Oracle® Communications Service Catalog and Design

Design Studio Modeling Network Integrity

Release 8.1
F96244-01
July 2024

ORACLE

Oracle Communications Service Catalog and Design Design Studio Modeling Network Integrity, Release 8.1

F96244-01

Contents

4 Working with Network Integrity Processors

Preface

The Modeling Network Integrity Help is loaded into Oracle Communications Service Catalog and Design - Design Studio when the Design Studio for Network Integrity feature is installed into Design Studio. In Design Studio, clicking **Help** displays relevant Help topics.

Audience

This guide is intended for business analysts, architects, development managers, developers, and designers who are responsible for system integration or solution development involving the Oracle Communications operational support systems applications.

Ideally, you should be knowledgeable about your company's business processes, the resources you need to model, and any products or services your company offers.

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

Getting Started with Design Studio for Network Integrity

You use the Oracle Communications Service Catalog and Design - Design Studio for Network Integrity features to develop and deploy cartridges that customize Oracle Communications Network Integrity for various environments and applications.

Although Design Studio automatically generates many cartridge artifacts, you will need to write or complete some Java code to complete your cartridges.

You use Design Studio to interactively deploy and undeploy Network Integrity cartridge projects to test environments. You can use the Design Studio Cartridge Management Tool (CMT) to automate the deployment of cartridge projects into Network Integrity environments. See the *Design Studio Developer's Guide* for more information about the CMT. You can also use the Network Integrity Cartridge Deployer Tool (CDT) to deploy to Network Integrity run-time environments. See the *Network Integrity Installation Guide* for information about deploying Network Integrity cartridges using the CDT.

When getting started with Design Studio for Network Integrity, see the following topics:

- Configuring Network Integrity Preferences
- Importing Prerequisite Network Integrity Projects

Configuring Network Integrity Preferences

You configure Network Integrity preferences in Design Studio by specifying a default cartridge package name for all created cartridge projects and specifying the default directory for management information base (MIB) objects.

The cartridge package name is applied as a prefix to the cartridge name in all generated Java classes in the various cartridge artifacts for the cartridge.

To configure Network Integrity preferences:

1. From the **Window** menu, select **Preferences**.

   The Preferences dialog box appears.

2. Expand **Oracle Design Studio**, then select **Network Integrity**.

   The configuration preferences for Network Integrity appear.

3. In the **Default Cartridge Package** field, enter the default cartridge package name.

   The default cartridge package name can be any valid Java string. Specify a name to suit your business needs. For example, the default cartridge package name can include your company name: **com.***company***.integrity**.

   The default cartridge package name is applied to new Network Integrity cartridge projects created in Design Studio.

   Changing this default package does not affect existing cartridges.

4. In the **MIB Directory** field, enter the directory that contains all of the MIB files that Design Studio uses to create SNMP processors.

If the MIB directory is not properly set, you cannot create SNMP processors.

5. Click **OK**.

   Design Studio restarts.

Importing Prerequisite Network Integrity Projects

All Network Integrity cartridge projects have dependencies on the following model projects:

- ora_uim_model
- ora_uim_mds
- ora_ni_uim_ocim
- NetworkIntegritySDK: this project contains common software components and libraries required for creating and extending Network Integrity cartridges.

Before creating or importing Network Integrity cartridge projects, import the prerequisite model projects into Design Studio.

> **Note:**
>
> Network Integrity cartridge projects must be defined with the same target version as the required model projects in a workspace. Ensure that you import the correct version of the required model projects into a workspace. See "Defining Cartridge Project Target Versions" for more information.
>
> See the *UIM Cartridge Guide* for more information about the ora_uim_model project and the ora_uim_mds project.

To import prerequisite Network Integrity model projects:

1. Go to the Oracle software delivery website:

   `https://edelivery.oracle.com`

2. Open the Network Integrity Software media pack.
3. Download a cartridge media pack.

   All cartridge media packs contain the prerequisite projects.

4. Import the prerequisite projects into Design Studio.

   See "Importing Projects" for more information.

2

Working with Network Integrity Cartridges

You use Design Studio for Network Integrity to develop and deploy cartridges that customize Oracle Communications Network Integrity for various environments and applications.

When working with Network Integrity cartridges, see the following topics:

- Working with Environment Projects for Network Integrity
- Working with Design Studio Cartridge Projects
- Network Integrity Project Editor

See *Network Integrity Concepts Guide* for a description of cartridge concepts, and see *Network Integrity Developer's Guide* for a description of cartridge extensibility scenarios.

Working with Environment Projects for Network Integrity

To deploy or undeploy a cartridge to Network Integrity using Design Studio, first create an Environment project. See "Working with Environment Projects" for more information.

Related Topics

Creating a Design Studio Environment for Network Integrity

Creating a Design Studio Environment for Network Integrity

An environment represents a connection to a particular server.

To create a Design Studio environment for Network Integrity:

1. Create an Environment project.

   See "Working with Environment Projects" for more information.
2. Click the Project editor **Connection Information** tab for the environment project.
3. In the **Address** field, enter the Cartridge Management web service (CMWS) URL.

   You may need to consult the Network Integrity administrator for this information. The URL must begin with **https** if SSL is used.
4. (Optional) In the **Cluster/Server** field, enter the name of the cluster or server on which the Network Integrity application is installed.

   Design Studio uses the default server if the field is left blank.
5. If SSL is used, do the following:
   a. Click the Project editor **SSL** tab.
   b. In the **Keystore** field, browse to the location of the keystore file on the local hard drive.

      Consult the Oracle WebLogic Server administrator for this information.

> **Note:**
>
> The keystore file must be transferred from the WebLogic server to the location where Design Studio is running. If you select the WebLogic server demonstration keystore, you must add the host name instead of the IP address in the **Address** field on the **Connection Information** tab.
>
> The WebLogic server demonstration keystore is generated against the host name, not the IP address, during Network Integrity installation.

6. Click the Project editor **Cartridge Management Variables** tab and set the **Override** field for the following cartridge management variables:
   - Set the **wladmin.host.name** variable to the host name or IP address where the WebLogic Administration Server is running.
   - Set the **wladmin.host.port** variable to the port number on which the WebLogic Administration Server is running.
   - Set the **wladmin.server.name** variable to the WebLogic Administration Server name.

   Consult the WebLogic Server administrator for this information.
7. Save the project.

Network Integrity Project Editor

This section details the contents of the Network Integrity Project editor.

The Network Integrity Project editor consists of the following tabs:

- Project Editor Properties Tab
- Project Editor Copyright Tab
- Project Editor Dependency Tab
- Project Editor Tag Tab
- Network Integrity Project Editor Model Variables Tab
- Project Editor Cartridge Management Variables Tab

Network Integrity Project Editor Model Variables Tab

Use the **Model Variables** tab to define property name/value pairs or to set a property with a model variable. See "Project Editor Model Variables Tab" for more information.

You can map model variables to processor properties. See "About Properties and Property Groups" for more information.

Related Topics

Working with Model Variables

3

Working with Network Integrity Actions

In Design Studio, you create actions to perform scans in Oracle Communications Network Integrity.

When working with actions for Network Integrity, see the following topics:

- About Network Integrity Actions
- Creating Network Integrity Actions
- Configuring Network Integrity Actions
- Network Integrity Action Editor
- Address Handler Editor
- Model Collection Editor

About Network Integrity Actions

Actions accomplish a particular function in Network Integrity at run time. Actions contain one or more processors.

Processors perform the sub-tasks of an action. See "Working with Network Integrity Processors" for more information.

By grouping processors in an action, the action can achieve a complex function such as discovering a network, importing an inventory system, assimilating discovered data, or detecting and resolving discrepancies.

At run time, actions are implemented as J2EE message driven beans (MDBs).

You can create the following types of actions:

- **Discovery action**: Discover data (typically from a network) and save it in the Results Model. See "About Discovery Actions for Network Integrity" for more information.
- **Import action**: Import data (typically from an inventory system) and save it in the Results Model. See "About Import Actions for Network Integrity" for more information.
- **Assimilation action**: Process data (typically discovered data) and save it in the Results Model. See "About Assimilation Actions for Network Integrity" for more information.
- **Discrepancy detection action**: Find discrepancies between discovered and imported data. See "About Discrepancy Detection Actions for Network Integrity" for more information.
- **Discrepancy resolution action**: Solve discrepancies in an external system or a network. See "About Discrepancy Resolution Actions for Network Integrity" for more information.

When creating actions, you can configure them as abstract actions. See "About Abstract Actions for Network Integrity" for more information.

Related Topics

Configuring Network Integrity Actions

About Abstract Actions for Network Integrity

Abstract actions are models of actions to be extended by other actions. Abstract actions cannot be deployed.

Abstract actions do not generate many build errors and do not need extensive configuration.

Related Topics

About Network Integrity Actions

Creating Network Integrity Actions

About Discovery Actions for Network Integrity

Discovery actions discover data, typically from the network, and to save the discovered data in the Results Model. Discovery actions can access networks using various technologies and protocols.

Network Integrity users trigger discovery actions by running a discovery scan.

Discovery actions are made up of discovery and SNMP processors. See "Working with Network Integrity Processors" for more information.

Discovered data is saved in the Oracle Communications Information Model. Discovered data is flagged as having come from a network system. The Network Integrity UI displays and reports on discovered data.

Discovery actions can be configured with address handlers. If the discovery action is configured with an address handler, Network Integrity can validate the addresses configured in the scope of a discovery scan at run time. Invalid addresses are identified before running a scan that would otherwise end in failure. See "About Address Handlers for Network Integrity" for more information.

A discovery action must be configured with a valid result category. See "About Result Categories for Network Integrity" for more information.

Related Topics

About Network Integrity Actions

About Network Integrity Processors

Creating Network Integrity Actions

About Import Actions for Network Integrity

Import actions import data, typically from an inventory system, into Network Integrity. The data is stored in the Information Model and is flagged as having come from an inventory system. The Network Integrity UI displays and reports on the imported data.

Network Integrity users trigger import actions by running an import scan.

An import action must be configured with a valid result category. See "About Result Categories for Network Integrity" for more information.

Related Topics

About Network Integrity Actions

About Network Integrity Processors

Creating Network Integrity Actions

About Assimilation Actions for Network Integrity

Assimilation actions perform additional processing on existing Network Integrity data, typically from the network, to derive or construct additional information, and to save the assimilated data in the Results Model. An assimilation action can use the results from a discovery or import scan or from another assimilation scan as input for additional processing.

Network Integrity users trigger assimilation actions by running an assimilation scan.

For example, an assimilation action might be used to derive connectivity relationships between endpoints discovered by previous scans.

Assimilated data is saved in the Information Model. Assimilated data is flagged as having come from a network system. The Network Integrity UI displays and reports on the assimilated data.

An assimilation action must be configured with a valid result category. See "About Result Categories for Network Integrity" for more information.

Related Topics

About Network Integrity Actions

About Network Integrity Processors

Creating Network Integrity Actions

About Discrepancy Detection Actions for Network Integrity

Discrepancy detection actions compare network data with inventory data and report differences.

Network Integrity users trigger discrepancy detection actions by running a discovery, import, or assimilation scan with the **Detect Discrepancy** option enabled.

You can also create a discrepancy detection action that automatically resolves some types of discrepancies. See the *Network Integrity Developer's Guide* for more information.

