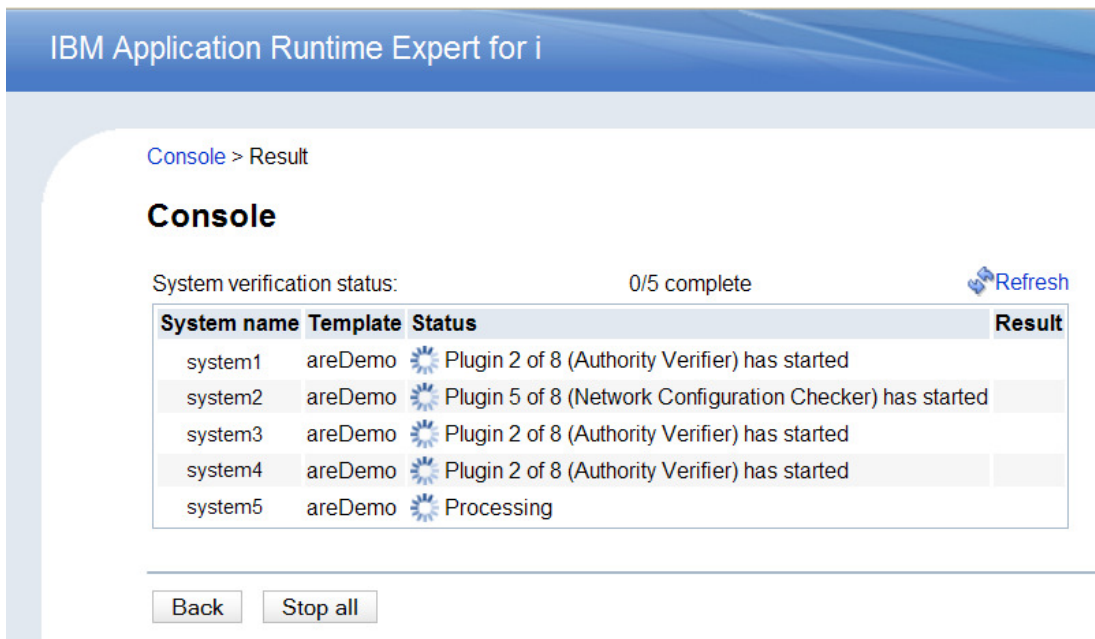

Figure 8 – System verification status

Once the system verification is complete, a 'Complete' icon is shown in the status column for that system and a brief summary of its verification is shown in the result column. If the console failed to perform the verification on a target system, a red icon is shown followed by a brief reason description of why the verification could not be performed. Additional details about the failure can be found by clicking on the 'View log' link in result column.

For systems that were verified, the results column contains a brief summary of the verification results. **The summary text in the result column is also a link.** This link provides access to the verification reports generated by the ARE core during the verification of the target system.
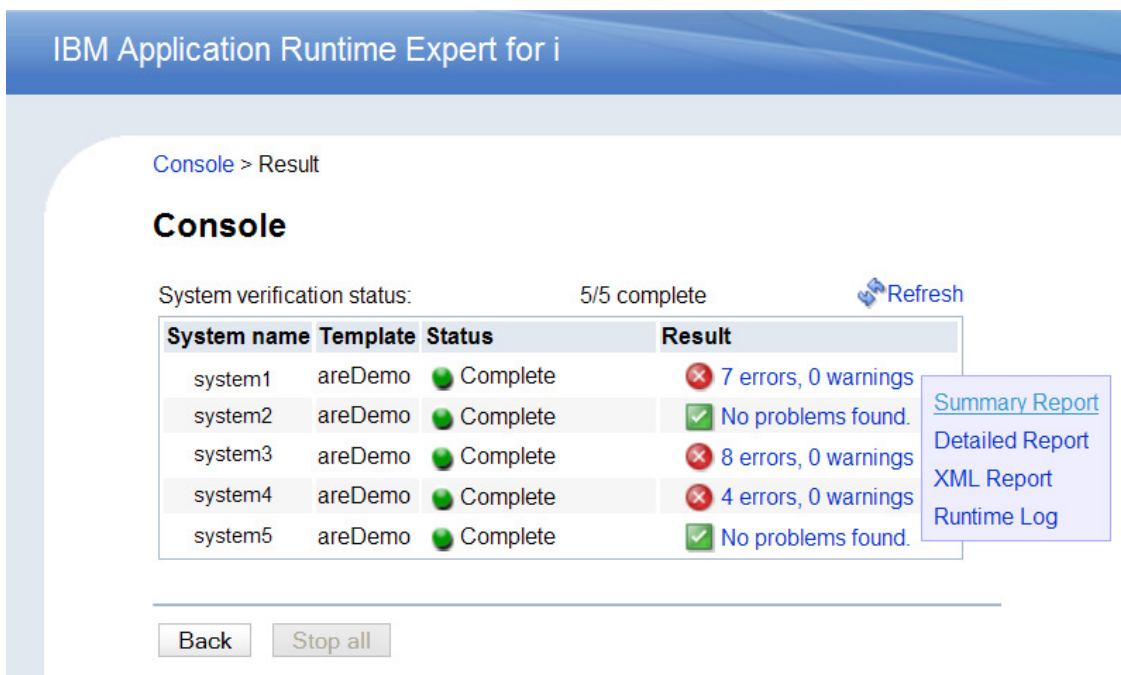

Figure 9 – Links to the verification reports

All three ARE reports (summary, detailed, and XML) are available via the link in the result column. For more information about ARE reports, see the 'Understanding the ARE reports' document on the ARE product Web site:

http://www.ibm.com/systems/power/software/i/are/documentation.html

In addition to the three ARE reports, there is a link to the runtime log. The runtime log contains events written to the console's log during the course of the target system's verification.

