Oracle® Communications Network Integrity

Online Help

Release 7.4.0

F99184-01

July 2024

Oracle Communications Network Integrity Online Help, Release 7.4.0

F99184-01

Contents

Preface

1 Using Network Integrity

2 Using Scans

Preface

The Oracle Communications Network Integrity Online Help explains how to use the Oracle Communications Network Integrity (NI) user interface to create, run and manage scans.

This Online Help guide provides step-by-step instructions related to the user interface. For a conceptual understanding of Network Integrity, see *Network Integrity Concepts*.

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

Using Network Integrity

This section describes how to use Oracle Communications Network Integrity.

Getting Started with Network Integrity

Network Integrity maintains the integrity of an inventory system, by:

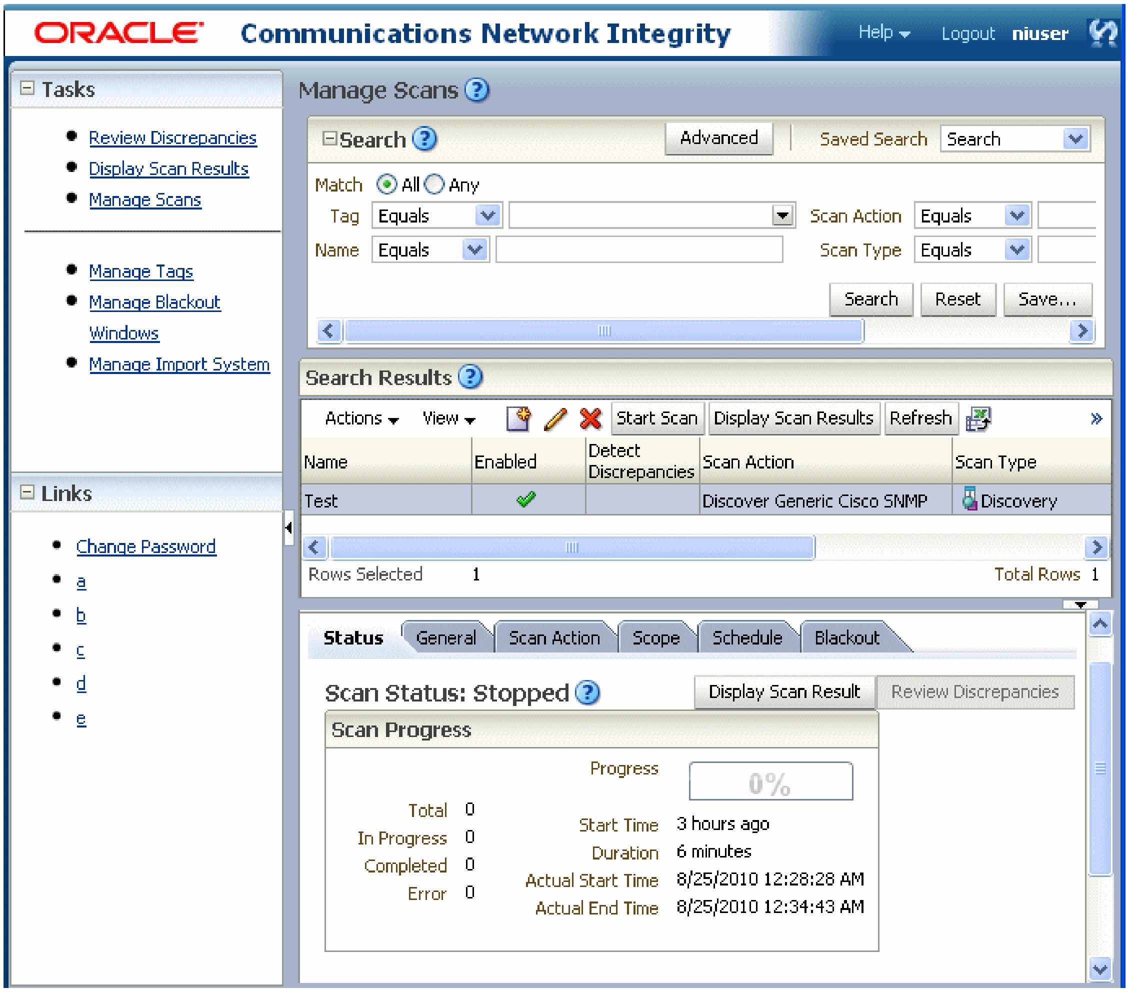
- Comparing the data in the inventory system with the data collected from the network devices themselves, and by
- Providing a means to resolve discrepancies on the inventory systems or elsewhere.

The features and functionality offered by Network Integrity are described in the following topics:

- Working with the Network Integrity UI
- Using Scans
- Working with Scan Results
- Discovering Devices
- Managing Tags
- Detecting Discrepancies
- Using Network Integrity to Review Discrepancies
- Using Blackout Windows
- Using Import Systems with Network Integrity

About the UI

The following figure provides an overview of the Network Integrity UI.



Name	Enabled	Detect Discrepancies	Scan Action	Scan Type
Test	✓		Discover Generic Cisco SNMP	Discovery

Rows Selected 1
Total Rows 1

Scan Status: Stopped

Progress	0%
Total	0
In Progress	0
Completed	0
Error	0
Start Time	3 hours ago
Duration	6 minutes
Actual Start Time	8/25/2010 12:28:28 AM
Actual End Time	8/25/2010 12:34:43 AM

The Network Integrity UI enables you to carry out tasks such as:

- Configuring network device discovery and inventory system import scans
- Initiating and/or scheduling scans
- Checking scan results
- Managing discrepancy comparisons between network and discovery results

The UI is made up of a number of work areas:

- The global area. See "About the Global Area".
- The regional area. See "About the Regional Area".
- The local area. See "About the Local Work Area".

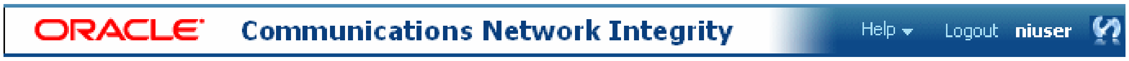
About the Global Area

The global area at the top of the Network Integrity UI consists of:

- A product identification area; *Oracle Communications Network Integrity*
- An area showing the name of the currently logged in user; *niuser*
- A logout link. See "Logging Out of Network Integrity"

- A Help menu. See "About the Help Menu"
- A processing indicator. See "About the Processing Indicator".

The following figure displays the global area.



About the Help Menu

The Help menu consists of two items:

- **Help**: Select to open a new browser window showing the main online Help page for Network Integrity. Expand the table of contents to view the subject headings, and select the required topic. Use the search function to look for a Help topic.
- **About**: Select to open a dialog box showing the version of the Network Integrity product, and the versions of all cartridges deployed in Network Integrity.

About the Processing Indicator

The processing indicator is an Oracle logo at the upper right corner of the global area. The indicator displays the following states:

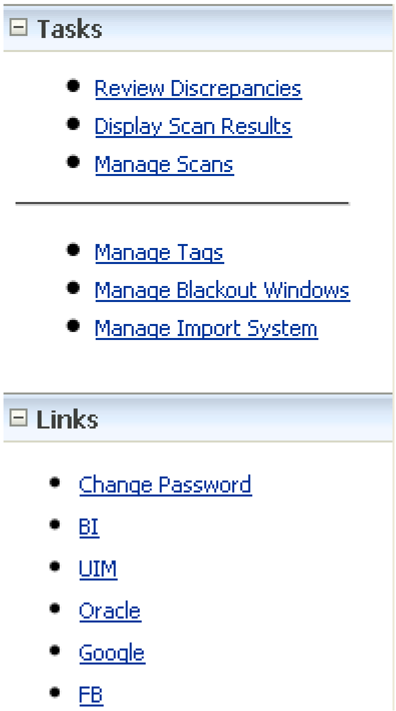
- Idle (the normal state): the indicator is not spinning
- Processing: the indicator is spinning; for example: a scan search is being carried out
- Disconnected: A red broken circle is displayed.

About the Regional Area

The regional area on the left of the UI consists of two panels:

- The Tasks panel; See "About the Tasks Panel"
- The Links panel; See "About the Links Panel"

The following figure displays the regional area.



⊟ Tasks

- Review Discrepancies
- Display Scan Results
- Manage Scans

- Manage Tags
- Manage Blackout Windows
- Manage Import System

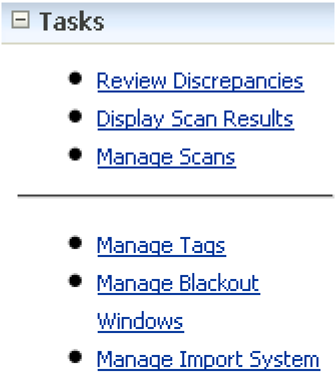
⊟ Links

- Change Password
- BI
- UIM
- Oracle
- Google
- FB

About the Tasks Panel

The Tasks panel provides access to tasks required to complete the business process associated with a work area. When you select a task link, it replaces the local area contents.

The following figure displays the Tasks panel.



⊟ Tasks

- Review Discrepancies
- Display Scan Results
- Manage Scans

- Manage Tags
- Manage Blackout Windows
- Manage Import System

The task panel for Network Integrity has the following links:

- Review Discrepancies. See "About the Review Discrepancies Link".
- Display Scan Results. See "About the Display Scan Results Link".
- Manage Scans. See "About the Manage Scans Link".
- Manage Tags. See "About the Manage Tags Link".
- Manage Blackout Windows. See "About the Manage Blackout Windows Link".

- Manage Inventory System. See "About the Manage Import System Link".

About the Review Discrepancies Link

Click this link to load the **Review Discrepancies** page. Initially, the search pane is expanded and the search results table is empty. Enter some search criteria, execute a search, and then review the resulting list of discrepancies.

You can then take further actions based on the discrepancies under review.

See "Using Network Integrity to Review Discrepancies".

About the Display Scan Results Link

Click this link to load the **Scan Results** page. Initially, the search pane is expanded and the results table is empty. Enter some search criteria, execute a search, and then review the resulting list of scan results.

If you use the default search criteria, and click **Search,** the latest scan results are returned.

See "Working with Scan Results".

About the Manage Scans Link

Click this link to load the **Manage Scans** page. Initially, the search pane is expanded and the results table is empty. Enter some search criteria, execute a search, and then review the resulting list of scans.

If you use the default search criteria, and click **Search,** you carry out a search for all scans.

See "Using Scans".

About the Manage Tags Link

Click this link to load the **Manage Tags** page. This page displays a tree-table of all tags in the Network Integrity system. From this page, you can create, edit, and delete tags.

See "Managing Tags".

About the Manage Blackout Windows Link

Click this link to load the **Manage Blackout Windows** page. This page displays a table of all blackout windows in the Network Integrity system. From this page, you can create, edit, and delete blackout windows. You can also view scans assigned to blackout windows.

See "Using Blackout Windows".

About the Manage Import System Link

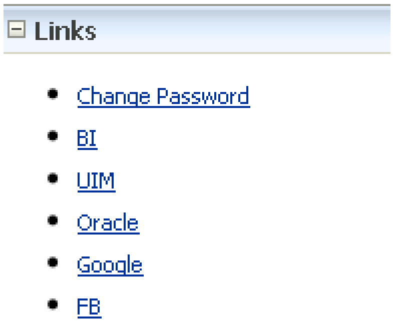
Click this link to load the **Manage Import System** page. This page is used to display and edit the connection setting for a single inventory system. This setting is used by all inventory import and inventory resolution actions to communicate with the target system. From this page, you can create, edit, and delete the connection setting.

See "Using Import Systems with Network Integrity".

About the Links Panel

You can place convenient web links in the Links panel. Typically, these are links to the web pages of external systems that may be used in conjunction with Network Integrity; for example, a link to the Oracle Communications Unified Inventory Management (UIM) login page or to the technical specifications for equipment on the network.

The following figure displays the Links panel.



Links are configured by the Network Integrity administrator. All links are application-wide, so all Network Integrity users see the same links with the same link text. For more information on creating links, see “Configuring System Wide Links" in *Oracle Communications System Administrator's Guide*.

If Oracle BI Publisher is installed as part of the Network Integrity install, then a link to the installed BI Publisher instance is created automatically by the installer. The Network Integrity administrator can edit or remove this link later.