Discrepancy detection actions must be configured with a valid result source. See "About Result Categories for Network Integrity" for more information.

Related Topics

About Network Integrity Actions

About Network Integrity Processors

Creating Network Integrity Actions

About Discrepancy Resolution Actions for Network Integrity

Discrepancy resolution actions act on an external system to resolve a discrepancy. Discrepancy resolution actions can update a mismatch in an inventory system using information gathered from the network or can generate a trouble ticket to begin a network configuration change process.

Network Integrity users trigger discrepancy resolution actions by selecting detected discrepancies and selecting a resolution command.

Related Topics

About Network Integrity Actions

About Network Integrity Processors

Creating Network Integrity Actions

Creating Network Integrity Actions

To create a Network Integrity action:

1. From the **Studio** menu, select **New**, then select **Integrity**, then select **Action**, and then select the action type.

   The Action Wizard for the type of action you selected appears.
2. From the **Project** list, select a project in which to include the new action.

   The currently selected project appears by default.
3. In the **Name** field, enter a name for the new action.

   This name appears in the Network Integrity UI when the cartridge is deployed. Oracle recommends that the action name describe the behavior of the action. For example, start action names with a verb, such as: *Discover MIB II SNMP* or *Import MIB II from UIM*.
4. (Optional) In the **Folder** field, specify a location for the action.

   By default, Design Studio saves the entity to your default workspace. You can browse to a different location using the **Browse** button.
5. (Optional) To configure the action as an abstract action, select the **Abstract** check box.

   Design Studio creates the action as an abstract class. An abstract action cannot be deployed to Network Integrity. It is extended by other actions. See "About Abstract Actions for Network Integrity" for more information.
6. Click **Finish**.

   Design Studio creates the new action and displays the Action editor.
7. Configure the action. See "Configuring Network Integrity Actions" for more information.

Configuring Network Integrity Actions

To configure a Network Integrity action:

1. Open the Action editor **Details** tab.
2. (Optional) In the **Description** field, enter a description.

3. For discrepancy resolution actions, enter a name in the **Resolution Action Label** field.

   The resolution action label name is the label that appears in the Network Integrity **Actions** menu.

   For example, if you enter **Correct in Inv** in the **Resolution Action Label** field, the Network Integrity **Actions** menu will have a **Correct in Inv** option after the cartridge containing this action is deployed.

4. (Optional) To configure the action as an abstract action, select the **Abstract** check box.

   Design Studio creates the action as an abstract class. An abstract action cannot be deployed to Network Integrity. It is extended by other actions. See "About Abstract Actions for Network Integrity" for more information.

   If the action is abstract, the rest of this procedure is optional.

5. (Optional) For discovery actions, add an address handler.

   See "Adding Address Handlers to Network Integrity Actions" for more information.

6. For assimilation, discovery, and import actions, add a result category.

   See "Adding Result Categories to Network Integrity Actions" for more information.

7. (Optional) In the **Documentation** field, add information about the action.

8. Add processors to the action. Do at least one of the following:

   - Add an existing processor to an action. See "Adding Existing Processors to Network Integrity Actions".
   - Create a new processor and add it to an action. See "Adding New Processors to Network Integrity Actions".

9. (Optional) To create a For Each processor and add it to an action, see "Adding For Each Processors to Network Integrity Actions".

10. (Optional) To organize the sequence of processors for the action, select a processor and click **Move Up** or **Move Down**.

    > **Tip:**
    >
    > Configuring the sequence of processors is important. The processors in an action are run in the order they appear in the Action Processors area of the Action editor **Processors** tab.

11. (Optional) For assimilation, discovery, and import actions, add scan parameter groups to the action.

    See "Adding Scan Parameter Groups to Network Integrity Actions" for more information.

12. Add model collections to the action.

    See "Adding Model Collections to Network Integrity Actions" for more information.

13. For discrepancy detection and discrepancy resolution actions, add a result source.

    See "Adding Result Sources to Network Integrity Actions" for more information.

14. (Optional) Create conditions and apply them to processors:

    a. Create conditions.

       See "Creating Conditions for Network Integrity" for more information.

    b. Apply the conditions to processors.

See "Applying Conditions to Network Integrity Processors" for more information.

15. Save the action.

Related Topics

About Network Integrity Actions

Creating Network Integrity Actions

Network Integrity Action Editor

About Address Handlers for Network Integrity

Discovery actions use address handlers to validate the scope of discovery scans run from Network Integrity. Oracle Communications provides basic address handlers in the Address Handler cartridge provided with Network Integrity.

Address handlers cannot exist in the same cartridge project as actions. See *Network Integrity Developer's Guide* for information about building custom address handlers.

If you do not add an address handler, Network Integrity cannot validate scope addresses at run time. Addresses are treated individually and invalid addresses fail.

Related Topics

About Discovery Actions for Network Integrity

Creating Network Integrity Address Handlers

Adding Address Handlers to Network Integrity Actions

Configuring Network Integrity Actions

Address Handler Editor

Creating Network Integrity Address Handlers

To create an address handler:

1. From the **Studio** menu, select **New**, then select **Integrity**, then select **Address Handler**.

   The Address Handler Wizard appears.
2. From the **Project** list, select the cartridge project to include the address handler.

   Address handlers cannot exist in the same cartridge project as actions.
3. In the Name field, enter a name for the address handler.
4. (Optional) In the **Folder** field, select a location for the address handler.

   If you leave the **Folder** field blank, the address handler is created in the default workspace.
5. Click **Finish**.

   Design Studio creates the address handler and displays the Address Handler editor.

Because address handlers and actions cannot exist in the same cartridge project, you must make the project with actions dependent on the one containing address handlers. See "Managing Project Dependencies" for more information.

See *Network Integrity Developer's Guide* for more information about building and configuring address handlers.

Related Topics

About Discovery Actions for Network Integrity

Adding Address Handlers to Network Integrity Actions

Configuring Network Integrity Actions

Address Handler Editor

Adding Address Handlers to Network Integrity Actions

This procedure assumes you have a cartridge project with address handlers. Oracle Communications provides basic address handlers in the Address Handler cartridge provided with Network Integrity.

To add an address handler to a discovery action:

1. On the Action editor **Details** tab, beside the **Address Handler** field, click **Select**.

   The Select Address Handler dialog box appears. The dialog box lists address handlers from dependent cartridge projects only. See "Managing Project Dependencies" for more information.

2. From the **Matching Items** list, select an address handler.

   You can filter the **Matching Items** list by typing in the **Select an item to open** field.

3. Click **OK**.

   The name of the address handler appears in the **Address Handler** field.

4. Save the action.

Related Topics

About Address Handlers for Network Integrity

Configuring Network Integrity Actions

Address Handler Editor

Network Integrity Action Editor

About Result Categories for Network Integrity

A result category is the identifier for a result group. It is used to identify and save scan results to the corresponding result model.

The name of the result category must match the name of the result group in the Java implementation into which the scan results are saved. The result category name appears in the Network Integrity UI scan results.

Assimilation, discovery, and import actions must be configured with a valid result category.

Related Topics

Adding Result Categories to Network Integrity Actions

Configuring Network Integrity Actions

About Assimilation Actions for Network Integrity

About Discovery Actions for Network Integrity

About Import Actions for Network Integrity

Network Integrity Action Editor

Adding Result Categories to Network Integrity Actions

Assimilation, discovery, and import actions must have a valid result category.

To add a result category to an action:

1. On the Action editor **Details** tab, in Result Categories area, click **Add**.

   The Create Results Categories dialog box appears.
2. In the **Name** field, enter a name for the result category.

> **Note:**
>
> The name of the result category must match the name of the result group in the Java implementation into which the scan results are saved. The result category name also appears in the Network Integrity UI scan results.

3. (Optional) In the **Description** field, add information about the result category.
4. Click **OK**.
5. Save the action.

Related Topics

About Address Handlers for Network Integrity

Configuring Network Integrity Actions

About Assimilation Actions for Network Integrity

About Discovery Actions for Network Integrity

About Import Actions for Network Integrity

Address Handler Editor

Network Integrity Action Editor

Adding New Processors to Network Integrity Actions

You can create a new processor from the Action editor to add to your action.

To create a new processor and add it to an action:

1. On the Action editor **Processors** tab, click **Add**.

   The Studio Model Entity Wizard appears.
2. From the **Project** list, select the cartridge project that contains the action in which you are creating the processor.
3. From the **Type** list, select the type of processor you want to create.

The **Type** list contains different processor types depending on the action you are configuring.

4. In the **Name** field, enter a name for the processor.

   The **Implementation Prefix** field takes the component name by default.

5. (Optional) In the **Folder** field, select a location for the processor.

   If you leave the **Folder** field blank, the processor is created in the default workspace.

6. Click **Finish**.

   Design Studio creates the processor and adds it to the Action Processors area.

7. Save the action.

8. Configure the processor.

   See "Configuring Network Integrity Processors" for more information.

Related Topics

Working with Network Integrity Processors

Creating Network Integrity Processors

Configuring Network Integrity Actions

Network Integrity Action Editor

Adding Existing Processors to Network Integrity Actions

This procedure assumes that you have already created and configured a processor for your action.

To add an existing processor to an action:

1. On the Action editor **Processors** tab, click **Select**.

   The Select an Action or Processor to Add dialog box appears. The dialog box lists processors from the current cartridge project and actions from dependent cartridge projects. See "Managing Project Dependencies" for more information.

2. From the **Matching Items** list, select a processor or action.

   You can filter the **Matching Items** list by typing in the **Select an item to open** field. Only valid entities for the action type appear in the **Matching Items** list.

3. Click **OK**.

   Design Studio adds the processor to the action.

4. Save the action.

Related Topics

Working with Network Integrity Processors

Creating Network Integrity Processors

Configuring Network Integrity Processors

Configuring Network Integrity Actions

Network Integrity Action Editor

About For Each Processors for Network Integrity

A For Each processor causes the processors it contains to run multiple times.

For example, when importing data, a For Each processor is typically used to read through a list of discovered devices, saving each device to the Network Integrity database.

Related Topics

Adding For Each Processors to Network Integrity Actions

Configuring Network Integrity Actions

Adding For Each Processors to Network Integrity Actions

To add a For Each processor to an action:

1. On the Action editor **Processors** tab, click **Add For Each**.

   The Create For Each dialog box appears.
2. From the **Collection Name** list, select the output parameter to which to associate the For Each processor.
3. Click **OK**.

   Design Studio adds the For Each processor to the Action Processors area.
4. Save the action.

Related Topics

About For Each Processors for Network Integrity

Configuring Network Integrity Actions

Network Integrity Action Editor

Adding Scan Parameter Groups to Network Integrity Actions

Scan parameter groups allow you customize the Network Integrity UI by adding input fields for configuring assimilation, discovery, and import scans.

This procedure assumes that you have already created scan parameter groups.

To add a scan parameter group to an action:

1. On the Action editor **Scan Parameter Group** tab, click **Select**.

   The Add Entities dialog box appears. The dialog box lists scan parameter groups from the current cartridge project and from dependent cartridge projects. See "Managing Project Dependencies" for more information.
2. From the **Matching Items** list, select a scan parameter group.

   You can filter the **Matching Items** list by typing in the **Select an item to open** field.
3. Click **OK**.

   Design Studio adds the scan parameter group to the action.
4. To organize the order of the scan parameter groups, select a scan parameter group and click **Move Up** or **Move Down**.