Of the three ARE reports, the most interesting one to view using the console is the summary report. This is because **the console provides a special, Web browser friendly, version of the summary report.**

The summary report contains a summary of all problems detected during the verification of a system. Each row in the summary table contains the results for a specific plugin, such as the 'Authority Verifier' or 'System Value Verifier' plugins. The icon directly before the plugin name indicates the highest severity problem that was found by that plugin. The other items in each row indicate the number of attributes verified by the plugin, and the number of problems found at each severity level (error, warning, and info). The final item in each row, the 'Fix actions' column, indicates how many of the detected problems can be fixed directly from the console Web interface. Details about how to fix problems is covered in the next section.

To view details about the problems each plugin found, click on either the twistie icon in front of the plugin name or the plugin name itself. This expands the summarized view of the plugin and displays detailed information about each problem found by the plugin. If a plugin did not find any problems, then there is no detailed information available for that plugin.

Console > Result > Summary Report

Summary Report

System name: system1

Remote core version: 1.0.3

Template: areDemo

User ID: USER1

Summary details   ? Learn more...

Plugin name	Attributes verified	Error	Warning	Info	Fix actions
▶ ✅ File Attribute Verifier	8068	0	0	0	None
▼ ❌ Authority Verifier	8074	3	0	0	🔧 Fix actions(3)

Description
❌ User USER1 has no data authority to object /home/user1
❌ User USER1 has no object authority to /home/user1
❌ Owner of /home/user1 is not what is expected Expected: USER1 Actual: QSYS

Plugin name	Attributes verified	Error	Warning	Info	Fix actions
▶ ✅ Configuration Attribute Verifier	110	0	0	0	None
▶ ✅ Network Verifier	0	0	0	0	None
▶ ✅ Network Configuration Checker	0	0	0	0	None
▶ ✅ Product Verifier	5	0	0	0	None
▶ ❌ User Profile Verifier	54	4	0	0	🔧 Fix actions(3)
▶ ✅ System Value Verifier	5	0	0	0	None

Figure 10 – Summary report

Fixing detected problems

The previous section briefly mentioned the 'Fix actions' column in the summary report. The purpose of this column is to allow certain problems that were detected during verification to be fixed directly from the console Web interface. This is a very convenient feature that allows you to solve certain problems without ever having to go and log into a different system! It is important, however, to understand that only certain types of detected problems can be fixed directly from the console.

In figure 12 below, there are two plugins with fix actions available: Authority Verifier and User Profile Verifier.

Console > Result > Summary Report

Summary Report

System name: system1

Remote core version: 1.0.3

Template: areDemo

User ID: USER1

Summary details ? Learn more...

Plugin name	Attributes verified	Error	Warning	Info	Fix actions
▶ ✅ File Attribute Verifier	8068	0	0	0	None
▼ ❌ Authority Verifier	8074	3	0	0	Fix actions(3)
Description					
❌ User USER1 has no data authority to object /home/user1					
❌ User USER1 has no object authority to /home/user1					
❌ Owner of /home/user1 is not what is expected Expected: USER1 Actual: QSYS					
▶ ✅ Configuration Attribute Verifier	110	0	0	0	None
▶ ✅ Network Verifier	0	0	0	0	None
▶ ✅ Network Configuration Checker	0	0	0	0	None
▶ ✅ Product Verifier	5	0	0	0	None
▶ ❌ User Profile Verifier	54	4	0	0	Fix actions(3)
▶ ✅ System Value Verifier	5	0	0	0	None

Figure 11 – Summary report with fix actions

When you click on the 'Fix actions' link, you are taken to page that summarizes all of the problems detected by that plugin that can be fixed directly from the console. You can select which problems to fix using the check box that precedes each problem description.

Figure 12 – Select problems to fix directly from the console

Once you have selected the problems to fix, simply click the 'Fix' button and the console begins the process of fixing the selected problems on the target system. Once the problems are fixed, a second table is displayed that shows the fix results. Note that in the results table, the first column (Result) shows the result of the console trying to fix the problem, and the second column (Description) contains a description of the *original* problem (not a description of the fix result).

Fix Problems

System name: system1
Problems found by: Authority Verifier

Select	Description
	This table is empty.

[Select all] [Deselect all]

▼ Processed problems

Result	Description
Fixed	☑ User USER1 has no data authority to object /home/user1
Fixed	☑ User USER1 has no object authority to /home/user1
Fixed	☑ Owner of /home/user1 is not what is expected Expected: USER1 Actual: QSYS

[Fix] [Back]

Figure 13 – Result of fixing problems on the target system

Once you have completed fixing the problems, click the 'Back' button to return to the summary report page.

IMPORTANT: The summary report is a static view of the verification results. This means that if you fix problems directly from the console, the summary report is <u>not</u> updated to reflect that some of the detected problems have now been fixed.