A link to the Change Password page is optionally created by the installer. This link is displayed as the Change Password link. The Network Integrity Administrator can edit or remove this link later. See "About the Change Password Link".

About the Change Password Link

The **Change Password** link is displayed only if the Oracle WebLogic Server Embedded LDAP server is selected as the authentication agent for Network Integrity during the installation.

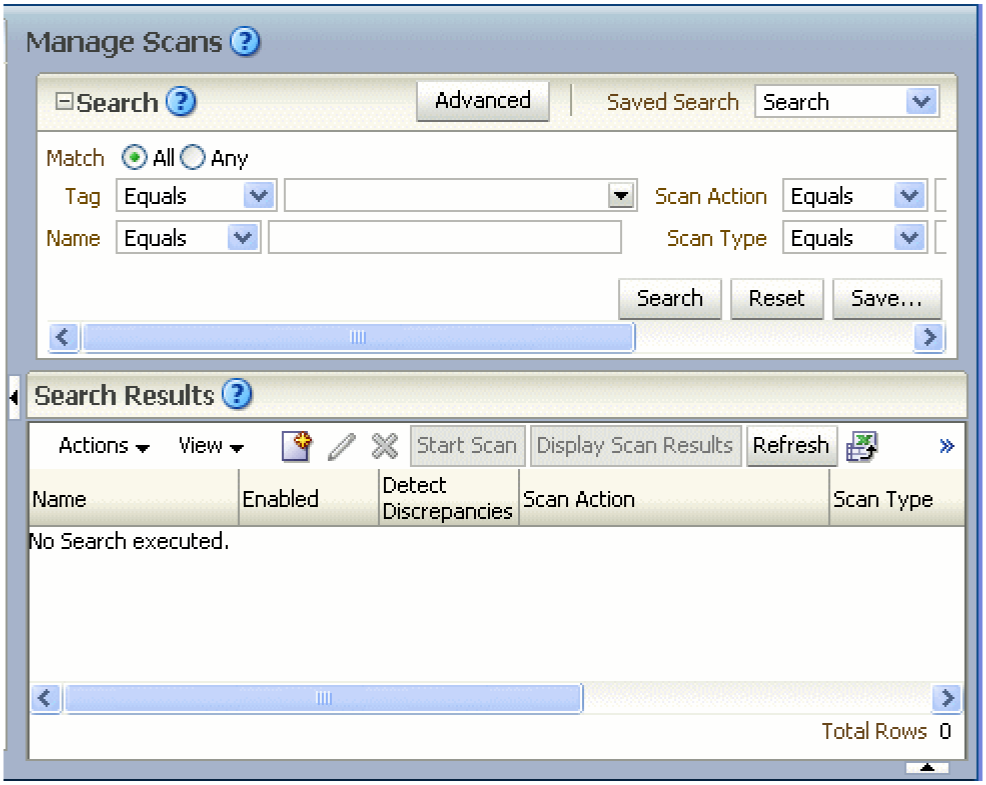
You can click this link to load the **Change Password** page where you can change your password for the Network Integrity UI.

See "Changing Your Password".

About the Local Work Area

The local work area is on the right of the UI. The default work area displays the Manage Scans page when Network Integrity first starts up. When a task link is selected from the Tasks panel, it replaces the local area contents.

The following figure shows the default work area at startup.



Match ● All ○ Any

Tag Equals

Name Equals

Scan Action Equals

Scan Type Equals

Name	Enabled	Detect Discrepancies	Scan Action	Scan Type
No Search executed.				

Total Rows 0

Working with the Network Integrity UI

For information on using the Network Integrity UI, see the following:.

- Navigating the UI
- Using the Integrated Online Help
- Creating a Network Integrity Object
- Editing a Network Integrity Object
- Deleting a Network Integrity Object
- Sorting Data in Tables
- Exporting Data in Microsoft Excel Format
- Logging Out of Network Integrity

Navigating the UI

The Network Integrity UI works entirely inside a single page display. You should not use your web browser buttons; for example: Back, Forward, Refresh, to navigate within the page. If the web browser is used accidentally, simply navigate to the main link, and log on to Network Integrity again if necessary.

Do not open multiple instances of Network Integrity in different tabs of the same browser; either in Internet Explorer, or Mozilla Firefox.

Using the Integrated Online Help

The Network Integrity online Help system features Help topics which are integrated with components of the application.

To select an integrated Help topic:

1. Click the **Help** icon associated with a component.

   The related Help topic appears in the main Network Integrity online Help page within a new browser window.
2. Use the information in the Help topic to configure the Network Integrity component.
3. (Optional) Expand the **Contents** node to view Help subject headings.
4. (Optional) Expand the **Search** node to find a Help topic.
5. Exit the browser window when finished.

Selecting a Help topic replaces any topics currently displayed in the web browser. To display multiple Help topics at the same time, right-click the Help icon and use the browser menu commands.

Creating a Network Integrity Object

To create a Network Integrity object:

1. Click the **Create** icon, or right-click the object and select **Create**.
2. Carry out the configuration required.
3. Click **Save and Close**.

Editing a Network Integrity Object

To edit a Network Integrity object:

1. Select a single object in a Network Integrity table.
2. Click the **Edit** icon, or right-click the object and select **Edit**.
3. Carry out the configuration required.
4. Click **Save and Close**.

Deleting a Network Integrity Object

To delete a Network Integrity object:

1. Select the object in the relevant table.
2. Click the **Delete** icon, or right-click the object and select **Delete**.
3. Confirm the deletion.

Sorting Data in Tables

All table sort operations in Network Integrity are case-sensitive. However, not all columns can be sorted. See "Data Sorting Exceptions".

To sort data in table columns:

1. Hold the mouse pointer over the column header to display arrows for sorting data in ascending (up arrow) or descending (down arrow) order.
2. Select the sorting method required.

Data Sorting Exceptions

On the **Review Discrepancies** page, **Search Results** table, there are a number of columns which do not use the standard sorting method:

- The **Type, Resolution, Status** columns do not sort alphabetically but instead follow their own order.
- The **Discovery Value, Discovery Source, Import Value, Import Source** columns cannot be sorted.

On the **Manage Scans** page, **Search Results** table, the following column does not use the standard sorting method:

- The **Scan Type** column does not sort alphabetically but instead follows its own order.

Exporting Data in Microsoft Excel Format

Certain tables in Network Integrity support the export of data in Microsoft Excel format.

To export data in Microsoft Excel format:

1. Click the Export All Rows to Excel icon on the table toolbar.
2. Carry out one of the following:
   - Open the spreadsheet.
   - Choose a directory into which to save the file and name the spreadsheet.

Logging Out of Network Integrity

To log out of Network Integrity:

1. On the top-level of the interface, click **Logout**.

Changing Your Password

The Change Password page allows a currently logged-in user to change the Network Integrity password. The password is changed using the Oracle WebLogic Server embedded LDAP server.

You can access this page using a pre-configured link in the Links panel.

To change your Network Integrity password:

1. On the **Links** panel, click **Change Password** to open the Password Details dialog box.
2. In the Current Password field, enter your current password.
3. In the New Password field, enter your new password.
4. In the Verify New Password field, confirm your new password.
5. Click **Save and Close**.

See also "About the Change Password Link".

2
Using Scans

This section describes how to use scans in Oracle Communications Network Integrity.

Managing Scans

A scan is a set of configurations that typically includes a scan action and scan action parameters, network addresses (scope), and schedules. A scan is used to perform a Network Integrity operation. After performing a scan, you can view scan results, scan result details, and discrepancies.

Network Integrity supports the following scan types:

- A discovery scan discovers your network: network elements, physical resources, and logical resources
- An assimilation scan produces additional scan results from existing scan results.
- An import scan imports the same data as a discovery scan, but from an inventory system.

If the scan has discrepancy detection enabled, a scan run reports discrepancies by comparing newly discovered network entities with previously imported inventory entities.

When the scan has been created and configured, it is available in the Manage Scans table in the Network Integrity UI.

Related Topics

Creating a Scan

Searching for a Scan

About the Search Results Table

Editing a Scan

Enabling or Disabling a Scan

Deleting a Scan

Creating a Scan

To create a scan:

1. From the Tasks panel, click **Manage Scans**.

   The Manage Scans page appears.

2. Do one of the following:

   - Click the Create icon on the Search Results table.

- From the **Actions** menu, click **Create**.

  The Create Scan page is displayed.

3. On the **General** tab, define scan properties. See "Defining Scan Properties":
4. On the **Scope** tab, define the scope of the scan. See "About the Scope of a Scan":
5. On the **Schedule** tab, define the scan schedule. See "Defining a Scan Schedule":
6. Click **Save and Close**.

Defining Scan Properties

Scan properties are defined on the **General** tab of the Create Scan page.

To define the properties of a scan:

1. In the **Name** field, enter the scan name.
2. (Optional) Select the **Enabled** check box to run the scan using the Start Scan operation or according to a schedule. Deselect the **Enabled** check box to disable the scan.
3. (Optional) Select the **Detect Discrepancies** check box to automatically initiate discrepancy detection at the end of the scan.

   See "About Discrepancy Detection" for more information.
4. In the **Scan Action** field, select the scan action to be associated with this scan.

   The **Scan Type** field will display the associated scan action:

   - Discovery
   - Import
   - Assimilation
5. (Optional) In the **Source** field, enter the data source assigned to the scan. This value is copied into all discrepancies detected by this scan.
6. (Optional) In the **Description** field, enter a description of the scan.
7. In the **Tags** area, associate this scan with one or more tags. See "Tagging a Scan" for more information.
8. In the **Scan Action Parameters** area, set protocol and vendor properties for the scan. The parameters vary according to the selected scan action.

   See "Example: Setting Scan Action Parameters for a Discovery Scan Using SNMP" for an example of setting the scan action parameters for an SNMP scan action type.
9. (Optional) Select the **Auto Resolve Discrepancies** check box to initiate automatic discrepancy resolution at the end of the scan. Automatic discrepancy resolution works only if the **Detect Discrepancies** option is also selected.

   See "About Automatic Discrepancy Resolution" for more information.

Example: Setting Scan Action Parameters for a Discovery Scan Using SNMP

To set protocol and vendor properties for a discovery scan using SNMP:

1. Go to the **Scan Action Parameters** area of the Create Scan page.
2. From the **Select Parameter Group** list, select the required parameter group.
3. Complete the following fields:

- **Version**: Select the supported version of the Simple Network Management Protocol (SNMP) protocol:
  - Version 1
  - Version 2c
  - Version 3
- **Port**: Enter the port through which SNMP communication is carried out. The range of valid port numbers is from 0 to 65535. The default is 161.
- **Community string**: Enter the string used to carry out authentication of clients. The default is *public*. This field applies only to SNMP Version 1 and 2c.
- **Timeout** (seconds): Enter the time between scans. The default is 5.
- **Number of retries**: Enter the number of times that the scan is carried out. The default is zero, that is, the scan is carried out once.
- **V3 User name**: Enter the user name used for authentication. This field applies only to SNMP Version 3.
- **V3 Context Name**: Enter the name of the context used in the SNMP communication. This field applies only to SNMP Version 3.
- **V3 Authentication protocol**: Select the protocol used for authentication. This field is used when the Authentication protocol is set to a value other than *None*. This field applies only to SNMP Version 3.
- **V3 Authentication password**: Enter the password used for authentication. This field is used when the Authentication protocol is set to a value other than *None*. This field applies only to SNMP Version 3.
- **V3 Privacy protocol**: Select the privacy protocol used by the parties to the SNMP communication. This field applies only to SNMP Version 3.
- **V3 Privacy password**: Enter the privacy password used by the parties to the SNMP communication. This field is used only when the V3 Privacy protocol is set to a value other than *None*. This field applies only to SNMP Version 3.

About the Scope of a Scan

The **Scope** tab allows you to view and define the range of data to be discovered, imported, or assimilated, depending on the scan type:

- For a discovery scan, the scope consists of network addresses of devices to be discovered.
- For an import scan, the scope consists of the network address and credentials of your inventory system. You cannot modify the settings for your inventory system on the Scope tab. See "Using Import Systems with Network Integrity" for more information.
- For an assimilation scan, the scope consists of results from discovery, import or assimilation scans.