5. Save the action.

Related Topics

About Network Integrity Scan Parameter Groups

Working with Network Integrity Scan Parameter Groups

Configuring Network Integrity Actions

Network Integrity Action Editor

About Model Collections for Network Integrity Actions

A model collection is a grouping of specifications from other cartridge projects.

Specifications created in a cartridge project are automatically related to all actions in the same cartridge project. You cannot add specifications to a model collection in the same cartridge project.

By default, when you create a Network Integrity cartridge project, Design Studio automatically creates a model collection for the cartridge project.

By default, when you create an action, all model collections in the same cartridge project are automatically added to the action. You should add only new model collections to an action.

Model collections allow Design Studio to generate specification helper classes for specifications from other cartridges to model data into the Oracle Communications Information Model.

Related Topics

Creating Network Integrity Model Collections

Adding Specifications to Network Integrity Model Collections

Adding Model Collections to Network Integrity Actions

Creating Network Integrity Model Collections

A model collection groups specifications from other dependent cartridge projects.

All Network Integrity cartridge projects have a default model collection. You can create additional model collections.

To create a model collection:

1. From the **Studio** menu, select **New**, then select **Integrity**, and then select **Model Collection**.

   The Model Collection Wizard appears.

2. From the **Project** list, select the name of the project in which to include the model collection.
3. In the **Name** field, enter a name for the model collection.
4. (Optional) In the **Folder** field, select a location for the new model collection.

   If you leave the **Folder** field blank, the model collection is created in the default workspace.

5. Click **Finish**.

Design Studio creates the model collection and displays its information in the Model Collection editor.

6. Add specifications to the model collection.

   See "Adding Specifications to Network Integrity Model Collections" for more information.

7. Add the model collection to an action.

   See "Adding Model Collections to Network Integrity Actions" for more information.

Related Topics

About Model Collections for Network Integrity Actions

Configuring Network Integrity Actions

Model Collection Editor

Adding Specifications to Network Integrity Model Collections

A model collection groups specifications from other dependent cartridge projects.

This procedure assumes that your current cartridge project has a model collection.

To add a specification to a model collection:

1. On the Model Collection editor **Model** tab, click **Select**.

   The Open Resource dialog box appears. The dialog box lists specifications from dependent cartridge projects that are supported by Network Integrity. See "Managing Project Dependencies" for more information.

2. From the **Matching Items** list, select the specifications.

   You can filter the **Matching Items** list by typing in the **Select an item to open** field. Only specifications from dependent cartridge projects appear in the **Matching Items** list.

3. Click **OK**.

   Design Studio adds the specifications to the model collection.

4. Save the model collection.

Related Topics

About Model Collections for Network Integrity Actions

Creating Network Integrity Model Collections

Adding Model Collections to Network Integrity Actions

Configuring Network Integrity Actions

Model Collection Editor

Adding Model Collections to Network Integrity Actions

Adding a model collection to an action allows the action to use the specifications contained in the model collection from other cartridge projects.

By default, when you create an action, all model collections in the same cartridge project are automatically added to the action. You should add only new model collections to an action.

To add a model collection to an action:

1. On the Action editor **Model** tab, click **Add**.

   The Select the Model Collection to Add dialog box appears.
2. From the **Matching Items** list, select the model collection.

   You can filter the **Matching Items** list by typing in the **Select an item to open** field.
3. Click **OK**.

   Design Studio adds the model collection to the action.
4. Save the action.

Related Topics

About Model Collections for Network Integrity Actions

Creating Network Integrity Model Collections

Adding Specifications to Network Integrity Model Collections

Configuring Network Integrity Actions

Network Integrity Action Editor

Adding Result Sources to Network Integrity Actions

Design Studio uses result sources to link results produced by assimilation, discovery, or import actions to discrepancy detection and discrepancy resolution actions.

Discrepancy detection and discrepancy resolution actions must have result sources.

To add a result source to an action:

1. On the Action editor **Result Source** tab, click **Add**.

   The Select Result Source dialog box appears.
2. Click **Select**.

   The Select Action dialog box appears, showing all assimilation, discovery, and import actions available as result sources.
3. Select an action from the list and click **OK**.

   The **Result Category** list shows all result categories generated by the action.
4. Select the check box beside each required category.

   Leave the check boxes empty to select all result categories.
5. Click **OK**.
6. Save the action.

Related Topics

Configuring Network Integrity Actions

Network Integrity Action Editor

About Conditions for Network Integrity

You can create conditions on an action and apply them to its processors to control if a processor is run during a run-time scan.

When you create a condition, Design Studio generates the Java class that implements the condition interface. You must complete the condition interface implementation.

The same condition can be set to different values on different processors. You can apply one or more conditions to a processor.

A processor is run only when all of its conditions are satisfied.

Related Topics

Creating Conditions for Network Integrity

Applying Conditions to Network Integrity Processors

Creating Conditions for Network Integrity

To create conditions:

1. On the Action editor **Conditions** tab, click **Add**.

   The Create Condition dialog box appears.
2. In the **Name** field, enter a name for the condition.
3. (Optional) In the **Description** field, enter a description for the condition.
4. Click **OK**.
5. Implement the condition:
   a. In the **Implementation Class** field, select or create an implementation class.

      The condition is implemented in Java.
   b. (Optional) In the **Input Parameters** field, add the output parameters from preceding processors from which the condition needs information.

      This condition can be applied only to processors that have access to this input parameter.
   c. Click **OK**.
6. Save the action.

Related Topics

About Conditions for Network Integrity

Configuring Network Integrity Actions

Network Integrity Action Editor

Applying Conditions to Network Integrity Processors

You apply conditions to processors so that conditions control the flow of the processors inside the action.

To apply conditions to a processor:

1. On the Action editor **Processors** tab, in the Action Processors area, select a processor.

   The Conditions area displays the name of the selected processor.
2. In the Conditions area, click **Select**.

   The Condition Selection dialog box appears.

3. From the **Matching Items** list, select the condition.

   You can filter the **Matching Items** list by typing in the **Select an item to open** field.

4. Click **OK**.
5. In the Conditions area, do one of the following:
   - To allow the processor to run when the condition returns true, set the **Equals** list to **True**.
   - To allow the processor to run when the condition returns false, set the **Equals** list to **False**.
6. Save the action.

Related Topics

About Conditions for Network Integrity

Configuring Network Integrity Actions

Network Integrity Action Editor

Network Integrity Action Editor

Use the Action editor to configure an action. To access the Action editor, double-click an action entity. The tabs in the Action editor depend on the type of action.

When using the Action editor to configure an action, see the following topics:

- Action Editor Details Tab
- Action Editor Processors Tab
- Action Editor Scan Parameter Groups Tab
- Action Editor Model Tab
- Action Editor Result Source Tab
- Action Editor Conditions Tab
- Action Editor Realization Tab

Action Editor Details Tab

Use the **Details** tab to specify general details about the action.

Field	Use
Description	Enter a short description of the action.
Implementation Prefix	Displays the implementation prefix. Design Studio creates the implementation prefix from the entity name and removing any invalid Java characters.
Abstract	Select to specify whether the action is abstract. See "About Abstract Actions for Network Integrity" for more information. If the action is abstract, then it can only be used as a component within another action. If the action is not abstract, then it can be deployed and a scan can be performed from it.
Address Handler	Specify the address handler for the action. Use the **Select** button to choose an address handler from a list of dependent cartridge projects. This field appears for assimilation, discovery, and import actions only.

Field	Use
Result Categories	Add result categories to the action. This field appears for assimilation, discovery, and import actions only.
Documentation	Add any other information about the action.

Related Topics

About Network Integrity Actions

Creating Network Integrity Actions

Configuring Network Integrity Actions

Network Integrity Action Editor

Action Editor Processors Tab

Use the **Processors** tab to view and manage the processors on an action.

Action Processors Area

Field	Use
Action Processors table	Lists all processors on the action by name and provider and indicates whether the processor has any conditions set.The Owner Action column identifies processors added from other actions.
Move Down **Move Up**	Select a processor and click to change the order of the processors in the **Action Processors** table.
Select	Add existing processors and actions from dependent cartridge projects to the action.
Open	Open the Processor editor for the selected processor.
Remove	Remove the selected processor from the action.
Add For Each	Add a For Each processor to the action.
Add	Create a new processor to add to the action.

Conditions Area

Field	Use
Conditions table	Displays the condition applied on the selected processor from the Action Processors table. Set to **true** to run the processor when the condition is true. Set to **false** to run the processor when the condition is false.
Remove	Remove the selected condition.
Select	Add an existing condition to the selected processor.

Related Topics

About Network Integrity Actions

Configuring Network Integrity Actions

Working with Network Integrity Processors

Adding Existing Processors to Network Integrity Actions

Adding New Processors to Network Integrity Actions

Adding For Each Processors to Network Integrity Actions

Applying Conditions to Network Integrity Processors

Network Integrity Action Editor

Action Editor Scan Parameter Groups Tab

Use the **Scan Parameter Groups** tab to view and manage the scan parameter groups for assimilation, discovery, and import actions.

Field	Use
Scan Parameter Groups Section table	Lists the scan parameter groups on the action, and to which cartridge project they belong.
Move Up **Move Down**	Reorder the selected scan parameter group for the action.
Select	Add an existing scan parameter group to the action, or a scan parameter group from a dependent cartridge project.
Open	Open the Scan Parameter Group editor for the selected scan parameter group.
Remove	Remove the selected scan parameter group from the action.
Add	Create a new scan parameter group and adds it to the action.

Related Topics

About Network Integrity Actions

Configuring Network Integrity Actions

Working with Network Integrity Scan Parameter Groups

Network Integrity Action Editor

Action Editor Model Tab

Use the **Model** tab to view and manage the model collections on an action.

Field	Use
Model Section table	Lists the model collections on the action.
Open	Opens the Model Collection editor for the selected model collection.
Remove	Removes the selected model collection from the action.
Select	Adds an existing model collection to the action, or creates a new model collection to add to the action.

Related Topics

About Network Integrity Actions

Configuring Network Integrity Actions

Network Integrity Action Editor

Action Editor Result Source Tab

Use the **Result Source** tab to view and manage the result sources on discrepancy detection and discrepancy resolution actions.

Field	Use
Result Source table	Adds a result source to the action. Result sources come from the result category on discovery, import, or assimilation actions. If the result category of the source action that this action acts against is set to **All**, this action acts against all the results that are generated by the source action.
Open	Edits the selected result categories for the selected result source.
Remove	Removes the selected result source from the action.
Add	Add a result source (and result category) on the action.

Related Topics

About Network Integrity Actions

Configuring Network Integrity Actions

Adding Result Sources to Network Integrity Actions

Network Integrity Action Editor

Action Editor Conditions Tab

Use the **Conditions** tab to view and manage the conditions on an action.

Conditions Area

Field	Use
Conditions table	Lists the condition on the action.
Remove	Removes the selected condition from the action.
Add	Creates a condition.

Condition Details Area

Field	Use
Condition Details table	Provides further details on the selection condition from the **Conditions** table.
Implementation Class	Specifies or creates a new Java implementation class for the condition. Click **Implementation Class** to create a new class for the processor implementation. Click **Select** to select an existing class for the processor implementation.
Input Parameters table	Specifies the input parameters that determine the result of the condition.
Open	Opens the Processor editor for the processor to which the selected input parameter is output.
Remove	Removes the selected input parameter.

Field	Use
Select	Adds an existing parameter, output from a predecessor processor in the sequence of processors in the action, as input to determine the result of the condition.

Related Topics

About Network Integrity Actions

Configuring Network Integrity Actions

About Conditions for Network Integrity

Creating Conditions for Network Integrity

Applying Conditions to Network Integrity Processors

Network Integrity Action Editor

Action Editor Realization Tab

Use the **Realization** tab to associate the Network Integrity action with a conceptual model technical action.

Field	Use
Realizes	Opens the selected technical action in the Action editor.
Select	Associates the Network Integrity action with a conceptual model technical action. To select from the available conceptual model technical actions, there must be a dependency defined between your Network Integrity cartridge project and the Model project in which your conceptual model is saved. See Managing Project Dependencies for more information.

Related Topics

Working with Conceptual Models

About Network Integrity Actions

Configuring Network Integrity Actions

Network Integrity Action Editor

Address Handler Editor

Use the Address Handler editor to configure address handlers. To access the Address Handler editor, double-click an address handler entity.

Use the **Details** tab to select the implementation class for the address handler and to specify information about the address handler.

Field	Use
Implementation Class	Specify the Java type that implements the specification. Create a new class or select an existing one.
Implementation Prefix	Displays the value of the component name.
Documentation	Specify any other information about the address handler.

Related Topics

Configuring Network Integrity Actions

About Address Handlers for Network Integrity

Adding Address Handlers to Network Integrity Actions

Model Collection Editor

Use the Model Collection editor to configure model collections. To access the Model Collection editor, double-click a model collection entity.

Use the **Model** tab to add specifications to the model collection.

Field	Usage
Model list	Lists the specifications contained in the model collection. • **Name**: the name of the specification • **Type**: the type of specification • **Project**: the name of the cartridge project to which the specification belongs
Open	Open the Specification editor for the selected specification.
Remove	Remove the selected specification from the model collection.
Select	Add specifications to the model collection. This dialog box lists specifications from other, dependent cartridge projects.

Related Topics

Configuring Network Integrity Actions

About Model Collections for Network Integrity Actions

Creating Network Integrity Model Collections

Adding Specifications to Network Integrity Model Collections

Adding Model Collections to Network Integrity Actions

4

Working with Network Integrity Processors

In the Design Studio for Network Integrity feature, processors perform the sub-tasks of actions. Use Design Studio to add processors to actions.

When working with processors, see the following topics:

About Network Integrity Processors

Processors perform the sub-tasks of actions. By adding processors to an action, the action performs several complex functions.

For example, a processor is included in an action to discover network devices, another processor is included to model the data from a network device, and another processor is added to save the modeled data to the database. Combined, these processors make up a discovery action.

Processors are of different types:

- **Discovery processor**: discovers network data through various technologies and protocols (such as TL1 or CORBA).
- **Import processor**: imports data from an inventory system.
- **Assimilation processor**: processes discovered data.
- **Discrepancy detection processor**: discovers discrepancies between imported and discovered data.
- **Discrepancy resolution processor**: resolves discrepancies between imported and discovered data.
- **SNMP processor**: discovers simple network management protocol (SNMP)-enabled network devices using SNMP. See "About the Network Integrity SNMP Processor" for more information.
- **File transfer processor**: transfers files from a remote location to an Oracle Communications Network Integrity file system. See "About the Network Integrity File Transfer Processor" for more information.
- **File parser processor**: used to parse XML and ASCII files and rewrite them in a Java implementation. See "About the Network Integrity File Parser Processor" for more information.

Related Topics

Creating Network Integrity Processors

Configuring Network Integrity Processors

Adding Existing Processors to Network Integrity Actions

Network Integrity Processor Editor

Creating Network Integrity Processors

You can create processors as part of configuring an action or you can create them independently.

See "Adding New Processors to Network Integrity Actions" for more information about creating processors as part of configuring an action.

To create processors independently:

1. From the **Studio** menu, select **New**, then select **Integrity**, then select **Processor**, and then select one of the processor types.

   The Processor Wizard for the type of processor you selected appears.
2. From the **Project** list, select the cartridge project in which to include the processor.
3. In the **Name** field, enter a name for the processor.

   The **Implementation Prefix** field takes the component name by default.
4. (Optional) In the **Folder** field, select a location for the processor.

   If you leave the **Folder** field blank, the specification is created in the default workspace.
5. Click **Finish**.

   Design Studio creates the new processor and displays the Processor editor.
6. Configure the processor.
   - To configure assimilation, discovery, discrepancy detection, discrepancy resolution, or import processors, see "Configuring Network Integrity Processors".
   - To configure SNMP processors, see "Configuring Network Integrity SNMP Processors".
   - To configure file transfer processors, see "Configuring Network Integrity File Transfer Processors".
   - To configure file parser processors, see "Configuring Network Integrity File Parser Processors".

Related Topics

About Network Integrity Processors

Adding Existing Processors to Network Integrity Actions

Network Integrity Processor Editor

Configuring Network Integrity Processors

To configure a processor:

1. Open the Processor editor **Details** tab.
2. (Optional) In the **Description** field, enter a description for the processor.
3. In the **Implementation Class** field, do one of the following:
   - To create a new Java implementation class, click the **Implementation Class** link.

     The New Java Class dialog box appears. Click the Help icon in the dialog box for more information about creating the Java class.
   - To choose an existing implementation class, click **Select**.

     The Select Java Implementation dialog box appears.

     Select an implementation class from the **Matching Items** list. You can filter the **Matching Items** list by typing in the **Choose type that implements interface** field.
4. (Optional) In the **Documentation** field, enter additional information about the processor.
5. Add context parameters.

   See "About Context Parameters for Network Integrity Processors" for more information.
6. Add property groups and properties.

   See "About Properties and Property Groups" for more information.
7. Save the processor.

Related Topics

About Network Integrity Processors

Creating Network Integrity Processors

Adding Existing Processors to Network Integrity Actions

Network Integrity Processor Editor

About Context Parameters for Network Integrity Processors

Context parameters identify individual inputs to, and outputs from, processors. These parameters are defined by name, data type, and description. Input and output parameters, with other processor-specific attributes like properties, are used in generated classes.

Configure context parameters on the Processor editor **Context Parameters** tab.

You can add the following types of context parameters:

- **Input parameters**: an object, output from a predecessor processor in the sequence of processors in the action, that contains parameters relevant to the current processor.
- **Output parameters**: an object, that is created or modified by the processor. If a processor is configured with an output parameter, Design Studio sets the interface to have the response object as the return type.

Related Topics

About Network Integrity Processors

Creating Network Integrity Processors

Configuring Network Integrity Processors

Adding Input Parameters to Network Integrity Processors

Adding Output Parameters to Network Integrity Processors

Configuring Network Integrity File Transfer Processors

Configuring Network Integrity File Parser Processors

Network Integrity Processor Editor

Adding Input Parameters to Network Integrity Processors

To add input parameters to a processor:

1. On the Processor editor **Context Parameter** tab, in the Input Parameters area, click **Select**.

   The Select Output Parameter dialog box appears.

2. From the list of parameters output by predecessor processors in the sequence of processors in the action, select parameters to add as input.

   Design Studio displays a warning message if there are no valid output parameters to choose from.

3. Click **OK**.

   Design Studio adds the output parameters to the Input Parameters area of the current processor.

Related Topics

About Context Parameters for Network Integrity Processors

Adding Output Parameters to Network Integrity Processors

About Network Integrity Processors

Configuring Network Integrity Processors

Configuring Network Integrity File Transfer Processors

Configuring Network Integrity File Parser Processors

Network Integrity Processor Editor

Adding Output Parameters to Network Integrity Processors

To add output parameters to a processor:

1. On the Processor editor **Context Parameter** tab, in the Output Parameters area, click **Add**.

   The Create Output Parameter dialog box appears.

2. In the **Parameter Name** field, enter a name for the parameter.

3. From the **Parameter Type** list, do one of the following:

   - Select a primitive type.

- Click **Browse** and select an existing qualified Java class name.
- Enter a valid and available Java object. This value is automatically validated to ensure that it is a valid Java object type.
- Enter a Java generic. For example, **java.util**.*primitive***<String>**.

4. (Optional) In the **Description** field, add information about the parameter.
5. Click **OK**.

   Design Studio generates the Request and Response Java classes.

Related Topics

About Context Parameters for Network Integrity Processors

Adding Input Parameters to Network Integrity Processors

About Network Integrity Processors

Configuring Network Integrity Processors

Network Integrity Processor Editor

About Properties and Property Groups

A property group is a container that contains properties. Properties are name/value pairs that are passed to the processor through the property group.

Design Studio generates the Java class for the property group so you can access the property values using getter and setter methods.

You can configure property groups as managed groups and as map groups. Map property groups produce a simplified API for properties used as maps.

Property values can be set in the following ways:

- At design time, by setting the property with a static value.
- At deployment time, by setting the property with a cartridge model variable.
- At run time, using the MBean interface, by configuring its property group as a managed group.

You can configure properties as sensitive. Sensitive properties must be contained in managed property groups. Therefore, you can set the value of sensitive properties at run time. You can also set sensitive property values at deployment time by setting it with a model variable. Sensitive properties cannot have static values.

For more information about properties and property groups, see *Network Integrity Developer's Guide*.

Related Topics

Adding Property Groups to Network Integrity Processors

Adding Properties to Network Integrity Property Groups

About Network Integrity Processors

Configuring Network Integrity Processors

Working with Model Variables

Adding Property Groups to Network Integrity Processors

To add property groups to a processor:

1. On the Processor editor **Properties** tab, in the Property Groups area, click **Add**.

   The Create Property Group dialog box appears.
2. In the **Name** field, enter a name for the property group.
3. (Optional) In the **Description** field, add information to identify the property group.
4. (Optional) To configure the property group as a managed property group, select the **Managed** check box.

   A managed property group is configurable at run time using the MBean interface. Managed property groups can contain sensitive properties.
5. (Optional) To configure the property group as a map property group, select the **Map** check box.

   A map property group produces a simplified API for properties used as maps.
6. Click **OK**.

   Design Studio creates the property group and adds it to the Property Groups area.
7. Save the processor.

Related Topics

About Properties and Property Groups

Adding Properties to Network Integrity Property Groups

About Network Integrity Processors

Configuring Network Integrity Processors

Working with Model Variables

Network Integrity Processor Editor

Adding Properties to Network Integrity Property Groups

To add properties to property groups:

1. On the Processor editor **Properties** tab, in the Property Groups area, select a property group.
2. In the Properties area, click **Add**.

   The Create Property dialog box appears.
3. In the **Name** field, enter a name for the property.
4. (Optional) To configure the property as sensitive, select the **Sensitive** check box.

   Sensitive property values must either be left blank or be assigned to a model variable. Sensitive properties can only be contained in managed property groups.
5. In the **Value** field, define the property value.

   Do one of the following:

   - To define a static value, enter the value in this field.

- To not define a value, leave this field blank.
- To define the property value with a model variable, select a model variable from the **Model Variables** list.

  Model variables allow you to set the property value at deployment time.

6. (Optional) In the **Description** field, add information to identify the property.
7. Click **OK**.

   The property is added to the property group.
8. Save the processor.