Related Topics

Defining the Scope of a Scan for a Discovery Scan Action Type

Viewing the Scope of a Scan for an Import Scan Action Type

Using Import Systems with Network Integrity

Defining the Scope of a Scan for an Assimilation Scan Action Type

Defining the Scope of a Scan for a Discovery Scan Action Type

The scope for a discovery scan consists of the network addresses for the devices to be discovered. A discovery scan must have at least one defined network address in its scope.

To define the scope of a discovery scan:

1. Click on the **Scope** tab for a new or saved discovery scan.
2. Enter the scope of the scan using one of the following methods:
   - In the **Scope** field, enter individual values, followed by the **Add** icon.

     Address Handler cartridges can be extended to allow ranges of values to be entered in the **Scope** field.
   - Click the **Import** icon and select a file containing the list of network addresses.

   The scope of a discovery scan can consist of the following types of network addresses:
   - IP Addresses
   - CORBA URLs, in the case of a TMF discovery scan.
   - FTP address, in the case of a File Transfer or File Parsing discovery scan.
3. Click **Save and Close** to confirm the scope definition.

Viewing the Scope of a Scan for an Import Scan Action Type

The scope of an import scan cannot be modified on the **Scope** tab, it can only be viewed. The import system details are displayed by name, address, and user name.

Related Topics:

- Using Import Systems with Network Integrity

Defining the Scope of a Scan for an Assimilation Scan Action Type

The scope for an assimilation scan consists of discovery scan results. An assimilation scan must have at least one defined input discovery scan.

To define an input discovery scan for an assimilation scan action type:

1. Click on the **Scope** tab for a new or saved assimilation scan.
2. Click the **Assign** icon.

   The Assign Scans dialog box appears, showing all available input scans.
3. Select the scans you want to add to the scope of the assimilation scan.

   If any input scans fail, the assimilation is not run.
4. In the **Assimilate Input Scan Results** field, select how input scans are assimilated:
   - To process input discovery scans simultaneously for all scan address and result groups for all scan runs, select **All Scans, All Scan Addresses**.
   - To process input discovery scans in parallel for all scan addresses and result groups by scan run, select **Single Scan, All Scan Addresses**.

- To process input discovery scans in parallel for each scan address by scan run, select **Single Scan, Single Scan Address**.

5. In the **Automatically Run Input Scans** field, select whether input scans are automatically re-run with the assimilation scan:

   - To not re-run input discovery scans before the assimilation scan, no matter how old the scan results are, select **Never**.
   - To re-run all input discovery scans before the assimilation scan, no matter how recent the scan results are, select **Always**.
   - To re-run input discovery scans before the assimilation scan only if the scan results are older than a specified value, select **If Older than** *X*.
   - **If Older than a Custom Age**: input scans are run before the assimilation scan only if the scan results are older than the specified value. Enter the value in Hours, Days, or Weeks. The value cannot exceed one year.
   - To re-run input discovery scans before the assimilation scan only if the scan results are older than a custom value, select **If Older than a Custom Age** and enter a value in Hours, Days, or Weeks.

6. Click **Save and Close**.

Defining a Scan Schedule

The scan schedule determines when a scan is run.

To define a scan schedule:

1. On the Create Scan page, click the **Schedule** tab.
2. Click the **Create** icon on the top-level menu of the **Scan Schedules** pane to display the **Create Schedule** dialog.
3. (Optional) In the **Description** field, enter the name of the schedule.
4. In the **Effective Date** field, enter the date on which the schedule starts.
5. In the **Start Time** field, enter the time at which the schedule starts.
6. In the **Frequency** field, select how often the scan repeats:

   - To define a daily schedule, select **Daily**.
   - To define a weekly schedule, select **Weekly**. You can select multiple days of the week for the schedule to recur.
   - To define a monthly schedule, select **Monthly**. Specify the monthly frequency:

     Click **On Day … from beginning of month** to specify the day of the month using a number in the range 1 to 28. For example, select 6 to repeat the scan on the 6th day of each month.

     Click **On Day … from end of month** to specify a scan schedule with respect to the end of the month. Enter a value in the range 1 to 7. For example, select 7 to repeat the scan on the day that falls seven days before the end of each month.

     Click **On the** to specify the day of the month using an ordinal and the day of the week; for example: the Last Saturday in the month. Supported ordinals are First, Second, Third, Fourth, Fifth, and Last.

   - To define a yearly schedule, select **Yearly**. Specify the yearly frequency:

     Click **On Date** to specify the month and the day; for example, January 24.

Click **On the** to specify the day of the year using an ordinal, the day of the week, and the month; for example, the First Monday of September. Supported ordinals are First, Second, Third, Fourth, Fifth, and Last.

- To define a single occurrence, select **Once Only**. Specify the date and time for the occurrence.

7. Click **OK**.

Assigning a Blackout Window

A blackout window defines a period of time when a specified scan should not run or be paused if it is already running. The scheduling options available for blackout windows are identical to those available for scheduling scans. See "Defining a Scan Schedule" for more information.

To assign a blackout window:

1. On the Create Scan page, select the **Schedule** tab.
2. Click the **+** icon on the top-level menu of the **Blackout Windows** pane.
3. From the Assign Blackout Windows table, select the blackout windows you want to assign. It is possible to assign a number of blackout windows to a particular scan, and to have blackout windows overlap. If there are no blackout windows configured, you may need to create one. See "Creating a Blackout Window" for more information.

   Blackout windows are created, updated, displayed, and executed in server time. The local time zone of the client browser is not used for assigning blackout windows. The Network Integrity server time zone details are provided on the dialog box.
4. Click **Save**.

   The blackout window is added to a table of blackout windows in the **Blackout Windows** pane.
5. Repeat the steps above to assign multiple blackout windows to the scan as required.

   See "Using Blackout Windows" for more information.

Searching for a Scan

You can search for scans using the **Search** pane on the Manage Scans page. The default search mode, **Basic**, offers the most commonly-used search criteria.

The **Advanced** option widens the search by providing other options, as well as allowing extra search fields to be added for complex searches that require multiple values for a particular field.

To search for a scan:

1. Expand the **Search** pane.
2. (Optional). Click **Advanced** to display additional search criteria. See "Carrying Out an Advanced Search for a Scan".
3. Select a saved search from the **Saved Search** list. See "Defining a Saved Search".
4. In the **Match** section, select whether to generate a response that matches *all* of the search criteria, or a response that matches *any* of the search criteria by clicking **All** or **Any**.
5. For each of the search criteria listed, select an operator and enter or select a value. The following operators are available:
   - Equals

- Not Equal
- Starts With (for **Tag** only)

You can use wildcards for text fields. The supported wildcard characters are “*'", “%", and “_". “*" and “%" both represent a match of zero or more characters. “_"represents a match of any single character. Wildcard characters can be escaped with a backslash “\". To insert a backslash in the query, insert two backslashes “\\".

In the **Tag** section, click a single tag identifier, or multiple tag identifiers, as required. A scan matches when it has been tagged with *one or more* of the selected tags. When a parent tag is selected, the children of that tag are automatically selected. Click **All** to search all tags.

6. Click **Search** to carry out the search. The result of the search is displayed in the **Search Results** table.
7. Click **Reset** to restore the saved criteria, operators, and mode of a saved search.

   If the search query selected is Search or Untagged, all of the search fields are cleared and operators are set to their default values.
8. Click **Save And Close** to save the scan search details.

Carrying Out an Advanced Search for a Scan

You can enhance the criteria used to search for a scan by using the **Advanced** search option, or by adding custom fields. See "Adding Search Fields" for more information.

To carry out an advanced search for a scan:

1. Expand the **Search** pane on the **Manage Scans** page.
2. Click **Advanced**.
3. Use the search options. See "Searching for a Scan" for more information.
4. In the **Enabled** section, select whether the scan is enabled.
5. In the **Description** section, enter the description of the scan.
6. In the **Source** section, specify the data source assigned to the scan.
7. In the **Detect Discrepancies** section, select whether discrepancy detection is enabled.
8. In the **Network Address** section, specify the network address, or addresses. Separate addresses using “,"; for example: *FD39:26B1:DA1C:1::1, 2001:0db8:000:000:000:000:1334:54ab, 2001:0db8:000:000:000:1248:57ab*.

   Specify a range of IP addresses by entering *10.10.10.** or *10.10.10.10-30*, for example, or by entering IP addresses separately; for example: *10.15.68.68, 10.15.68.20, 10.15.68.61*.

   A scan matches when one or more of the selected addresses are associated with it.
9. (Optional) Add custom fields to enhance the search functionality. See "Adding Search Fields" for more information.
10. Click **Reset** to restore the saved criteria, operators, and mode of a saved search.

    If the search query selected is Search or All Latest or Untagged, all of the search fields are cleared and operators are set to their default values.
11. Click **Search** to carry out the search. The result of the search is displayed in the **Search Results** table.
12. Click **Save And Close** to save the scan search details.

Adding Search Fields

You can add extra fields when searching for a scan.

To add search fields:

1. Expand the **Search** pane on the **Manage Scans** page.
2. Click **Advanced** to display the advanced search options.
3. Click the arrow on the **Add Fields** button to view the list of available fields.
4. Add any required fields. Save the choices made.
5. Carry out a new search.

Defining a Saved Search

You can refine the search by selecting or defining a particular set of scans.

To define a saved search for a scan:

1. Expand the **Search** pane on the **Manage Scans** page.
2. From the **Saved Search** list, select one of the following:
   - **Search**. Use this to search all scans. This is the default.
   - **Untagged**. Use this to search all untagged scans.
   - **Personalize**. Use this to define a set of scans to search. See "Personalizing a Saved Search" for more information.
   - A custom option.

Personalizing a Saved Search

To define a custom set of scans to search:

1. From the **Saved Search** list, click **Personalize**.

   The Personalize Saved Searches dialog box appears.
2. Edit or delete the saved searches.
3. Select the **Run Automatically** check box.

   The selected search starts immediately.
4. Select the **Show in Search List** check box.

   The selected search is displayed in the **Saved Search** list.
5. Click **Apply**.

About the Search Results Table

The **Search Results** table lists the Network Integrity scans. Each scan is defined by:

- **Name**: the name of the scan
- **Scan Action**: the scan action associated with the scan
- **Scan Type**: the scan type based on the selected scan action:

  - Discovery
  - Import
  - Assimilation
- **Source**: the data source assigned to the scan
- **Status**: the current status of the scan
  - In progress
  - Completed (even if completed with errors)
  - No Scan Status - the scan was never run
- **Scan Error**: the total number of errors encountered during the scan
- Discrepancy type and total number:
  - Critical (denoted by **C**)
  - Major (denoted by **M**)
  - Minor (denoted by **m**)
  - Warning (denoted by **w**)
- **Scan Start Time**: the time at which the scan started; in the form *4 hours ago* or *10 days ago*.
- **Scan Duration**: the time taken for the scan to complete; in the form *1 minute*.
- **Discrepancy Start Time**: (optional) the time at which discrepancy detection was initiated at the end of the discovery scan; in the form *4 hours ago* or *10 days ago*
- **Discrepancy Duration**: (optional) the time for discrepancy detection to complete; in the form *0 seconds*.

Select a scan from the **Search Results** table to carry out these actions:

- Displaying Scan Result Details
- Viewing a Scan Result Detail
- Viewing an Entity Detail
- Displaying Addresses
- Displaying Scan Configurations
- Refreshing the Scan Results View

Editing a Scan

To edit a scan:

1. Click the scan in the **Search Results** table on the **Manage Scans** page.
2. Carry out one of the following to display the **Edit Scan** dialog:
   - From the **Actions** menu, select **Edit**
   - Right-click on the scan and select **Edit**
   - Click the pencil icon
3. Edit the scan. See "Creating a Scan" for more information.
4. Click **Save And Close**.

Related Topics

Editing a Running Scan

Multiple Users Editing a Scan

Editing a Running Scan

You cannot edit a scan while it is running, but you can stop the scan, edit it, and re-run it. The changes will take effect on any subsequent runs of the scan.

To edit a running scan:

1. Click the scan in the **Search Results** table on the **Manage Scans** page.
2. To stop the scan, carry out one of the following:
   - From the **Actions** menu, select **Stop Scan**
   - Right-click on the scan and select **Stop Scan**
3. Edit the scan. See "Creating a Scan" for more information.
4. Click **Save And Close**.
5. Run the scan again. See "Starting a Scan" for more information.