Related Topics

About Properties and Property Groups

Adding Property Groups to Network Integrity Processors

About Network Integrity Processors

Configuring Network Integrity Processors

Working with Model Variables

Network Integrity Processor Editor

About the Network Integrity SNMP Processor

The SNMP processor is a fully-implemented, code-generated discovery processor for SNMP-enabled network devices.

The SNMP processor sends a request to the SNMP device and receives the response. The response consists of a strongly-typed XML file which represents the raw SNMP results.

The processor interface, request, response, properties, and relevant helper classes are code-generated and fully implemented.

Before you can create SNMP processors, specify the management information base (MIB) directory in the Design Studio preferences for Network Integrity. See "Configuring Network Integrity Preferences" for more information.

Related Topics

About Network Integrity Processors

Configuring Network Integrity SNMP Processors

Configuring Network Integrity SNMP Processors

This procedure assumes you have specified the MIB directory in the Design Studio preferences for Network Integrity. See "Configuring Network Integrity Preferences" for more information.

To configure SNMP processors:

1. On the Processor editor **SNMP** tab, click **Load MIB** to load the MIB files into the SNMP processor.

   The Select MIB Files to Load dialog box appears.

2. From the **Matching Items** list, select MIB files.

   You can filter the **Matching Items** list by typing in the **Select an item to open** field.

3. Click **OK**.

   Design Studio adds the MIBs to the SNMP area.

4. Add OIDs to the SNMP table:

   a. In the SNMP Data Tree area, expand the MIBs until you reveal its objects.

   b. Select an object and click **Add**.

      Network Integrity supports only scalar and table column objects.

      Design Studio adds the object and its information to the SNMP table.

   SNMP processors must contain at least one OID.

5. Save the processor.

Related Topics

About Network Integrity Processors

About the Network Integrity SNMP Processor

Creating Network Integrity Processors

Network Integrity Processor Editor

About the Network Integrity File Transfer Processor

The file parser processor moves files from a remote location to a Network Integrity file system using FTP or SFTP protocols. The file parser processor can also be used to access files that are on a file system that is shared by all the nodes in a Network Integrity cluster.

The file parser processor can be used in discovery, import, and assimilation actions.

File transfer processors generate collections of Java file objects as output context parameters. These parameters are pointers to local file system versions of the transferred files. All subsequent processors in the parent action have access to the files retrieved by the file parser processor.

File transfer processors can retrieve parameter values from the following sources:

- From scan parameter groups: When the **Parameter Source** field is set to the **Scan Parameter Group** option, the file parser processor parameter values are set by the Network Integrity user in the UI.
- From context parameters: When the **Parameter Source** field is set to the **Context Parameter** option, the file parser processor parameter values are inherited from predecessor processors in the sequence of processors in the action.

For more information about file transfer, see *Network Integrity File Transfer and Parsing Guide*.

Related Topics

About Network Integrity Processors

Configuring Network Integrity File Transfer Processors

About the Network Integrity File Parser Processor

The file parser processor is a fully-implemented, code-generated processor that parses XML- and ASCII-delimited files into Java. The file parser processor outputs an iterable that the other processors can use to access the records and data in the file.

The file parser processor can be used in discovery, import, and assimilation actions.

For more information about file parsing, see *Network Integrity File Transfer and Parsing Guide*.

Related Topics

About Network Integrity Processors

Configuring Network Integrity File Parser Processors

Configuring Network Integrity File Parser Processors

This procedure assumes that the file parser processor has already been created and added to an action. You cannot configure the file parser processor unless it belongs to an action. See "Creating Network Integrity Processors" and "Adding Existing Processors to Network Integrity Actions" for more information.

The **File Parameter** field is mandatory and indicates what context parameter holds the reference to the files to be parsed at run time. The context parameter holding the file references must be output by a predecessor processor in the sequence of processors in the action. The processor outputting the file parameter is typically a file parser processor that has transferred the files from a remote system, but it can be any type of processor.

To configure a file parser processor:

1. On the Processor editor **Details** tab, in the **Parser Type** field, specify the type of file to be parsed.
2. In the **File Parameter** field, specify the input file parameter:
   a. Next to the **File Parameter** field, click **Select**.

      The Select Output Parameter dialog box appears, listing java.util.Collection.java.io.File context parameters output by predecessor processors in the sequence of processors in the action. If there are no available context parameters, an error message appears.

   b. Select a parameter.

   c. Click **OK**.
3. Configure the file parser processor for the selected parser type:
   - If you specified the **ASCII** option in the **Parser Type** field, configure the ASCII file parser processor settings.

     See "Configuring Network Integrity File Parser Processor ASCII Settings".
   - If you specified the **XML** option in the **Parser Type** field, configure the XML file parser processor settings.

     See "Configuring Network Integrity File Parser Processor XML Settings" for more information.
4. Add context parameters.

   See "About Context Parameters for Network Integrity Processors" for more information.

5. Save the processor.

Related Topics

About Network Integrity Processors

Creating Network Integrity Processors

About the Network Integrity File Parser Processor

Network Integrity Processor Editor

About Records for Network Integrity File Parser Processors

You can specify multiple header, body, or trailer records. If two header records are defined, the first two records in the file are header records and must match the definition specified. Similarly for multiple body and trailer records: if four trailer records are defined, then the last four records defined in the file are trailer records. When specifying multiple records of the same record type, the order of the records becomes important.

You can either create record definitions or import record definitions from an ASCII file.

After a record is created, its fields become editable.

The file parser processor outputs an iterable for each record returned from the file at run time. The iterable can be used within a For Each processor so that the processor can be written to handle a single record at a time.

Related Topics

Configuring Network Integrity File Parser Processor ASCII Settings

Network Integrity Processor Editor

Importing ASCII Record Definitions to Network Integrity File Parser Processors

You can import record definitions from a sample delimited file to discover field names and to populate the record and field definitions.

Before importing record definitions, the sample file must conform to the following:

- Sample files must have a header with field names.
- Sample files cannot have empty header field names.
- Field names must be unique. If the sample file contains duplicate field names, Design Studio displays a warning message and appends a prefix to the field names to differentiate them.

> **Note:**
>
> Importing ASCII record definitions only imports a single header record and matching body record. Any existing records and fields defined in the file parser processor are deleted. The created header record is marked as Ignored by default.

To import ASCII record definitions:

1. From the ASCII Parser Definition area, click the **Import** button.

The Import Sample ASCII File dialog box appears.

2. (Optional) Change the following default values:
   - In the **Header Record Name** field, enter a name for the header record.
   - In the **Body Record Name** field, enter a name for the body record.
   - From the **Field Delimiter** list, specify a field delimiter.

     If you specify **Custom**, enter the custom field delimiter expression in the **Custom Field Delimiter** field.
3. In the **Sample File Path** field, enter the path to the sample ASCII file to import.

   Click the **Browse** button to navigate to the location of the sample file.
4. Click **OK**.

   Design Studio imports the sample ASCII file. The record definitions appear in the Record Definition Details area.
5. Create trailer records.

   You cannot import trailer records. See "Configuring Network Integrity File Parser Processor ASCII Settings" for more information.

Configuring Network Integrity File Parser Processor XML Settings

A file parser processor configured to parse XML files uses an XML schema to generate an XMLBeans representation of the XML schema file to bind it to Java types.

> **Note:**
>
> It is recommended that you create a **schemas** directory in the project and put all XML schemas in this directory. If a different cartridge needs to parse different types of XML documents, defined by different schemas, you can create separate directories. For more information about XML schemas, see *Network Integrity File Transfer and Parsing Guide*.

To configure file parser processor XML settings:

1. On the Processor editor **XML** tab for the file parser processor, next to the **XML Schema** field, click **Select**.

   The Select XML Schema dialog box appears.
2. From the **Matching Resources** list, select the XML schema.

   You can filter the **Matching Resources** list by typing in the **Select a resource to open** field.

   Only schemas that are in the current project appear in the Select XML Schema dialog box.
3. Click **OK**.

   Design Studio displays the relative path to the schema in the **XML Schema** field.
4. Save the processor.

> **Note:**
>
> If your XML Schema file contains import elements that do not specify the schema location, and if you are working in an environment that uses a proxy server for HTTP access, you must configure the proxy settings for Design Studio. See *Design Studio System Administrator's Guide* for more information.
>
> Schemas sometimes import other schemas. You may need to include imported schemas in the project at the correct directory.

Configuring Network Integrity File Parser Processor ASCII Settings

A file parser processor that is configured to parse ASCII-delimited files uses parsing rules, records, and field definitions to generate Java classes for accessing file data and to parse input files at run time.

To configure file parser processor ASCII settings:

1. On the Processor editor **ASCII** tab, from the **Record Delimiter** list, select the delimiter type that indicates a new record.
2. Do one of the following:
   - Import a list of record definitions. See "Importing ASCII Record Definitions to Network Integrity File Parser Processors" for more information.

     > **Caution:**
     >
     > Importing record definitions removes all existing record definitions.

   - Create record definitions:
     a. In the Record Definitions area, click **Add**.

        The Create Record Definition dialog box appears.

     b. In the **Name** field, enter a name for the new record.

     c. Click **OK**.

        Design Studio adds the record to the Record Definitions area.

     d. In the Record Definitions area, select a record and configure it.

        All the columns in the Record Definitions area are editable fields. See "Processor Editor ASCII Tab" for information about the fields in the Record Definitions area.
3. Add field definitions to records:
   a. In the Record Definitions area, select a record name.

   b. In the Field Definitions area, click **Add**.

      The Create Field Definition dialog box appears.

   c. In the **Name** field, enter a name for the field definition.

   d. Click **OK**.

      Design Studio adds a field definition to the Field Definitions area for the selected record.

e. In the Field Definitions area, select a field definition and configure it.

   All columns in the Field Definitions area are editable fields. See "Processor Editor ASCII Tab" for information about the fields in the Field Definitions area.

Related Topics

About Records for Network Integrity File Parser Processors

Configuring Network Integrity File Parser Processors

Network Integrity Processor Editor

Network Integrity Processor Editor

Use the Processor editor to create and configure a processor. To access the Processor editor, double-click a processor entity. The tabs in the Processor editor depend on the type of processor.

When using the Processor editor, see the following topics:

- Processor Editor Details Tab
- Processor Editor Context Parameters Tab
- Processor Editor Properties Tab
- Processor Editor SNMP Tab
- Processor Editor File Transfer Tab
- Processor Editor XML Tab
- Processor Editor ASCII Tab

Configuring Network Integrity File Transfer Processors

This procedure assumes that the file parser processor has already been created and added to an action. You cannot configure the file parser processor unless it belongs to an action. See "Creating Network Integrity Processors" and "Adding Existing Processors to Network Integrity Actions" for more information.

To configure a file parser processor:

1. On the Processor editor **File Transfer** tab, specify the input parameter source by doing one of the following:
   - To inherit input parameters from a predecessor processor in the sequence of processors in the action, specify the **Context Parameter** option.

     A predecessor processor sets file transfer context parameter values. For more information about file transfer context parameters, see "Configuring File Transfer Properties for Network Integrity File Transfer Processors".
   - To allow Network Integrity users to specify the input parameters in the UI, specify the **Scan Parameter Group** option and do one of the following:
     – To select an existing scan parameter group, click **Select**.
     – To create a new scan parameter group, click **Scan Parameter Group**.

       Design Studio builds the new scan parameter group using information from the Network Integrity SDK cartridge.

See "About FTP Characteristics for Network Integrity File Transfer Processors" for more information about the input parameters for configuring file transfer processors from the Network Integrity UI.

2. Configure the address parameter.

   See "Configuring the Address Parameter for Network Integrity File Transfer Processors" for more information.

3. Configure the file transfer properties.

   See "Configuring File Transfer Properties for Network Integrity File Transfer Processors" for more information.

4. Add context parameters.

   See "About Context Parameters for Network Integrity Processors" for more information.

5. Save the processor.

Related Topics

About Network Integrity Processors

About the Network Integrity File Transfer Processor

Network Integrity Processor Editor

About FTP Characteristics for Network Integrity File Transfer Processors

The following table lists the default and required input parameters for configuring file transfer processors from the Network Integrity UI.

Characteristic Name	Default	Mandatory	Description
ftaFileTransferType	FTP	Yes	Indicates how files should be transferred (FTP, SFTP, Local). **Note:** Do not add or remove options or the file parser processor will have errors.
ftaFilePattern	N/A	No	A pattern to match file names. The pattern supports wildcard characters. The supported wildcard characters are the asterisk, percent, and underscore. The asterisk and percent represent a match of zero or more characters, while the underscore represents a match of a single character. Wildcard characters can be escaped with a slash \.
ftaPort	N/A	No	The port used to connect to the remote server. If not specified, defaults to 21 for FTP and 22 for SFTP.
ftaUser	N/A	No	The user name to connect to the remote location.
ftaPassword	N/A	No	The password to connect to the remote location.
ftaSessionTimeOut	60	No	The amount of time, in seconds, before an idle connection times out. The valid range is from 1 to 3600.
ftaSourceFileManagement	Rename	No	Indicates the action to take on source files when the file transfer is complete. Options are Delete, Rename, Nothing. **Note:** Do not add or remove options or the file parser processor will have errors.
ftaRenameSuffix	Processed	No	The suffix to add to the source file if the ftaSourceFileManagement is set to **Rename**.

Configuring the Address Parameter for Network Integrity File Transfer Processors

The address parameter indicates the host and directory to retrieve the files from. It must be in the format *host/directory* for FTP or SFTP transfer types, where *host* can be an IPv4 or IPv6 address, or a host name, and *directory* is a file path, for example, **10.10.10.10/tmp/files**.

For local file system transfer types, the address field holds the directory name only. The directory name must start with a slash. For example, **/tmp/files**.

To configure the Address Parameter:

1. On the Processor editor **File Transfer** tab, do one of the following:
   - To retrieve the address from the discovery action scope address defined in the Network Integrity UI, select the **Use Scope Address** check box.

     This option is available only for discovery actions.
   - Click **Select** next to the **Address Parameter** field.

     A dialog box opens, listing string-type parameters. Select the parameter representing the address and click **OK**.

     If there are no string-type parameters, an error message appears.

Related Topics

About the Network Integrity File Transfer Processor

Configuring Network Integrity File Transfer Processors

Network Integrity Processor Editor

Configuring File Transfer Properties for Network Integrity File Transfer Processors

The file transfer context parameters are set in predecessor processors in the sequence of processors in the action so that some or all of the properties can be defined in the action. You can configure the action to specify all the file transfer properties programmatically, rather than requiring the user to enter values.

For example, when a processor at the beginning of an action calls an external system or device to generate a file containing device data, the processor triggers the generation of a file, and then programmatically sets the file transfer properties with information such as file name pattern and the directory where the file can be found.

To select the file transfer context parameters:

1. Click the Processor editor **File Transfer** tab for the file parser processor.
2. In the Input Parameters area, click **Select**.

   The Select Output Parameter dialog box appears listing, oracle.communications.sce.integrity.sdk.fileTransfer context parameters output by predecessor processors in the sequence of processors in the action. If there are no available context parameters, an error message appears.
3. Select a parameter.
4. Click **OK**.

Related Topics

About the Network Integrity File Transfer Processor

Configuring Network Integrity File Transfer Processors

Network Integrity Processor Editor

Processor Editor Details Tab

Use the **Details** tab to select the implementation class for the processor and specify other information about the processor.

The **Details** tab is available for all processor types.

Field	Use
Description	Enter a short description of the processor.
Parser Type	Specify the type of files the processor can parse. Appears for file parser processors only.
File Parameter	Specify the input file parameter generated as output by a predecessor processor in the sequence of processors in the action. The file parameter must be of type java.util.Collection.java.io.File. If there are no available context parameters, an error message appears. Appears for file parser processors only.
Implementation Class	Specify the Java implementation class for the processor. Design Studio automatically generates an interface class that the implementation class must implement. You can select an existing class, or create a new one by clicking the **Implementation Class** link. The implementation class is created to match the processor interface. This field is read-only for some processor types.
Implementation Prefix	Displays the Java name for the entity.
Documentation	Add other information about the processor.

Related Topics

About Network Integrity Processors

Creating Network Integrity Processors

Configuring Network Integrity Processors

Network Integrity Processor Editor

Processor Editor Context Parameters Tab

Use the **Context Parameters** tab to manage input and output parameters for the processor.

The **Context Parameters** tab is available for assimilation, discovery, discrepancy detection, discrepancy resolution, file transfer, file parser, and import processors.

Input Parameters Area

Field	Use
Name	Displays the parameter name.

Field	Use
Type	Displays the parameter type.
Source	Displays the processor from which the parameter is produced.
Description	Displays the parameter description.
Open	Open the Processor editor for the processor from which the parameter is produced.
Remove	Remove the selected input parameter.
Select	Select an existing output parameter from a predecessor processor in the sequence of processors in the action to add as an input parameter to this processor.

Output Parameters Area

Field	Use
Name	Displays the parameter name output by the current processor.
Type	Displays the parameter type.
Description	Displays the parameter description.
Usage	Lists the processors that use the parameter as an input parameter.
Open	Modify the output parameter.
Remove	Removes the selected output parameter.
Add	Create an output parameter to add to the processor.

Related Topics

About Network Integrity Processors

Creating Network Integrity Processors

Configuring Network Integrity Processors

About Context Parameters for Network Integrity Processors

Network Integrity Processor Editor

Processor Editor Properties Tab

Use the **Properties** tab to manage property groups and properties for the processor.

The **Properties** tab is available for assimilation, discovery, discrepancy detection, discrepancy resolution, and import processors.

Property Groups Area

Field	Use
Name	Displays the name of the property group.
Managed	Set the property group as managed. Properties belonging to managed property groups can be set during run time using the MBean interface. A property group must be managed to contain a sensitive property.
Map	Set the property group as a map. Design Studio generates a simplified API for map property groups.

Field	Use
Description	Enter additional information about the property group.
Add	Create a property group.
Remove	Remove a property group.

Properties Area

Field	Use
Name	Displays the name of the property.
Value	Edit the property value. The value can be left blank, set to a static value, or assigned a model variable. Properties with model variables as values can be set at deployment time.
Sensitive	Specify whether the property is sensitive. Sensitive properties can only be contained in managed property groups. Sensitive properties values are encrypted and are never displayed to users.
Description	Enter additional information about the property.
Add	Create a property in the selected property group.
Remove	Remove the property from the selected property group.

Related Topics

About Network Integrity Processors

Creating Network Integrity Processors

Configuring Network Integrity Processors

About Properties and Property Groups

Network Integrity Processor Editor

Processor Editor SNMP Tab

Use the **SNMP** tab to load object IDs (OIDs) for the SNMP processor to poll.

The **SNMP** tab is available for SNMP processors.

Field	Use
SNMP Data Tree area	Lists the MIB files that are loaded into the SNMP processor.
Add	Add the selected OID from the **SNMP data tree** to the Loaded OID area.
Remove	Remove the selected OID from the Loaded OID area.
Load MIB	Select MIB files to load into the SNMP processor.
Full Name	Displays the full name of the selected MIB object.
OID	Displays the object ID of the selected MIB object.
Description	Displays the description of the selected MIB object.
Loaded OID area	Lists the MIB objects that the SNMP processor will poll for.

Related Topics

About the Network Integrity SNMP Processor

Creating Network Integrity Processors

Configuring Network Integrity Processors

Network Integrity Processor Editor

Processor Editor File Transfer Tab

Use the **File Transfer** tab to configure the file transfer settings for file parser processors.

The **File Transfer** tab is available for file parser processors.

Field	Use
Parameter Source	Specify the parameter source for the file parser processor. Select **Scan Parameter Group** to allow the user to provide the parameter values using scan parameter groups. Select **Context Parameter** to allow the processor to inherit parameter values from the output of predecessor processors in the sequence of processors in the action.
Scan Parameter Group	Specify the scan parameter group used to pass parameter values to the processor. Clicking **Select** opens a dialog listing available scan parameter groups. This field is enabled when **Parameter Source** is set to **Scan Parameter Group**. Click the **Scan Parameter Group** link to create a new scan parameter group.
Context Parameter	Specify the processor output from which the file parser processor inherits its parameter values. Click the **Select** button to open a dialog listing available output. This field is enabled when **Parameter Source** is set to **Context Parameter**.
Address Parameter	Specify the address parameter that contains the host and directory to retrieve the files from. Click the **Select** button to open a dialog box listing available output for the address parameter. Clicking the **Address Parameter** link opens the Processor editor for the processor that generates the address parameter output.
Use Scope Address	Specify whether to use the discovery scan scope address at run time as the address parameter. Appears only if the file transfer processor is added to a discovery action.

Related Topics

About the Network Integrity File Transfer Processor

Creating Network Integrity Processors

Configuring Network Integrity File Transfer Processors

Network Integrity Processor Editor

Processor Editor XML Tab

Use the **XML** tab to configure the file parser processor XML settings.

The **XML** tab is available for file parser processors.

This tab is editable only when **Parser Type** on the Processor editor **Details** tab is set to **XML**.

Field	Use
XML Schema	Specify the XML schema and path that validates the parsing of XML files. Click the **Select** button to open a dialog box from which to choose from available XML schemas. Clicking the **XML Schema** link opens the selected XML schema in an XML editor.

Related Topics

About the Network Integrity File Parser Processor

Creating Network Integrity Processors

Configuring Network Integrity File Parser Processors

Network Integrity Processor Editor

Processor Editor ASCII Tab

Use the **ASCII** tab to configure the file parser processor ASCII settings.

The **ASCII** tab is available for file parser processors.

This tab is editable only when **Parser Type** on the Processor editor **Details** tab is set to **ASCII**.