Multiple Users Editing a Scan

If multiple users edit a scan, changes to the scan are committed to the database in the order in which they are made. If a scan is being edited, it may be opened by another user, but the last user to save the scan will receive an error message.

Enabling or Disabling a Scan

You need to enable a scan before you can run it, either manually, or on a schedule. A disabled scan may not be run.

To enable or disable a scan:

1. Select the scan in the **Manage Scans** table.
2. To enable it, from the **Actions** menu, select **Enable**.
3. To disable it, from the **Actions** menu, select **Disable**.

The result of the search is displayed in the **Search Results** table.

Deleting a Scan

To delete a scan:

1. Carry out one of the following:
   - Select a tag in the Scans table, and from the **Actions** menu, select **Delete**

     Or
   - Right-click an existing scan in the Scans table and select **Delete**.
2. Confirm the deletion.

3
Managing Tags

This section describes how to use tags to group scans created using Oracle Communications Network Integrity.

Managing Scan Groups (Using Tags)

You can manage groups of scans using tags, which can relate to geography, ownership, network type, or other reference.

Refer to the following sections:

- Creating a Tag
- Tagging a Scan
- Editing a Tag
- Deleting a Tag

Creating a Tag

To create a tag:

1. Carry out one of the following tasks:
   - Click the **Create** icon on the **Manage Tags** page

     Or
   - Right-click an existing tag in the **Tags** table and select **Create Tag** to display the **Create Tag** dialog box.
2. Complete the following fields:
   - **Name**: the name of the scan group. Scans are usually grouped by device type, network location, and so on. This is a required field.
   - **Parent Tag**: the name of the scan group family to which this tag belongs. Select from the previously configured options, or leave blank, as required. This is an optional field.
   - **Description**: provides some information about the scan group. This is an optional field.
3. Click **Save and Close** to complete the tag configuration or click **Cancel** to exit.

Tagging a Scan

You can manage scans via tags, which can relate to geography, ownership, network type, or other reference.

Each tag displays the names of its parents, followed by its own name, all separated by the character “/". For example, if a scan has been tagged “Supply Chain", and its parent tag is “AceMart", then the displayed tag name is “AceMart/Supply Chain".

To tag a scan:

1. Select the **+** icon in the **Tags** section to display the **Select Tag** dialog.
2. From the tree table of all tags defined in Network Integrity, select the required tag.
3. Click **OK** to confirm the selection. The tag is added to a table of tags in the **General** pane of the **Manage Scan** panel.
4. Repeat the steps above to add multiple tags to the scan as required.

Editing a Tag

To edit a tag:

1. Carry out one of the following tasks:
   - Click **Edit** in the Tags table

     Or
   - Right-click an existing tag and select **Edit**, to display the **Edit Tag** dialog box.
2. Edit the following fields:
   - **Name**: the name of the scan group. Scans are usually grouped by device type, network location, and so on. This is a required field.
   - **Parent Tag**: the name of the scan group family to which this tag belongs. Select from the previously configured options, or leave blank, as required. This is an optional field.
   - **Description**: provides some information about the scan group. This is an optional field.
3. Click **Save and Close** to complete the tag configuration or click **Cancel** to exit.

Deleting a Tag

To delete a tag:

1. Carry out one of the following:
   - Select a tag in the Tags table, and click **Delete**

     Or
   - Right-click an existing tag in the **Tags** table and select **Delete**.
2. Confirm the deletion.

4 Working with Scan Results

This section describes how to work with the results of scans carried out using Oracle Communications Network Integrity.

About Scan Results

This page enables you to use scan results.

Refer to the following sections:

- About the Scan Results Page
- Searching for Scan Results
- About the Search Results Table
- Displaying Scan Result Details
- Viewing a Scan Result Detail
- Viewing an Entity Detail
- Displaying Addresses
- Displaying Scan Configurations
- Refreshing the Scan Results View

About the Scan Results Page

You can use the **Scan Results** page to search for and display a table of scan results. For a selected scan result, it also displays a list of scan result details that you can use to search for discrepancies.

Searching for Scan Results

You can search for scan runs using the **Search** pane on the **Scan Results** page. Use the basic search functionality described in this section, or to enhance the search criteria, click **Advanced**.

To carry out an advanced search for a scan run, there are a number of separate tasks to carry out:

- Specifying the Range and Type of Scans
- Specifying the Scan Name and Associated Scan Action
- Specifying the Scan Status
- Specifying the Scan Type
- Setting the Scan Start and End Times
- Setting the Discrepancy Detection Start and End Times
- Setting the Critical Discrepancy Severity Requirements

- Setting the Major Discrepancy Severity Requirements
- Setting the Minor Discrepancy Severity Requirements
- Setting the Warning Discrepancy Severity Requirements
- Carrying out the Search for the Scan Run

Specifying the Range and Type of Scans

To specify the range and type of scan to return in the search:

1. Expand the **Search** pane.
2. In the **Match** section, select whether to generate a response that matches all of the search criteria, or a response that matches any of the search criteria, by clicking **All** or **Any**.
3. In the **Restrict to Previously Selected Scans** section, check the box to search scan results already selected, or uncheck the box to ignore them. The default is checked: search scan runs already selected.
4. Expand the tag group. Click a single tag, or multiple tags, as required. Multiple tag selections are combined in an OR condition when the query is generated (even when **Match All** is selected in the **Match** section above). When a parent tag is selected, the children are automatically selected.
5. In the **Latest Completed Result Only** section, check the box to return information using only the most recent completed scan run, or uncheck the box to return information using all scan results. The default is checked.

Specifying the Scan Name and Associated Scan Action

To specify the scan name and the scan action associated with the scan:

1. In the **Name** section, enter the name of the scan you are searching for.
2. In the **Scan Action** section, associate the scan with a custom scan action, such as Inventory Import or Discovery, for example.

Specifying the Scan Status

To specify the status of the scan:

1. Go to the **Status** section.
2. Choose one of the following:
   - Running
   - Suspended
   - Completed
   - Stopped
   - Stopping

Specifying the Scan Type

To specify the scan type:

1. Go to the **Type** section.
2. Select the operator.

3. Choose from the list of types.

Setting the Scan Start and End Times

To set the time when the scan began running, and the time when the scan completed:

1. In the **Scan Start Time** fields, set the start time by selecting the required condition:
    - **Not Between**: Specify a range of times during which the scan did not take place.
    - **Before**: Specify a time before which the scan took place
    - **After**: Specify a time after which the scan took place
    - **On or After**: Specify a time on which, or after which, the scan took place. This is the default.
    - **Between**: Specify a range of times during which the scan took place
2. In the **Scan End Time** fields, carry out the same procedure to set the end time for the scan.

Setting the Discrepancy Detection Start and End Times

To set the time when the discrepancy detection job began running, and the time when it completed:

1. In the Discrepancy Detection Start Time field, set the start time by selecting the required condition:
    - **Not Between**: Specify a range of times during which the discrepancy detection job did not take place.
    - **Before**: Specify a time before which the discrepancy detection job took place
    - **After**: Specify a time after which the discrepancy detection job took place
    - **On or After**: Specify a time on which, or after which, the discrepancy detection job took place. This is the default.
    - **Between**: Specify a range of times during which the discrepancy detection job took place
2. Click the calendar icon to display the date and time selector
3. Select the date and time, specifying whether the time is AM or PM.
4. Click **Save** to confirm, or click **Cancel** to exit without saving.
5. In the Discrepancy Detection End Time field, carry out the same procedure for the discrepancy detection job end time.

Setting the Critical Discrepancy Severity Requirements

To set the discrepancy severity requirements:

1. In the **Critical Discrepancies** field, use one of the following conditions:
    - **Equals**: Specify discrepancies of critical severity
    - **Does Not Equal**: Specify discrepancies not of critical severity
    - **Less Than**: Specify discrepancies of a severity lower than critical
    - **Between**: Specify a range of severities

- **Not Between**: Specify a range of severities in which the required severity is not included.

2. Complete the second field by selecting the discrepancy type applicable to the scan.The values on this list depend on the scan action selected.

Setting the Major Discrepancy Severity Requirements

To set the major discrepancy severity requirements:

1. In the **Major Discrepancies** field, use one of the following conditions:
   - **Equals**: Specify discrepancies of major severity
   - **Does Not Equal**: Specify discrepancies not of major severity
   - **Less Than**: Specify discrepancies of a severity lower than major
   - **Greater Than**: Specify discrepancies of a severity higher than major
   - **Between**: Specify a range of severities
   - **Not Between**: Specify a range of severities in which the required severity is not included.
2. Complete the second field by selecting the discrepancy type applicable to the scan.The values on this list depend on the scan action selected.

Setting the Minor Discrepancy Severity Requirements

To set the minor discrepancy severity requirements:

1. In the **Minor Discrepancies** field, use one of the following conditions:
   - **Equals**: Specify discrepancies of minor severity
   - **Does Not Equal**: Specify discrepancies not of minor severity
   - **Less Than**: Specify discrepancies of a severity lower than minor
   - **Greater Than**: Specify discrepancies of a severity higher than minor
   - **Between**: Specify a range of severities
   - **Not Between**: Specify a range of severities in which the required severity is not included.
2. Complete the second field by selecting the discrepancy type applicable to the scan.The values on this list depend on the scan action selected.

Setting the Warning Discrepancy Severity Requirements

To set the warning discrepancy severity requirements:

1. In the **Warning Discrepancies** field, use one of the following conditions:
   - **Equals**: Specify discrepancies of warning severity
   - **Does Not Equal**: Specify discrepancies not of warning severity
   - **Greater Than**: Specify discrepancies of a severity higher than warning
   - **Between**: Specify a range of severities
   - **Not Between**: Specify a range of severities in which the required severity is not included.

2. Complete the second field by selecting the discrepancy types applicable to the scan.The values on this list depend on the scan action selected.

Carrying out the Search for the Scan Run

To search for the scan run:

1. Add custom fields to enhance the search functionality as required. See "Adding Search Fields" for more information.
2. Click **Search** to carry out the search or click **Reset** to revert to the default search options, and clear all input fields.

   The result of the search is displayed in the **Search Results** table. The table is populated with data that matches your search criteria.

About the Search Results Table

The **Search Results** table lists the outcomes for one or more Network Integrity scans. Each scan is defined by:

- **Name**: the name of the scan
- **Scan Action**: the scan action associated with the scan
- **Scan Type**: the scan type based on the selected scan action:
  - Discovery
  - Import
  - Assimilation
- **Source**: the data source assigned to the scan
- **Status**: the current status of the scan
  - In progress
  - Completed (even if completed with errors)
  - No Scan Status - the scan was never run
- **Scan Error**: the total number of errors encountered during the scan
- Discrepancy type and total number:
  - Critical (denoted by **C**)
  - Major (denoted by **M**)
  - Minor (denoted by **m**)
  - Warning (denoted by **w**)
- **Scan Start Time**: the time at which the scan started; in the form *4 hours ago* or *10 days ago*.
- **Scan Duration**: the time taken for the scan to complete; in the form *1 minute*.
- **Discrepancy Start Time**: (optional) the time at which discrepancy detection was initiated at the end of the discovery scan; in the form *4 hours ago* or *10 days ago*
- **Discrepancy Duration**: (optional) the time for discrepancy detection to complete; in the form *0 seconds*.

Select a scan from the **Search Results** table to carry out these actions:

- Displaying Scan Result Details
- Viewing a Scan Result Detail
- Viewing an Entity Detail
- Displaying Addresses
- Displaying Scan Configurations
- Refreshing the Scan Results View

Displaying Scan Result Details

The **Scan Result Details** table lists information discovered as part of the scan. The list displays scan properties, such as name, type, status, duration, as well as an outline of discrepancy types - if discrepancy detection was enabled when the scan was configured was enabled - organized by severity (Critical, Major, Minor, and Warning).

To display scan result details:

1. Click the scan in the **Search Results** table to display the scan result details.
2. Use the **Scan Result Details** table to view, but not to edit, the following information:
   - **Category**: the category of each network element scanned; for example: device
   - **Name**: the device identifier. Click the device identifier to display detailed information about the entity. See "Viewing a Scan Result Detail" for more information.
   - **C**/**M**/**m**/**w**: the discrepancy types organized by severity (Critical, Major, Minor, and Warning), and total numbers
   - **Network Address**: the network address of the device
3. (Optional) Click **Review Discrepancies** to examine discrepancies associated with a device. See "Using Network Integrity to Review Discrepancies" for more information.