ASCII Parser Definition Area

Field	Use
Record Delimiter	Identifies the type of expression that constitutes a new record.
Name	Enter the name of the record.
Record Type	Select the type of the record. If a header record is present, it is always the first record in a file. If a trailer record is present, it is always the last record in the file. The body records are all the records in between.
Field Delimiter	Select the character that separates fields within the record. If you select **Custom**, the Custom Field column becomes editable and a single character value must be entered in this field.
Custom Field Editor	Select the custom single character field delimiter. This column is enabled only if **Custom** is selected in the Field Delimiter column.
Aggregate Extra Fields	Specify whether the remaining data in a record should be appended to the last field element in the records list. This is useful for records that have a fixed set of information at the beginning of the record and a variable set of information at the end of the record. The fixed set can be represented as normal using field elements, and the variable set can be aggregated into the final field element for further parsing in processor code.
Ignore	Specify whether this record should be processed. Enable when the header or trailer records exist and the data that they contain does not need to be processed.
Skip Consecutive	Specify whether consecutive delimiters should be treated as multiple delimiters or as a single delimiter. Oracle recommends that you leave this option unchecked as it is preferable to report that there is an empty field between consecutive delimiters. For example, if a CSV file contained a record of "1,2,,4", then it is likely missing the 3rd field for a reason, and this fact should be reflected in the record data. However, there are cases when it is preferable to skip consecutive delimiters. This usually occurs when the field delimiter is a blank space. The reason for setting it to true (checked) in this case is that incoming records often contain multiple spaces between fields.
Move Up **Move Down**	Reorder selected record definition.
Import	Import record definitions from a sample file.

Field	Use
Remove	Remove the selected record definition.
Add	Create a record definition.

Record Definition Details Area

Field	Use
Name	Enter the name of the field, which is used to generate a getter method on a record class that can be used by subsequent processors for retrieving the data.
Ignore	Specify whether this field should be processed. If checked, a getter method is not generated for this field, and the data in this field is not accessible to the action.
Container	Specify a grouping character, which allows field-delimiter characters to be treated as regular data, provided they are contained within the specified container character. The container must be a single character, if specified.
Container is Optional	Specify whether the container character is mandatory for every record or if the container character is optional.
Move Up **Move Down**	Reorder the selected field definition.
Remove	Remove the selected field definition.
Add	Create a field definition.

Related Topics

About the Network Integrity File Parser Processor

Configuring Network Integrity Processors

Configuring Network Integrity File Parser Processors

Network Integrity Processor Editor

5

Working with Network Integrity Specifications

In the Design Studio for Network Integrity feature, specifications provide a way to classify entities and augment them with additional properties. Specifications are added to actions to classify found or produced entities.

When working with specifications for Oracle Communications Network Integrity in Design Studio, see the following topics:

About Network Integrity Specifications

A specification is a representation of an Oracle Communications Information Model entity that is augmented with characteristics using Design Studio. Each specification relates to a single Information Model entity. You can create multiple specifications that all relate to or extend the same entity.

All actions must specify which specification types they support. By default, actions support all specifications created in the same cartridge project as the action.

Specifications can be shared between cartridges. When multiple cartridges are deployed together, their shared specifications are compatible. To add specifications to actions from another cartridge project, the specifications must be added to a model collection and the model collection added to the action.

Related Topics

Creating Network Integrity Specifications

Configuring Network Integrity Specifications

Adding Characteristics to Network Integrity Specifications

Adding Specifications to Network Integrity Model Collections

About Model Collections for Network Integrity Actions

Creating Network Integrity Specifications

To create a specification in an Integrity cartridge project:

1. From the **Studio** menu, select **New**, then select **Integrity**, and then select a specification from one of the following submenus:
    - The **Administration** menu
    - The **Infrastructure** menu

- The **Resources** menu
- The **Services** menu

The Specification Wizard for the type of specification you selected appears.

2. From the **Project** list, select the cartridge project in which to include the specification.
3. In the **Name** field, enter a name for the specification.
4. (Optional) In the **Folder** field, specify a location for the specification.

   By default, Design Studio saves the entity to your default workspace. You can browse to a different location using the **Browse** button.
5. Click **Finish**.

   Design Studio creates the specification and automatically adds it to all actions in the same cartridge project as the specification.
6. Configure the processor. See "Configuring Network Integrity Specifications" for more information.

Related Topics

About Network Integrity Specifications

Adding Characteristics to Network Integrity Specifications

Adding Specifications to Network Integrity Model Collections

About Model Collections for Network Integrity Actions

Network Integrity Specification Editor

Configuring Network Integrity Specifications

To configure Network Integrity Specifications:

1. In the Studio Projects view, double-click a specification.

   The Specification editor appears.
2. (Optional) In the **Display Name** field, enter a display name for any localizable languages.

   Design Studio supports multiple languages for this field. You can specify a name for each language available in the list beside the **Display Name** field.

   If your preferences are set up to work in one language only, the list displays only the **[default]** option. See "Defining Language Preferences" for more information.
3. Do one of the following:
   - Add characteristics to the specification.

     See "Adding Characteristics to Network Integrity Specifications" for more information.
   - Add configuration items.

     See "Adding Configuration Items" for more information. Configuration items can be added to configuration specification types only.

     See "About Configurations" for more information about configuration specification types.
4. Define the layout for the specification.

   See "Defining Network Integrity Specification Layouts" for more information.

5. Define UI settings for the specification characteristics.

   See "Defining Network Integrity Specification Layouts" for more information.

6. (Optional) To add the specification to an action in another cartridge project, do the following:

   a. Ensure the cartridge project containing the action is dependent on the cartridge project containing the specifications.

      See "Managing Project Dependencies" for more information.

   b. Add the new specification to a model collection in the other cartridge project.

      See "Adding Specifications to Network Integrity Model Collections" for more information.

   c. Add the model collection to the action.

      See "Adding Model Collections to Network Integrity Actions" for more information.

Related Topics

About Network Integrity Specifications

Creating Network Integrity Specifications

Network Integrity Specification Editor

Adding Characteristics to Network Integrity Specifications

Specifications can be augmented with characteristics to collect information about entities. Some specifications come with default characteristics.

You can add characteristics to Network Integrity specifications in the following ways:

- Creating Characteristics from the Network Integrity Specification Editor
- Adding Existing Characteristics to Network Integrity Specifications

Creating Characteristics from the Network Integrity Specification Editor

To create characteristics from the Specification editor:

1. On the Specification editor **Characteristics** tab for a Network Integrity specification, right-click the data tree area and select **Add Characteristic**.

   The Create and Add Characteristic dialog box appears.

2. Do the following:

   - From the **Primitive Type** list, select the data type for the characteristic.

     Depending on the data type you select, some fields may not appear.

   - In the **Name** field, enter the name for the characteristic.
   - In the **Display Name** field, enter the display name for the characteristic.

     The display name is the name of the input field in the Network Integrity UI.

   - In the **Multiplicity** field, specify whether the characteristic is required.

     Do not select **Range**.

- In the Length area, use the **Maximum** and **Minimum** fields to specify the length for string data types. Select the **Unbounded** check box to not set an explicit maximum value.
- (Optional) In the **Default** field, enter a default value.

3. Click **Finish**.

   Design Studio creates the data element in the data schema as a characteristic and adds the new characteristic to the Specification editor **Characteristics** tab.

4. Configure the characteristic.

   See "Creating Characteristics" in the Modeling Inventory Help for more information.

Adding Existing Characteristics to Network Integrity Specifications

To add existing characteristics to a specification:

1. On the Specification editor **Characteristics** tab for a Network Integrity specification, right-click the data tree area and click **Select Characteristic**.

   The Select Characteristic dialog box appears. The dialog box lists characteristics from the current cartridge project and from dependent cartridge projects. See "Managing Project Dependencies" for more information.

2. Select one or more characteristics.

   You can filter the list by element name by typing in the **Element** field and clicking the **Filter** icon, or by entity name by typing in the **Entity Name** field and clicking the **Filter** icon.

3. Click **OK**.

   Design Studio adds the characteristics to the Specification editor **Characteristics** tab.

Defining Network Integrity Specification Layouts

You define layouts for specifications to specify how and where characteristics appear as fields in the Network Integrity UI scan results.

To define specification layouts:

1. On the Specification editor **Layouts** tab, select a characteristic.

   > **Note:**
   >
   > Design Studio for Network Integrity does not support suppressing characteristics from the run-time UI. All characteristics appear in the run-time UI.

2. Organize the order of the characteristics:

   a. From the **Selected** list, select a characteristic.

   b. Click the **Up Arrow** or **Down Arrow** icons.

3. (Optional) To add rows, right-click a characteristic and select **Insert New Row**.

   Characteristics appear in the order indicated from left to right in the Network Integrity UI. By inserting a row, the proceeding characteristics restart on the left of the UI on a new row.

4. Save the specification.

> **Note:**
>
> Clicking the **Reset** button resets the order of the characteristics in the Panels / Elements area and remove any added rows.

Related Topics

Creating Network Integrity Specifications

Network Integrity Specification Editor

Defining UI Settings for Network Integrity Specification Characteristics

You define the UI settings for each characteristic on a specification to determine how it appears in the Network Integrity UI scan results. Repeat the procedure for all characteristics appearing in the UI.

To define UI settings for a characteristic:

1. On the Specification editor **Layouts** tab, from the **Selected** list, select a characteristic.

   The configurable options for the characteristic appear in the UI Settings area.
2. Configure the following UI settings:
   a. In the **Display Name** field, enter the field name as you want it to appear in the Network Integrity UI.
   b. In the **ToolTip** field, enter a tooltip value for the field, to appear when a user mouses over the field in the Network Integrity UI.

   All other fields inherit their values from the data schema.
3. Save the specification.

Related Topics

Creating Network Integrity Specifications

Network Integrity Specification Editor

Network Integrity Specification Editor

Use the Specification editor to augment and configure Network Integrity specifications. To access the Specification editor, double-click a Network Integrity specification entity.

The tabs in the Specification editor depend on the type of specification.

When using the Specification editor, see the following topics:

- Specification Editor Characteristics Tab
- Specification Editor Layouts Tab
- Specification Editor Extends Tab
- Specification Editor Details Tab

Specification Editor Characteristics Tab

Use the **Characteristics** tab to create, add, and configure characteristics for specifications or to remove characteristics from specifications.

Characteristics belonging to sealed cartridges are read-only.

When working with the **Characteristics** tab, see the following topics:

- About the Characteristics Tab Context Menu for Specifications
- Usage Tab
- Notes Tab

About the Characteristics Tab Context Menu for Specifications

The **Characteristics** tab context menu contains commands specific to specification characteristics. To access the context menu, right-click in the left column of the tab. The context menu options that are available depend on the selection in the editor.

Field	Use
Add Characteristic	Create a new characteristic to add to the specification.
Select Characteristic	Add an existing characteristic to the specification.
Delete	Delete a characteristic.
Refactoring	Select to access a menu of options for improving names and locations of the characteristics. See "Refactoring Entities and Data Elements" for more information.
Refresh	Refresh the view.

Related Topics

About Network Integrity Specifications

Creating Network Integrity Specifications

Adding Characteristics to Network Integrity Specifications

Network Integrity Specification Editor

Specification Editor Layouts Tab

Use the **Layouts** tab to configure which characteristics appear in the Network Integrity UI scan results.

Field	Use
Page/Panels	Select the Network Integrity run-time page to lay out.
Available	Lists the characteristics available to be displayed in the Network Integrity UI for the selected page or panel.
Selected	Lists the characteristics to be displayed in the Network Integrity UI for the selected page or panel.

Field	Use
Left Arrow **Right Arrow** **Up Arrow** **Down Arrow**	Move characteristics back and forth between the **Selected** and **Available** lists and to reorder the characteristics in the **Selected** list.
UI Settings area	Displays the available UI settings for the selected characteristic.
Reset	Revert the layout back to the most recently saved version.