Viewing a Scan Result Detail

To view detailed information about a particular device:

- 1. From the **Scan Result Details** table, click a device name (in blue) to display the **Scan Result Detail** page.

     This page displays an entity tree for the device, that is, a hierarchical outline of all device information. The entity tree defines each entity by entity name and type.
  2. Drill down into the entity tree to view a particular root entity. For example, expand a *cisco3640* entity to view the chassis, container slots, cards, and so on.
  3. Click any element in the tree to view the attribute and relationship details of that entity.

See "Viewing an Entity Detail" for more information.

Viewing an Entity Detail

The attribute and relationship details for each element in the entity tree displayed on the **Scan Result Detail** page can be viewed on a separate pane.

To view the attributes and relationships of a particular entity:

- 1. From the **Scan Result Detail** page, select an element in the entity tree to display the **Entity Detail** pane.

The Entity Detail pane opens to the right of the Scan Detail page. Use the arrow icons at the side of each pane to collapse and restore panes as required.

2. Click any color-coded attribute or relationship to link to its location in the entity tree.

   For example, to link to a particular device interface in the entity tree, from the **Device Interfaces** list in the **Relationships** section, click the interface name. The **Scan Result Detail** page refreshes to display the particular device interface within the entity tree.

Displaying Addresses

You can view the list of IP addresses scanned. The list is shown in a read-only dialog, providing failure reasons (if applicable).

To display addresses:

1. Carry out one of the following:
   - Right-click the scan run and select **View Addresses**
   - From the top-level of the Search Results page, select the **View Addresses** tab
2. Use the **Addresses** table to view, but not to edit, the following information:
   - The address for a particular scan
   - The completion status of a particular address scan
   - The reason for an error in the discovery of an individual IP address; for example, a ping timeout
   - The start and end time for a particular scan
3. When you are finished with the dialog, click **Close** to exit.

Displaying Scan Configurations

You can view the original scan configuration parameters. The details are presented in a read-only dialog, showing a list of parameters.

To display the scan configuration:

1. Double-click the scan in the list of scans.
2. Use the following tabs to view, but not to edit, general scan configuration information, such as:
   - **Status**: See "Displaying Scan Status Information " for more information.
   - **General**: See "Displaying Common Scan Parameters " for more information.
   - **Scan Action**: See "Displaying Scan Action Information" for more information.
   - **Scope**: See "Displaying Scan Scope Information " for more information.
   - **Schedule**: See "Displaying Scan Schedule Information " for more information.
   - **Blackout**: See "Displaying Scan Blackout Information" for more information.
3. When you have viewed the scan configuration, you can carry out the following actions on the scan:
   - Click **Review Discrepancies** to review the discrepancies associated with the scan.

     See "Using Network Integrity to Review Discrepancies".

- Click **Display Scan Result** to view the results of the scan.

  See "Displaying Scan Result Details".

Displaying Scan Status Information

To display the status of a completed scan:

1. Double-click the scan run in the **Search Results** table.
2. Click the **Status** tab to view the following information:
   - **Scan Progress**: the overall status of the scan: this takes one of the values: Running, Stopped, Suspended, Completed, or Cancelled.
     - **Progress**: a progress bar indicating the percentage completion of the scan.
     - **Total**: the total number of scans completed.
     - **In Progress**: the total number of scans still in progress when the scan result details were requested.
     - **Error**: the total number of errored device scans.
     - **Start Time**: the time at which the scan started; in the form *4 hours ago* or *10 days ago*.
     - **Duration**: the time taken for the scan to complete; in the form *1 minute*.
     - **Actual Start Time**: the time at which the scan started, in the form MM-DD-YYYY HH:MM:SS AM/PM; for example: 08-19-2010 4:59:37 PM.
     - **Actual End Time**: the time at which the scan ended, in the form MM-DD-YYYY HH:MM:SS AM/PM; for example: 08-19-2010 5:01:36 PM.
   - **Discrepancy Detection Progress**: the status of the discrepancy detection process (if selected).
     - **Progress**: a progress bar indicating the percentage completion of the discrepancy detection.
     - **Total**: the total number of discrepancy detections completed.
     - **In Progress**: the total number of discrepancy detections still in progress when the scan result details were requested.
     - **Error** lists the number of discrepancy detection processes that have run unsuccessfully.

       To investigate discrepancy detection failures, refer to the server logs from the Network Integrity application. See *Network Integrity System Administrator's Guide* for further information about logging.

       The designer of the cartridge pack should also be able to provide information about the cause of these errors.
     - **Start Time**: the time at which discrepancy detection was initiated at the end of the discovery scan; in the form *4 hours ago* or *10 days ago*.
     - **Discrepancy Duration**: the time taken for discrepancy detection to complete; in the form *0 seconds*.
     - **Actual Start Time**: the time at which discrepancy detection started, in the form MM-DD-YYYY HH:MM:SS AM/PM; for example: 08-19-2010 5:01:36 PM.
     - **Actual End Time**: the time at which the discrepancy detection ended, in the form MM-DD-YYYY HH:MM:SS; for example: 08-19-2010 5:01:36 PM.

- **Discrepancy Counts**: the total number and type of discrepancies.
  - Critical (denoted by **C**)
  - Major (denoted by **M**)
  - Minor (denoted by **m**)
  - Warning (denoted by **w**)

3. Click **Review Discrepancies** to examine discrepancies associated with a device. See "Using Network Integrity to Review Discrepancies" for more information.

Displaying Common Scan Parameters

The top half of the **General** tabbed pane shows parameters common to all scans. The bottom half shows scan action parameters defined by cartridge pack developers. See "Displaying Scan Action Information" for more information.

To display the common properties and the tag list of a scan:

1. Double-click the scan run in the **Search Results** table.
2. Click the **General** tab to view the following information:
   - **Name**: The scan identifier.
   - **Enabled**: If the box is checked, the scan is enabled to be started. If the box is not checked, the scan could not be executed.
   - **Detect Discrepancies**: If this box is checked, discrepancy detection is automatically initiated at the end of the discovery scan. If the box is not checked, discrepancy detection did not occur.
   - **Scan Action**: The custom scan action associated with the scan; for example: Cisco Router or UIM Inventory.
   - **Scan Type**: A scan type based on the selected scan action. It may be one of the following:
     - Discovery
     - Import
     - Assimilation
   - **Source**: The data source assigned to the scan.
   - **Description**: A textual description of the scan.
   - **Tags**: Shows the tag list associated with this scan. See "Tagging a Scan" for more information.

Displaying Scan Action Information

The bottom half of the **General** tabbed pane shows scan action parameters defined by cartridge pack developers. The top half shows parameters common to all scans. See "Displaying Common Scan Parameters " for more information.

To display the scan action configuration details of the selected scan:

1. Double-click the scan run in the **Search Results** table.
2. Click the **Scan Action** tab to view the following information for the SNMP scan action:

3. - **Version**: The version of the Simple Network Management Protocol (SNMP) protocol selected:
     – Version 1
     – Version 2c
     – Version 3
   - **Community string**: A string used to carry out authentication of clients.
   - **Number of retries**: The number of times that the scan was carried out. The default is zero, that is, the scan was carried out once.
   - **Timeout** (seconds): The time between scans. The default is 5.
   - **Port**: the port through which SNMP communication was carried out. The range of valid port numbers is from 0 to 65535. The default is 161.
   - **User name**: the user name used for authentication.
   - **Authentication password**: A password used for authentication. This field applies only to SNMP Version 3.
   - **Authentication protocol**: A protocol used for authentication. This field applies only to SNMP Version 3.
   - **Privacy protocol**: A privacy protocol used by the parties to the SNMP communication. This field applies only to SNMP Version 3.
   - **Privacy password**: A privacy password used by the parties to the SNMP communication. This field applies only to SNMP Version 3.
   - **Context Name**: The name of the context used in the SNMP communication. This field applies only to SNMP Version 3.

Displaying Scan Scope Information

To display the scope parameters of the selected scan:

1. Double-click the scan run in the **Search Results** table.
2. Click the **Scope** tab to view the following information per scan type:
3. - Discovery/Import scan types: Displays a table listing columns of network addresses or network address ranges.
   - Assimilation scan type: Displays a table listing input scan details:
     – **Scan Name**: The scan identifier.
     – **Scan Action**: The custom scan action associated with the scan; for example: Cisco Router or UIM Inventory.
     – **Scan Type**: A scan type based on the selected scan action. It may be one of the following:
     – **Source**: The data source assigned to the scan.
     – **Description**: A textual description of the scan.

Displaying Scan Schedule Information

All times refer to the time on the Network Integrity server, as shown on the dialog. Scans are created, updated, displayed, and executed in server time. The local time zone of the client browser is not used for scheduling scans.

To display the schedule configuration for the selected scan:

1. Click **Display Scan** in the **Search Results** table.
2. Click the **Schedule** tab to view the following information:
   - **Description**: A description of the schedule.
   - **Effective Date**: The schedule begins on this date.
   - **Start Time**: The time at which the schedule starts.
   - **Frequency**: Shows how often the schedule takes place. The options are:
   - - **Daily**: The time of day in 24 hour format.
     - **Weekly**: The day on which the schedule applies.
     - **Monthly**: The day of the month on which the schedule applies.
     - **Yearly**: The day of the year on which the schedule applies.
     - **Once Only**: A time and date on which the schedule applies on one occasion only.
   - **Recurrence Pattern**: Shows the recurrence pattern. See "Defining a Scan Schedule" for more information.

     If the scan has no schedules associated with it, the **Scan Schedules** table displays “No Schedules"**.**
3. Click **Close** to exit the dialog.

Displaying Scan Blackout Information

All times refer to the time on the Network Integrity server, as shown on the dialog. Blackout windows are created, updated, displayed, and executed in server time. The local time zone of the client browser is not used for scheduling blackout windows.

To display the blackout windows assigned to the selected scan:

1. Double-click the scan run in the **Search Results** table.
2. Click the **Blackout** tab to view the following information:
   - **Description**: A description of the blackout schedule.
   - **Effective Date**: The blackout schedule begins on this date.
   - **Start Time**: The time at which the blackout schedule starts.
   - **Frequency**: Select the recurrence pattern. The options are:
   - - **Daily**: The time of day in 24 hour format.
     - **Weekly**: The day on which the blackout schedule applies.
     - **Monthly**: The day of the month on which the blackout schedule applies.
     - **Yearly**: The day of the year on which the blackout schedule applies.
     - **Once Only**: A time and date on which the blackout schedule applies on one occasion only. This is the default.
   - **Recurrence Pattern**: Shows the recurrence pattern. See "Creating a Blackout Window" for more information.
   - **Duration**: The time period covered by the blackout schedule:
     - **Days**: The number of days for which the blackout window applies.

- **Hours**: The number of hours for which the blackout window applies.
- **Minutes**: The number of minutes for which the blackout window applies.

Refreshing the Scan Results View

The table that displays scan results is not auto-refreshed. On the top-level of the **Search Results** pane, click **Refresh** to repeat the last executed search (including Display Scan Results, if there were no search criteria entered in the Search pane).

5

Discovering Devices

This section describes how to use Oracle Communications Network Integrity to discover devices.

About Discovering Devices

Discovery is the process of scanning a live network to discover a set of individual IP addresses or particular network equipment. The discovery process is carried out by associating the scan with a particular protocol, such as SNMP, TL1, or CORBA, with custom scan actions, such as MIB II, and with vendor-specific properties, if required. Both the scope of the scan and the details of its recurrence are also configured through the scan profile. After the scan is complete, the discovered data results are output in MTOSI or MTNM XML format.

Starting a Scan

To start a scan:

1. Click the scan you want to start in the Manage Scans table.
2. Carry out one of the following:
   - From the **Actions** menu, select **Start Scan**
   - Right-click the scan and select **Start Scan**
   - Click the **Start Scan** button.

   The scan is executed immediately.

The scan is started immediately.

Related Topics

Stopping a Scan

Editing a Scan

Stopping a Scan

To stop a running scan:

1. Select the scan you want to stop in the Manage Scans table.
2. Carry out one of the following:
   - From the **Actions** menu, select **Stop Scan**
   - Right-click the scan and select **Stop Scan**
   - Click the **Stop Scan** button.

A running scan does not stop immediately when you click **Stop Scan**. If a processor had already started before you clicked **Stop Scan**, the processor continues to run until its completion; the next processor in the sequence looks for the value of the set condition and the custom code in its invoke method, which will stop the processor; if the condition is **True**, the scan is stopped before the next processor starts and all the results of the scan are deleted.

See *Network Integrity Developer's Guide* for more information about adding the custom code in the processor's invoke method to stop the processor.

Related Topics

Starting a Scan

Editing a Scan

Viewing a Scan Status

To view the status of a completed scan or to monitor the status of a running scan, click the scan you want to view in the Manage Scans table. The **Scan Status** information is generated in the bottom section of the Manage Scans page.

- The scan heading takes the form **Scan**: *Scan_Name*. Scan completion status is shown under the tabs in the form **Scan Status**: *Completed*/*In progress*.
- The **Progress** bar, in blue, shows the progress of a live scan in percentage terms. When it reaches 100 per cent, scan status changes to **Completed**.
- **Start Time** displays the time at which the scan commenced. The time is displayed in the format MM-DD-YYYY HH:MM:SS, and specifies the local time zone and year; For example, 2009-07-12 3:45:00 PM.
- **End Time** displays the time at which the scan ended. The time is displayed in the format MM-DD-YYYY HH:MM:SS, and specifies the local time zone and year; For example, 2009-07-12 4:12:13 PM.
- **Duration** lists the time taken for the scan to complete. The time is displayed in the format DDd HHh MMm SSs, where the capital letters are numeric values corresponding to day, hour, minute, and second, and the lower case letters are printed verbatim; For example: 2d 7h 14m 22s. The bigger units will not be printed if they are 0; For example: 27m 13s.
- **Total** indicates the total number of network addresses that this scan has processed.
- **In Progress** indicates the total number of network addresses that are actively being processed by the scan.
- **Completed** indicates the total number of network addresses for which the scan has completed.
- **Error** indicates the total number of network addresses for which the scan has failed.

To view further details of a scan result, such as the object tree for a particular scanned device, see "Viewing the Details of a Scan Result" for more information.

To view discrepancy detection, see "About Discrepancy Detection" for more information.

Viewing the Details of a Scan Result

By clicking an individual device in a scan run, you can display a tree browser called the Object Tree that lists the device, the device type, and all of its children and their individual device types.

For example, by clicking an equipment, you can drill down to its constituent shelves, slots, cards and ports. Each device type is identified by a different icon, and the object display is tiered at the level of each device type to make the relationships more obvious.

By clicking an individual object in the Object Tree, for example: a card, a read-only dialog is displayed that outlines the name and type of the card, as well as other identifying information such as its part number and serial number, and lists its child equipments (if any) and other hierarchical information, such as the ports listed on the card.

6 Detecting Discrepancies

This section describes how to use Oracle Communications Network Integrity to detect discrepancies.

About Discrepancy Detection

Discrepancy detection is the process of comparing discovered data with imported data and enumerating any differences between the sets of data.

The discrepancy detection process is part of a scan configuration. You can configure a manual scan or a scheduled scan that detects discrepancies.

To configure a scan to detect discrepancies, create or configure a scan and select the **Detect Discrepancies** option when defining scan properties. The discrepancy detection process will start at the conclusion of the scan on which it is enabled. See "Defining Scan Properties" for more information.

You can configure discrepancy detection on import scans, discovery scans, or assimilation scans. Because discrepancy detection compares data, ensure that you enable discrepancy detection on the last scan before your scan data is complete.

For example, if you are planning to run an import scan, followed by a discovery scan, followed by an assimilation scan, configure the assimilation scan with the **Detect Discrepancies** option selected.

Viewing Discrepancy Results

The results of the discrepancy detection process are displayed in the result of a scan. To view the discrepancy detection progress report, click the scan you wish to view in the Manage Scans table. The **Scan Status** information is generated in the final section of the Manage Scans table, and is divided into three separate reports:

- **Scan Progress**
- **Discrepancy Detection Progress**
- **Discrepancy Counts**

See "Viewing a Scan Status" for more information on the Scan Progress report.

- **Total** displays how many times the discrepancy detection process has been run (the scan may also be in progress).
- **In Progress** shows whether the discrepancy detection process is currently running. If this value is zero, this scan is not currently running.
- **Completed** displays the number of discrepancy detection processes that have run successfully.
- **Error** lists the number of discrepancy detection processes that have run unsuccessfully.

To investigate discrepancy detection failures, refer to the server logs from the Network Integrity application. See *Network Integrity System Administrator's Guide* for further information about logging.

The designer of the cartridge pack should also be able to provide information about the cause of these errors.

- **Critical** lists the discrepancies with a severity of critical. This is the highest discrepancy severity.
- **Major** lists the discrepancies with a severity of major.
- **Minor** lists the discrepancies with a severity of minor.
- The **Progress** bar, in blue, shows the progress of the discrepancy detection process in percentage terms. When it reaches 100 per cent, the status changes to **Completed**.
- **Start Time** displays the time at which the discrepancy detection process commenced. The time is displayed in the format YYYY-MM-DD HH:MM:SS, and specifies the local time zone and year; For example, 2009-03-12 04:13:00.
- **End Time** displays the time at which the discrepancy detection process ended. The time is displayed in the format YYYY-MM-DD HH:MM:SS, and specifies the local time zone and year; For example, 2009-03-12 04:18:24.
- **Duration** lists the time taken for the discrepancy detection process to complete. The time is displayed in the format (DD) (HH) MMm SSs; For example, 5m 24s.
- **Warning** lists the discrepancies with a severity of warning. This is the lowest discrepancy severity.

To review the discrepancies discovered during a scan:

- Select **Review Discrepancies** from the list of tasks.
- Select **View Latest Scan Results** from the list of tasks. From the **Scan Results** page, select a scan in the **Search Results** table.

  Click the **Review Discrepancies** tab.
- Select **Manage Scans** from the list of tasks. From the **Manage Scans** page, select a scan in the **Search Results** table.

  Click the **Review Discrepancies** tab.

See "Using Network Integrity to Review Discrepancies" for more information.

7 Using Network Integrity to Review Discrepancies

This section describes how to use Oracle Communications Network Integrity to review discrepancies.

About Discrepancy Resolution

Discrepancy resolution is the process of addressing discrepancies reported by Network Integrity. For more information about how Network Integrity discovers discrepancies, see "About Discrepancy Detection".

You can configure import scans, discovery scans, and assimilation scans to automatically resolve discrepancies. See "About Automatic Discrepancy Resolution" for more information.

You can manually review, correct (in the network or inventory), ignore, and edit discrepancies manually. When manually working with discrepancies, see the following topics:

- Searching for Discrepancies
- Viewing Discrepancy Details: the Search Results Table
- Editing Discrepancies
- Correcting Discrepancies
- Sending Discrepancies to an External System
- Ignoring Discrepancies
- Canceling Discrepancy Resolutions
- Submitting Discrepancies
- Viewing an Entity Tree
- Viewing Entity Detail Panes

About Automatic Discrepancy Resolution

If your system administrator has enabled automatic discrepancy resolution, you can configure a manual or scheduled scan to automatically resolve discrepancies. Your system administrator has already pre-configured the types of discrepancies that can be resolved.

You can configure automatic discrepancy resolution on any scan with the **Discrepancy Detection** option selected.

To configure a scan to automatically resolve discrepancies, create or configure a scan and select the **Detect Discrepancies** and **Auto Resolve Discrepancies** options when defining the scan properties. The automatic discrepancy resolution process will start after discrepancy detection is complete. See "Defining Scan Properties" for more information.

Searching for Discrepancies

You can search for discrepancies using the **Search** pane on the Review Discrepancies page. The **Search Results** pane on the Review Discrepancies page displays a list of discrepancies generated by a search operation.

The default text operator is **Equals**. The default date condition is **On or After**.

To search a scan run for discrepancies:

1. Expand the **Search** pane.
2. In the **Match** section, select whether to generate a response that matches all of the search criteria, or a response that matches any of the search criteria by clicking **All** or **Any**.
3. In the **Restrict to Previously Selected Results** section, check the box to search the set of scan results already selected on other pages, or uncheck the box to ignore them. The default is checked.

   > **Note:**
   >
   > This option is presented only if you navigate to this page by selecting **Review Discrepancies** on the **Manage Scans** or **Scan Results** pages.

4. In the **Last Completed Result Only** section, check the box to return information using only the most recent scan run or uncheck the box to return information using all scan results. The default is unchecked: return information using all scan results.
5. In the **Tag** section, select the required tags as follows:
   1. Expand the tag group
   2. Select a single tag, or multiple tags, as required. Multiple tag selections are combined in an OR condition when the query is generated (even when **Match All** is selected in the **Match** section above). When a parent tag is selected, the children are automatically selected.
6. In the **Severity** section, select the required severity as follows:
   1. Select the operator.
   2. Choose from Critical, Major, Minor, Warning.
7. In the **Status** section, select the required status as follows:
   1. Select the operator.
   2. Choose the discrepancy status from:

   - **Failed**: This status indicates that the discrepancy resolution operation has failed.
   - **Ignored**: This status indicates that the discrepancy should be ignored.
   - **Not Implemented**: This status indicates that the operation was delivered to a scan action that did not handle it.
   - **Opened (blank)**: This status indicates that the discrepancy has been raised. This is the default state for newly detected discrepancies.
   - **Processed**: This status indicates that the discrepancy resolution operation has been successfully processed.

   - **Ready**: This status indicates that a corrective operation has been identified for this discrepancy.
   - **Received**: This status indicates that the discrepancy resolution scan action has received the resolution operation, but has not yet determined the outcome.
   - **Submitted**: This status indicates that the discrepancy has been submitted for resolution.

8. In the **Resolution Action** section, select the required resolution as follows:
   a. Select the operator.
   b. Choose the action; for example: *Correct in UIM*.
9. In the **Owner** section, select the required owner as follows:
   a. Select the operator.
   b. Enter the name of the discrepancy owner if known.
10. In the **Priority** section, select the assigned priority as follows:
    a. Select the operator.
    b. Enter the name of the priority if known.
11. In the **Entity Name** section, select the required discrepancy name as follows:
    a. Select the operator.
    b. Enter the name of the object on which the reconciliation has been carried out. This defaults to the object on which the scan run was done.
12. In the **Scan Result Detail Name** section, select the required discrepancy name as follows:
    a. Select the operator.
    b. Enter the name of the discrepancy result.
13. In the **Scan Name** section, select the name of the required scan as follows:
    a. Select the operator.
    b. Enter the scan name.
14. When you have completed the configuration, carry out one of the following:
    - Click **Search** to carry out the search.
    - Click **Reset** to revert to the default search options and clear all input fields.
    - Click **Save** to display the **Create Saved Search** dialog. Enter the name of the search. Check the **Run Automatically** field to run the search on saving. Click **OK** to confirm the search creation or click **Cancel** to exit the dialog without saving the search.

The result of the search is displayed in the **Search Results** pane on the **Review Discrepancies** page.

Using an Advanced Search

It is possible to enhance the criteria used to search a scan run by using the **Advanced** search option or by adding custom fields. See "Adding Search Fields" for more information.

To use advanced features to search a scan run:

1. Expand the **Search** pane on the Review Discrepancies page.
2. Click **Advanced**.

3. In the **Type** section
    a. Select the operator.
    b. Choose from the list of types:

        Assoc +: indicates an extra association

        Assoc -: indicates a missing association

        Assoc Order: indicates an association ordering error

        Attribute: indicates an attribute value mismatch

        Entity +: indicates an extra entity

        Entity -: indicates a missing entity

        Order: indicates an ordering error
4. In the **Attribute/Relationship** section:
    a. Select the operator.
    b. Enter the attribute/relationship name.
5. In the **Submitted Time** section, set the time at which the discrepancy was submitted
    a. Select the operator for the submitted time.
    b. Use the calendar to set the time.
6. In the **Last Status Change Time** section, set the time at which the discrepancy status was last changed:
    a. Select the operator.
    b. Use the calendar to set the time.
7. In the **Entity Type** section, select the entity type as follows:
    a. Select the operator.
    b. Enter the type of entity on which the reconciliation has been carried out.
8. In the **Corrected by** section:
    a. Select the operator.
    b. Enter the name of the person who corrected the discrepancy.
9. In the **Submitted by** section:
    a. Select the operator.
    b. Enter the name of the person who submitted the discrepancy.
10. In the **Parent Entity Name** section, select the name of the parent entity as follows:
    a. Select the operator.
    b. Enter the name of the parent entity.
11. In the **Parent Entity Type** section, select the parent entity type as follows:
    a. Select the operator.
    b. Enter the parent entity type.
12. In the **Discovery/Import Value** section:
    a. Select the operator.
    b. Enter the inventory or discovered scan value name.