Related Topics

About Network Integrity Specifications

Creating Network Integrity Specifications

Defining Network Integrity Specification Layouts

Defining UI Settings for Network Integrity Specification Characteristics

Network Integrity Specification Editor

Specification Editor Extends Tab

Use the **Extends** tab to display the Information Model entity type to which the specification belongs.

Related Topics

About Network Integrity Specifications

Creating Network Integrity Specifications

Network Integrity Specification Editor

6

Working with Network Integrity Scan Parameter Groups

Use Design Studio to create and configure scan parameter groups and to assign them to actions. Add characteristics to scan parameter groups to add input fields to the Oracle Communications Network Integrity UI, where the user can pass parameter values to run-time scans.

When working with scan parameter groups, see the following topics:

About Network Integrity Scan Parameter Groups

Scan parameter groups allow you customize the Network Integrity UI by adding input fields for configuring assimilation, discovery, and import scans. Input field values are passed to actions at run time.

Related Topics

Creating Network Integrity Scan Parameter Groups

About Characteristics for Network Integrity Scan Parameter Groups

Network Integrity Scan Parameter Group Editor

Creating Network Integrity Scan Parameter Groups

To create a scan parameter group:

1. Do one of the following:
   - From the **Studio** menu, select **New**, then select **Integrity**, and then select **Scan Parameter Group**.
   - On the Action editor **Scan Parameter Groups** tab, click the **Add** button.

   The Scan Parameter Group Wizard appears.
2. From the **Project** list, select the cartridge project in which to include the scan parameter group.
3. In the **Name** field, enter a name for the scan parameter group.
4. (Optional) In the **Folder** field, specify a location for the scan parameter group.

   By default, Design Studio saves the entity to your default workspace. You can browse to a different location using the **Browse** button.

5. Click **Finish**.

   Design Studio creates the scan parameter group and displays the Scan Parameter Group editor.

   If you created the scan parameter group from the Action editor, the scan parameter group is automatically added to the action.

6. Configure the scan parameter group. See "Configuring Network Integrity Scan Parameter Groups" for more information.

Related Topics

About Network Integrity Scan Parameter Groups

About Characteristics for Network Integrity Scan Parameter Groups

Adding Scan Parameter Groups to Network Integrity Actions

Network Integrity Scan Parameter Group Editor

Action Editor Scan Parameter Groups Tab

Configuring Network Integrity Scan Parameter Groups

To configure a scan parameter group:

1. Add characteristics to the scan parameter group.

   See "Adding Characteristics to Network Integrity Scan Parameter Groups" for more information.

2. Define the layout for the scan parameter group.

   See "Defining Network Integrity Scan Parameter Group Layouts" for more information.

3. Define UI settings for scan parameter group characteristics.

   See "Defining UI Settings for Network Integrity Scan Parameter Group Characteristics" for more information.

Related Topics

About Network Integrity Scan Parameter Groups

About Characteristics for Network Integrity Scan Parameter Groups

Creating Network Integrity Scan Parameter Groups

Adding Scan Parameter Groups to Network Integrity Actions

Network Integrity Scan Parameter Group Editor

Action Editor Scan Parameter Groups Tab

About Characteristics for Network Integrity Scan Parameter Groups

Scan parameter groups can be augmented with characteristics to collect additional information about entities. One characteristic can be associated to multiple scan parameter groups.

You add characteristics to scan parameter groups and configure them to appear in the Network Integrity UI as input fields.

Scan parameter group layouts define how characteristics appear as fields in the Network Integrity UI. These settings define how the characteristics appear and behaves in the Network Integrity UI.

Related Topics

Adding Characteristics to Network Integrity Scan Parameter Groups

Defining Network Integrity Scan Parameter Group Layouts

Defining UI Settings for Network Integrity Scan Parameter Group Characteristics

About Network Integrity Scan Parameter Groups

Creating Network Integrity Scan Parameter Groups

Network Integrity Scan Parameter Group Editor

Adding Characteristics to Network Integrity Scan Parameter Groups

Characteristics are data elements that add properties to scan parameter groups. See "About Characteristics for Network Integrity Scan Parameter Groups" for more information.

You can add characteristics to scan parameter groups in the following ways:

- Creating Characteristics from the Network Integrity Scan Parameter Group Editor
- Adding Existing Characteristics to Network Integrity Scan Parameter Groups

Related Topics

About Network Integrity Scan Parameter Groups

Creating Network Integrity Scan Parameter Groups

Network Integrity Scan Parameter Group Editor

Creating Characteristics from the Network Integrity Scan Parameter Group Editor

To create a characteristic from the Scan Parameter Group editor:

1. On the Scan Parameter Group editor **Characteristics** tab, right-click in the data tree area and select **Add Characteristic**.

   The Create and Add Characteristic dialog box appears.

2. Do the following:
   - From the **Primitive Type** list, select the data type for the characteristic.

     Depending on the data type you select, some of the following fields may not appear.
   - In the **Name** field, enter the name for the characteristic.
   - In the **Display Name** field, enter the display name for the characteristic.

     The display name is the name of the input field in the Network Integrity UI.
   - In the **Multiplicity** field, specify whether the characteristic is required.

     Do not select **Range**.

- In the Length area, use the **Maximum** and **Minimum** fields to specify the length for string data types. Select the **Unbounded** check box to not set an explicit maximum value.
- (Optional) In the **Default** field, enter a default value.

3. Click **Finish**.

   Design Studio creates the data element in the data schema as a characteristic and adds the new characteristic to the Scan Parameter Group editor **Characteristics** tab.

Adding Existing Characteristics to Network Integrity Scan Parameter Groups

To add existing characteristics to a scan parameter group:

1. On the Scan Parameter Group editor **Characteristics** tab, right-click in the data tree area and select **Select Characteristic**.

   The Select Characteristic dialog box appears. The dialog box lists characteristics of the current cartridge project and from dependent cartridge projects. See "Managing Project Dependencies" for more information.

2. Select one or more characteristics from the list.

   You can filter the list by element name by typing in the **Element** field and clicking the **Filter** icon, or by entity name by typing in the **Entity Name** field and clicking the **Filter** icon. The entity name is the data schema to which the characteristic belongs.

3. Click **OK**.

   Design Studio adds the characteristics to the Scan Parameter Group editor **Characteristics** tab.

Defining Network Integrity Scan Parameter Group Layouts

You define layouts for scan parameter groups to specify which characteristics appear as fields in the Network Integrity UI. You can lay out how scan parameter group characteristics behave on the Network Integrity Create Scan page and on the Network Integrity Scan Details page. The same characteristic can appear and behave differently on different UI pages.

To define scan parameter group layouts:

1. On the Scan Parameter Group editor **Layouts** tab, in the **Page/Panels** field, select the Network Integrity UI page you want to lay out.

   You can define different attributes for a characteristic when it appears on different pages.

2. In the Panels / Elements area, select the characteristics that you want to appear as fields in the UI:

   a. From the **Available** list, select the characteristics.

   b. Click the **Right Arrow** icon to move the characteristic into the **Selected** list.

   Characteristics left in the **Available** list are still collected but are not displayed in the UI.

3. Organize the order of the characteristics:

   a. From the **Selected** list, select a characteristic.

   b. Click the **Up Arrow** and **Down Arrow** icons.

4. (Optional) To add rows, right-click a characteristic and select **Insert New Row**.

Characteristics appear in the order indicated from left to right in the Network Integrity UI. By inserting a row, the proceeding characteristics restart on the left of the UI on a new row.

5. Save the scan parameter group.

> **Note:**
>
> Clicking the **Reset** button resets the order of the characteristics in the Panels / Elements area and remove any added rows.

Related Topics

About Network Integrity Scan Parameter Groups

Creating Network Integrity Scan Parameter Groups

About Characteristics for Network Integrity Scan Parameter Groups

Network Integrity Scan Parameter Group Editor

Defining UI Settings for Network Integrity Scan Parameter Group Characteristics

You define the UI settings for each characteristic on a scan parameter group to determine how the characteristic appears and behaves on the Network Integrity UI. Repeat the procedure for all scan parameter group characteristics. You can assign settings and values to characteristics that you do not want to have appear in the Network Integrity UI.

To define UI settings for a characteristic:

1. On the Scan Parameter Group editor **Layouts** tab, in the Panels / Elements area, select a characteristic.

   The configurable options for the characteristic appear in the UI Settings area.

2. Configure the following UI settings:

   a. In the **Display Name** field, enter the field name as you want it to appear in the Network Integrity UI.

   b. In the **ToolTip** field, enter a tooltip value for the field, to appear when a user selects the field in the Network Integrity UI.

   All other fields inherit their values from the data schema.

3. Save the scan parameter group.

Related Topics

About Network Integrity Scan Parameter Groups

Creating Network Integrity Scan Parameter Groups

About Characteristics for Network Integrity Scan Parameter Groups

Network Integrity Scan Parameter Group Editor

Network Integrity Scan Parameter Group Editor

Use the Scan Parameter Group editor to configure an action. To access the Scan Parameter Group editor, double-click a scan parameter group entity.

When using the Scan Parameter Group editor to configure an action, see the following topics:

- Scan Parameter Group Editor Characteristics Tab
- Scan Parameter Group Editor Layouts Tab

Scan Parameter Group Editor Characteristics Tab

Use the **Characteristics** tab to create, add, and configure characteristics for scan parameter groups or to remove characteristics from scan parameter groups.

Characteristics that are added from sealed cartridges are read-only.

When working with the **Characteristics** tab, see the following topics:

- About the Characteristics Tab Context Menu for Scan Parameter Groups
- Details Tab
- Usage Tab
- Notes Tab

About the Characteristics Tab Context Menu for Scan Parameter Groups

The **Characteristics** tab context menu contains commands specific to scan parameter group characteristics. To access the context menu, right-click in the left column of the tab. The context menu options that are available depend on the selection in the editor.

Field	Use
Add Characteristic	Create a new characteristic to add to the scan parameter group.
Select Characteristic	Add an existing characteristic to the scan parameter group.
Delete	Delete a characteristic.
Refactoring	Select to access a menu of options for improving names and locations of the characteristics. See "Refactoring Entities and Data Elements" for more information.
Refresh	Refresh the view.

Related Topics

About Network Integrity Scan Parameter Groups

About Characteristics for Network Integrity Scan Parameter Groups

Creating Characteristics from the Network Integrity Scan Parameter Group Editor

Adding Existing Characteristics to Network Integrity Scan Parameter Groups

Network Integrity Scan Parameter Group Editor

Scan Parameter Group Editor Layouts Tab

Use the **Layouts** tab to configure which characteristics appear in the Network Integrity UI and how they behave.

Field	Use
Page/Panels	Select the Network Integrity run-time page to lay out.
Available	Lists the characteristics available to be displayed in the Network Integrity UI for the selected page or panel.
Selected	Lists the characteristics to be displayed in the Network Integrity UI for the selected page or panel.
Left Arrow **Right Arrow** **Up Arrow** **Down Arrow**	Move characteristics back and forth between the **Selected** and **Available** lists and to reorder the characteristics in the **Selected** list.
UI Settings area	Displays the available UI settings for the selected characteristic.
Reset	Revert the layout back to the most recently saved version.

Related Topics

About Network Integrity Scan Parameter Groups

About Characteristics for Network Integrity Scan Parameter Groups

Network Integrity Scan Parameter Group Editor

Defining Network Integrity Scan Parameter Group Layouts

Defining UI Settings for Network Integrity Scan Parameter Group Characteristics