13. In the **Discovery/Import Source** section:
    1. Select the operator.
    2. Enter the inventory source or discovered scan source.
14. In the **Scan Result Detail Category** section, select the type of the required scan result detail as follows:
    1. Select the operator.
    2. Enter the scan result detail type.
15. In the **Scan Start Time** section, set the time at which you want to start the search of the scan results:
    1. Select the operator.
    2. Use the calendar to set the time.
16. In the **Scan End Time** section, set the time at which you want to end the search of the scan results:
    1. Select the operator.
    2. Use the calendar to set the time.
17. In the **Discrepancy Detection End Time** section, set the time at which you want to end the search of the discrepancy detection process:
    1. Select the operator.
    2. Use the calendar to set the time.
18. In the **Discrepancy Detection Start Time** section, set the time at which you want to start the search of the discrepancy detection process:
    1. Select the operator.
    2. Use the calendar to set the time.
19. In the **Scan Type** section, select the type of the required scan as follows:
    1. Select the operator.
    2. Enter the scan type.
20. When you have completed the configuration, carry out one of the following:
    - Click **Search** to carry out the search.
    - Click **Reset** to revert to the default search options and clear all input fields.
    - Click **Save** to display the **Create Saved Search** dialog. Enter the name of the search. Check the **Run Automatically** field to run the search on saving. Click **OK** to confirm the search creation or click **Cancel** to exit the dialog without saving the search.
    - Click Add to define custom fields to enhance the search functionality. See "Adding Search FieldsAdding Search Fields" for more information,

The result of the search is displayed in the **Search Results** pane on the **Review Discrepancies** page.

Adding Search Fields

To add fields to enhance the search functionality:

1. Expand the **Search** pane on the Scan Results page.

2. Click **Advanced**.
3. Click **Add Fields**.
4. Add any required fields. Save the choices made.
5. Carry out a new search.

Viewing Discrepancy Details: the Search Results Table

The **Search Results** pane on the Review Discrepancies page displays a list of discrepancies generated by a search operation.

To view the discrepancies detected during a scan, search for discrepancies. See "Searching for Discrepancies" for more information.

From the **Search Results** pane on the Review Discrepancies page, you can edit discrepancies, correct discrepancies, and submit discrepancy resolutions.

Related Topics:

- Editing Discrepancies
- Sending Discrepancies to an External System
- Correcting Discrepancies
- Ignoring Discrepancies
- Canceling Discrepancy Resolutions
- Submitting Discrepancies

The **Search Results** pane on the Review Discrepancies page displays the following information about discrepancies:

- **Scan Result Detail Name** displays the name by which the scan result detail is recognized in the network and on the Entity Tree.
- **Scan Result Detail Category** displays the scan result detail category.
- **Entity Name** displays the name by which the object is recognized in the network and on the Entity Tree.
- **Entity Type** displays the type by which the object is recognized in the network and on the Entity Tree.
- **Entity Attribute/Relationship** denotes the relationship between the entity and its attribute. The attribute/relationship field is blank when the discrepancy is one of the following types:
  - Extra Entity
  - Missing Entity
  - Ordering Error

  As you can define new attributes and relationships when creating discovery and inventory cartridge packs, any values are possible. Examples might include:
  - Subnet Mask
  - Duplex
  - Serial Number
- **Discovery Value/Entity** displays the value of the attribute or entity named by the Attribute/Relationship.

- **Import Value/Entity** displays the value of the attribute or entity named by the Attribute/ Relationship.
- **Type** displays the discrepancy type:
  - Assoc +: indicates an extra association. This is equivalent to Entity +, but for a relationship not owned by the parent entity., that is, the target entity is not a dependent child. The inventory entity may or may not exist; the relationship is missing in inventory.

    Assoc +

  - Assoc -: indicates a missing association. This is equivalent to Entity -, but, but for a relationship not owned by the parent entity, that is, the target entity is not a dependent child. The network entity may or may not exist; the relationship is missing in network.
  - Assoc Order: indicates an association ordering error. In some cases, ordering of associated entities is significant. This discrepancy is applied to the parent entity and indicates that matched associations appear in a different order in network and inventory.
  - Attribute: indicates an attribute value mismatch. For a given entity present in both network and inventory, a specific attribute does not have the same value. This can include the case where one or the other value is missing. Where multiple attributes on the same entity do not match, multiple discrepancies are generated.

    Attribute

  - Entity +: indicates an extra entity, that is, an entity (and any dependent children) is present in network but not in inventory.

    Entity +

  - Entity -: indicates a missing entity, that is, an entity (and any dependent children) is present in inventory but not in network.

    Entity -

  - Order: indicates an ordering error. In some cases, ordering of child entities is significant. This discrepancy is applied to the parent entity and indicates that matched entities appear in a different order in network and inventory.
- **Severity** lists discrepancies in decreasing order of color-coded severity:
  - Critical (C)

    Critical

  - Major (M)

    Major

  - Minor (m)

  - Warning (w)

- **Priority** displays the priority for a particular discrepancy in this field.
- **Resolution Action** indicates where the discrepancy has been resolved:
  - In inventory
  - In the network
  - In an external system
- **Status** displays discrepancy status:
  - **Failed**: This status indicates that the discrepancy resolution operation has failed. You take no action with a discrepancy of this status.
  - **Ignored**: This status indicates that the discrepancy should be ignored. Right-click the discrepancy and select **Ignore**.
  - **Not Implemented**: This status indicates that the operation was delivered to a scan action that could not resolve it because resolution for this type of entity is not supported. You take no action with a discrepancy of this status.
  - **Opened (blank)**: This status indicates that the discrepancy has been raised. This is the default state for newly detected discrepancies. You take no action with a discrepancy of this status.
  - **Processed**: This status indicates that the discrepancy resolution operation has been successfully processed. You take no action with a discrepancy of this status.
  - **Ready**: This status indicates that a corrective operation has been identified for this discrepancy. Right-click the discrepancy and select one of the following:
    - **Correct Inventory**
    - **Correct Network**
    - **Send to External System**
  - **Received**: This status indicates that the discrepancy resolution scan action has received the resolution operation, but has not yet determined the outcome. You take no action with a discrepancy of this status.
  - **Submitted**: This status indicates that the discrepancy has been submitted for resolution. You take no action with a discrepancy of this status.
- **Owner** identifies the person responsible for the discrepancy.
- **Discovery Source** displays the name of the discovery source in which this discrepancy is present.
- **Import Source** displays the name of the import source in which this discrepancy is present.

Editing Discrepancies

The actions available when editing discrepancies depend whether you are:

- Editing a single discrepancy. See "Editing a Single Discrepancy" for more information.

- Editing a number of discrepancies. See "Editing Multiple Discrepancies" for more information.

Editing a Single Discrepancy

To edit a single discrepancy:

1. Select the discrepancy you wish to edit in the **Search Results** table.
2. From the **Actions** menu at the top of the table, select **Edit**, or right-click the discrepancy and select **Edit**.
3. Carry out the following:
   a. Assign the person responsible for the discrepancy in the **Owner** field.
   b. Edit the **Priority** field for the discrepancy.
   c. Edit the **Notes** field to add extra information about the discrepancy.

      When you create a note, a note icon is added to the **Notes** field for the discrepancy, indicating the presence of Notes text.

      The tooltip shows the content of the note.
4. Click **Save and Close** to commit the revised discrepancy, or click **Cancel** to exit without changes.

Editing Multiple Discrepancies

When there are multiple selected discrepancies, you can only take an action that can be applied to *all* selected discrepancies, based on all of their status values.

For example, if there are three selected discrepancies, and one discrepancy has a status of Ignored, and two discrepancies have the status of Identified/Ready, then the actions you can take are:

- Correct Import System
- Correct Network System
- Send to External System
- Cancel Resolution

That is, you can take any action except Ignore. If the three selected discrepancies have status of Submitted and Opened, then you can take no action.

To edit a number of discrepancies at the same time:

1. Select the rows corresponding to the discrepancies you wish to edit in the **Search Results** table. Multiple rows may be selected using the mouse and the Ctrl button.
2. From the **Actions** menu at the top of the **Search Results** table, select **Edit**, or right-click the discrepancy and select **Edit**.
3. Carry out the following:
   a. Assign the person responsible for the discrepancies in the **Owner** field.

   b. Edit the **Priority** field for the discrepancies.

   c. Edit the **Notes** field to add extra information about the discrepancies.

      When you create a note, a note icon is added to the **Notes** field for the selected discrepancies, indicating the presence of Notes text.

      The tooltip shows the content of the note.

4. Select **Overwrite** to overwrite previous values, or select **Append** to add to the existing information.

5. Click **Save and Close** to commit the revised discrepancies, or click **Cancel** to exit without changes.

Correcting Discrepancies

To correct discrepancies on the network, or in inventory:

1. Select a discrepancy or a number of discrepancies on the **Search Results** pane on the Review Discrepancies page.

2. Carry out one of the following options:

   - From the **Actions** menu, select one of the following options:
     - **Correct Inventory**
     - **Correct Network**
   - Right-click the discrepancy, and select one of the following options:
     - **Correct Inventory**
     - **Correct Network**

Sending Discrepancies to an External System

To send discrepancies to an external system:

1. Select a discrepancy or a number of discrepancies on the **Search Results** pane on the Review Discrepancies page.

2. Carry out one of the following options:

   - From the **Actions** menu, select **Send to External System**.
   - Right-click the discrepancy, and select **Send to External System**.

Ignoring Discrepancies

To ignore discrepancies:

1. Select a discrepancy or a number of discrepancies on the **Search Results** pane on the Review Discrepancies page.

2. Carry out one of the following options:

- From the **Actions** menu, select **Ignore**.
- Right-click the discrepancy, and select **Ignore.**

When the status of a discrepancy is set to Ignore, the color of the text in the table row is set to gray.

Canceling Discrepancy Resolutions

To cancel discrepancy resolutions:

1. Select a discrepancy or a number of discrepancies in the **Search Results** table on the Review Discrepancies page.
2. Carry out one of the following options:
   - From the **Actions** menu, select **Cancel Resolution**
   - Right-click the discrepancy, and select **Cancel Resolution.**

Submitting Discrepancies

All discrepancies of status Ready can be submitted. A discrepancy is set to Ready status by one of the following actions:

- Correcting the network or inventory. See "Correcting Discrepancies" for more information.
- Sending the discrepancy to an external system. "Sending Discrepancies to an External System" for more information.

When the discrepancies are submitted, they are sent to the relevant cartridge to be resolved.

To submit discrepancies from the current list of discrepancies discovered:

1. Click **Submit** on the Search Results pane to display a Submit Ready Resolutions dialog. The Submit button is disabled if there are no valid results in the table.
2. Click **Save** to submit the resolution operations, or click **Cancel** to exit the dialog without saving.

   When the discrepancies are submitted, and the dialog is closed, the Review Discrepancies page is refreshed to show the updated status. This may change the list of discrepancies, depending on the search criteria used.

Viewing an Entity Tree

Each discrepancy in the **Search Results** table is represented by an entity tree providing a hierarchical model of the parent entity and its children, as well as the relationships between all of the entity components, and how they are defined by attributes and characteristics. Each discrepancy displays an entity defined by the Communications Information Model (CIM), which describes the information and data concepts, structures and patterns for the Oracle Communications Suite.

For each entity, the entity tree displays:

- The entity name
- The entity type
- The discrepancy count for the parent entity
- The discrepancy count for each child entity

- Whether this entity exists in:
  - The Discovery source only
  - The Import source only
  - Both the Discovery and Import sources

To view an entity tree for a selected discrepancy:

1. Click a discrepancy in the Search Results table to display an entity tree.
2. Expand the tree to view the component parts of the entity. For example, the parent entity could be a physical device, such as a router. The children of this device are shelves, each containing slots filled by cards, with each card populated by ports or other sub-entities such as an Ethernet IP interface.

Selecting Discrepancies in the Entity Tree

When a single discrepancy in the **Search Results** table is selected, the entity tree is refreshed, and displays the result group containing the entity of the discrepancy (the target entity). The tree automatically expands each parent object to show the target entity. The tree scrolls so that the target entity is immediately visible, and the row of the tree containing the target entity is highlighted in a different color, blue.

Selecting an Entity in the Entity Tree

When a single entity in the entity tree is selected, the selection is marked with the color green, and the text of the Entity Name and Entity Type of the selected scan result detail in the Search Results table uses a bold font. This is to aid in identifying the scan result that produced the selected discrepancies.

Expanding the Entity Tree

To expand the entity tree:

1. Select the required entity in the Search Results table.
2. Carry out one of the following:
   - Expand the entity by clicking the **+** sign.
   - Right click the entity and select one of the following options:
     - **Expand**: to expand the entity, showing all of its children
     - **Expand All Below**: to expand the entity, showing all of its children, and all of the components of each of the children.

Viewing Entity Detail Panes

The following detail panes are found at the bottom of the Review Discrepancies page, providing entity detail views for a selected entity with discrepancies:

- Discovery Entity Detail
- Import Entity Detail

If the selected entity has no discrepancies, a single pane called **Entity Detail** is displayed.

The entity panes display the result of a scan in a formatted read-only list of all attributes and relationships for the selected entity.

If a selected entity exists only in the network, only the Discovery Entity Detail is displayed. If a selected entity exists only in inventory, only the Import Entity Detail is displayed. In both cases, this means that the parent root entity has a Missing Entity or Extra Entity discrepancy raised against it. In this case, either the Network or the Inventory detail pane is visible; the other one is not shown.

The details provided on the entity panes are defined as follows:

- **Name**: the name attribute for the entity. The name is formatted as a link.

  Click this link to display this entity as the first row in the Entity Tree. See "Viewing an Entity Tree" for more information.
- **Type**: the type attribute for the entity.
- **Vendor Name**: the name of vendor of the entity.
- **Model Number**: the model number of the entity.
- **Part Number**: the part number of the entity.
- **Serial Number**: the serial number of the entity.
- **Manufactured Date**: the date on which the entity was manufactured.
- **Discovered Location**: the location which the scan attributed to the entity.
- **Relationships**: provides a list of other entities to which the selected entity has relationships defined in the scan. Each related entity is defined by the name of the entity, followed by its type in parenthesis; for example, lddec6451b (Logical Device).

  If the related entity exists in the same Scan Result Detail as the selected entity, then it is represented as a link. Click this link to display the related entity as the first row in the Entity Tree, without changing the selected item. If the related entity does not exist in the same Scan Result Detail as the selected entity, it is shown in text format, that is, not as a link.

  If the relationship is to a number of entities in the same Scan Result Detail, then the entities are displayed as a list of links, with one link per line, or it is displayed as a table.

  A Relationship label is displayed in red when there is a discrepancy raised against this relationship of this entity (in this scan result), regardless of whether this discrepancy is displayed inside the Search Results table. A warning icon is also displayed beside the label. A relationship discrepancy is one of the following:

  - Missing Entity
  - Extra Entity
  - Missing Association
  - Extra Association
  - Association Ordering Error.

About the Scan Result

The **Scan Result** page provides information about the scan. Each scan is defined by:

- **Scan Action**: the scan action associated with the scan
- **Scan Type**: the scan type based on the selected scan action:
  - Discovery

  - Import
  - Assimilation
- **Name**: the name of the scan
- **Source**: (optional) the data source assigned to the scan
- **Scan Start Time**: the time at which the scan started; for example: 79 minutes ago.
- **Scan Duration**: the time taken for the scan to complete; for example: 1 minute.
- **Discrepancy Detection Start Time**: the time at which discrepancy detection started; for example: 77 minutes ago.
- **Discrepancy Detection Duration**: the time taken for discrepancy detection to complete; for example: 2 seconds.

8
Using Blackout Windows

This section describes how to use blackout windows when configuring scans using Oracle Communications Network Integrity, and also outlines how to assign scans to a blackout window. See:

- Managing Blackout Windows
- Managing the Scans Assigned to Blackout Windows

Managing Blackout Windows

A blackout window is a period of time during which a scan is not run, or is paused if already running. Typically, a blackout window is applied when the network is too busy to fulfill requests for discovery and reconciliation activities. So, for example, if you create a scan configuration - either to run immediately, or on a schedule - you can add a blackout window to specify when network and inventory systems cannot be contacted for discovery and reconciliation.

A single blackout window can be applied to multiple scans and updated independently of the scans.

Refer to the following sections:

- Creating a Blackout Window
- Editing a Blackout Window
- Deleting a Blackout Window

Creating a Blackout Window

To create a blackout window:

1. Click the **Manage Blackout Windows** link on the **Tasks** pane to display the **Manage Blackout Windows** page that lists existing blackout windows, if any.
2. Click the **Create** icon on the **Manage Blackout Windows** page.
3. Enter the following information in the **Create Blackout Windows** dialog:
   - **Description**: The name of the blackout window.
   - **Effective Date**: Click the calendar icon to select the date on which the blackout window is to be applied. The default is today's date.
   - **Start Time**: Choose the time at which the blackout window starts. The start time must specify a time in the future. The time refers to the time on the Network Integrity server, as shown on the dialog. Blackout windows are created, updated, displayed, and executed in server time. The local time zone of the client browser is not used for scheduling blackout windows.
   - **Frequency**: Select the recurrence pattern. The options are:
   - – **Daily**: This is the default. Enter the time of day in 24 hour format.

  - **Weekly**: Select the day on which the blackout window is to apply. You can select multiple days of the week for the blackout window to recur.
  - **Monthly**: Select the day of the month on which the blackout window is to be apply:

    Click **On Day … from beginning of month** to specify the day of the month using a number in the range 1 to 28. For example, select 6 to repeat the blackout window at the specified time on the 6th day of each month.

    Click **On Day … from end of month** to specify a blackout window with respect to the end of the month. Enter a value in the range 1 to 7. For example, select 7 to repeat the blackout window at the specified time on the day that falls seven days before the end of each month.

    Click **On the** to specify the day of the month using an ordinal and the day of the week; for example: the Last Saturday in the month. Supported ordinals are: First, Second, Third, Fourth, Fifth, and Last.
  - **Yearly**: Select the day of the year on which the blackout window is to be applied:

    Click **On Date** to specify the month and the day; for example January 24.

    Click **On the** to specify the day of the year using an ordinal, the day of the week, and the month; for example: the First Monday of September. Supported ordinals are: First, Second, Third, Fourth, Fifth, and Last.
  - **Once Only**: Specify a future time and date on which to apply the blackout window on one occasion only.
- **Duration**: The time period covered by the blackout window:
  - **Days**: Enter the number of days for which the blackout window applies. This field does not apply to the Daily frequency.
  - **Hours**: Enter the number of hours for which the blackout window applies.
  - **Minutes**: Enter the number of minutes for which the blackout window applies.

  The maximum duration for the blackout window depends on the frequency selection. For Daily, it is 24 hours; for Weekly, it is 7 days; for Monthly, it is 31 days; for Yearly and Once only, it is 366 days.

4. Assign a scan (or multiple scans) to the blackout window. See"Assigning Scans to a Blackout Window".
5. Click **Save** to complete the blackout window configuration or click **Cancel** to exit.

Editing a Blackout Window

To edit a blackout window:

1. Click the **Manage Blackout Windows** link on the **Tasks** pane to display the **Manage Blackout Windows** page that lists existing blackout windows, if any.
2. Right-click the required blackout window, and select **Edit** to display the **Edit Blackout Windows** dialog box
3. Modify the fields. See "Creating a Blackout Window" for more information.

Deleting a Blackout Window

To delete a blackout window:

1. Click the **Manage Blackout Windows** link on the **Tasks** pane to display the **Manage Blackout Windows** page that lists existing blackout windows, if any.
2. Carry out one of the following:
   - Select the required blackout window and click the **X** icon on the top-level menu.
   - Right-click the required blackout window and select **Delete**.
3. Click **OK** to confirm the deletion or click **Cancel** to maintain the blackout window.

Managing the Scans Assigned to Blackout Windows

This section deals with assigning scans to blackout windows. A blackout window can be applied to multiple scans and updated independently of the scans.

Refer to the following sections:

- Assigning Scans to a Blackout Window
- Removing an Assigned Scan from a Blackout Window
- Viewing the Scans Assigned to a Blackout Window

Assigning Scans to a Blackout Window

To assign a scan to a blackout window:

1. Navigate to the Scans section of the Create/Edit Blackout Windows page that displays all scans defined by name, scan action, type, source, and description.
2. Click the **+** icon on the top-level menu to display the Assign Scans dialog.
3. Select the scans to assign. You can assign multiple scans to a blackout window.

   If there are no scans configured, you may need to create one. See "Creating a Scan" for more information.
4. Click **OK** to confirm the selection. The scan is added to a table of scans in the Scans section of the **Create/Edit Blackout Windows** page.

To remove a scan assigned to a blackout window, see "Removing an Assigned Scan from a Blackout Window".

Removing an Assigned Scan from a Blackout Window

To remove a scan assigned to a blackout window:

1. Navigate to the Scans section of the **Create/Edit Blackout Windows** page that displays all scans defined by name, scan action, type, source, and description.
2. Carry out one of the following:
   - Select the required scan or scans and click the **X** icon on the top-level menu.
   - Right-click the required scan or scans and select **Remove**.
3. Confirm the removal of the scan from the blackout window.

Viewing the Scans Assigned to a Blackout Window

To view the scans assigned to a blackout window:

1. Click the blackout window in the **Manage Blackout Windows** table.
2. View the scan or scans assigned to the blackout window in the **Scans Assigned to Selected Blackout Window** table.

   Each scan is defined by name, associated scan action, scan type, source, and description.

   You cannot carry out any actions on the scans in this table.

9 Using Import Systems with Network Integrity

This section describes how to using import systems for use with Oracle Communications Network Integrity.

Managing Import Systems

The Manage Import System page is used to display the connection settings for the supported system. These settings are used by all inventory import and inventory resolution scan actions to communicate with the target import system.Network Integrity supports a single import system at any one time.

You can edit the connection settings to change the supported import system. The settings information consists of a display name, an address, a user name, and a password. The display name is required as it is used to identify the import system.

The address, user name, and password specify the connection parameters of the import system, but are not required fields in the Network Integrity UI, because data requirements may vary depending on the scan action used. It is the responsibility of the developer implementing the scan action to determine if this data is needed.

Refer to the following sections:

- Creating the Import System
- Editing the Import System

Creating the Import System

To create the connection details for the import system:

1. Click the **Manage Import System** link on the **Tasks** pane to display the **Import System** page.
2. Click the **Create** icon to display the Create Import System Detail dialog.

   > **Note:**
   >
   > If an import system has already been configured, the Create icon is disabled. To edit the connection details of an existing import system, see "Editing the Import System".

3. Enter the following information:
   - **Name**: The name of the import system. It must have a unique value.
   - **Address**: An identifier used to locate the import system (a URL, for example).
   - **User Name**: The user name associated with the import system. This is used for login purposes.

- **Password**: The password associated with the import system. This is used for login purposes. Password data is stored securely.

4. Click **Save** to complete the configuration or click **Cancel** to exit.

Editing the Import System

To edit the connection details for the import system:

1. Click the **Manage Import System** link on the **Tasks** pane to display the **Import System** page.
2. Click the **Edit** icon (the pencil) to display the **Edit Import System Detail** dialog.
3. Enter the following information:
   - **Name**: The name of the import system. It must have a unique value
   - **Address**: An identifier used to locate the import system (a URL, for example).
   - **User Name**: The user name associated with the import system. This is used for login purposes.
   - **Password**: The password associated with the import system. This is used for login purposes. Password data is stored securely.
4. Click **Save** to complete the configuration or click **Cancel** to exit.