Oracle® Communications Network Integrity

Release Notes

Release 7.3.5

E81519-01

February 2017

This document provides information about Oracle Communications Network Integrity Release 7.3.5.

This document consists of the following sections:

> **Note:** For the Network Integrity documentation set for release 7.3.5, only *Network Integrity Installation Guide* and the release notes changed. Refer to the documentation set for Network Integrity Release 7.3.2 for the remaining documentation.

See *Oracle Communications Design Studio Release Notes* for the release notes for the Design Studio for Network Integrity feature.

See *Network Integrity Licensing Information User Manual* for license and dependency information for Network Integrity components and cartridges.

Software Compatibility

See *Network Integrity Installation Guide* for more information about software requirements and compatibility.

Network Integrity 7.3.5 New Features

Network Integrity 7.3.5 includes the following new features and enhancements:

Device Interface Name Modeling Enhancement

The new device interface name modeling feature allows the extension of existing SNMP based cartridges to transform network entities discovered via SNMP. These network entities are transformed into the format readable names via the command-line interface (CLI). The entities are then used by Activation Systems or Domain Controllers for fulfillment purposes.

See "About Modeling Device Interfaces in MIB-II SNMP Cartridge" for more information.

Platform Upgrade

With Network Integrity 7.3.5, the application platform upgrades Oracle Fusion Middleware Application software and Oracle WebLogic Server Enterprise Edition, and also other software version upgrades which include the following:

- Oracle Fusion Middleware 12.2.1.2.0
- Oracle WebLogic Server 12.2.1.2.0
- Java JDK 8
- Eclipse 4.6 (Neon)

There is no change in the version of the Oracle Database.

See *Network Integrity Installation Guide* for more information on the software version requirements.

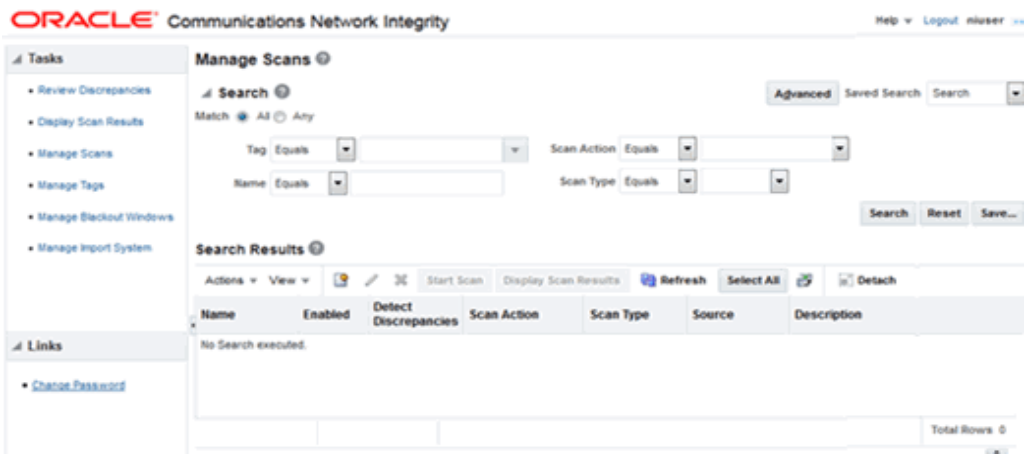
User Interface Screen Layouts

With Network Integrity 7.3.5, the user interface screen layouts are changed. The new user interface provides for simple and uncluttered layouts. The new layout provides the following features:

- Larger text
- Faster loading
- More open space allows for more focus on the data content

The data content is the same as the previous release of Network Integrity with fields and labels unchanged. Figure 1 shows a screenshot of a Manage Scan page as an example of the new user interface layout.

Figure 1 Network Integrity Manage Scans Window



In addition to the new user interface layout, the initial landing page display is enhanced. After a successful login, the initial landing page display has an area to the right that is populated with additional functional links to navigate to various areas of the application.

About Modeling Device Interfaces in MIB-II SNMP Cartridge

This section provides information on modeling of Device Interfaces in the Oracle Communications Network Integrity MIB-II SNMP cartridge. This feature provides enhanced modeling of device interface entities of SNMP based on configuration provided in **Autodiscover.cfg** file.

This enhancement supports a subset of the **Autodiscover.cfg** file properties which are relevant to Network Integrity Device Interface modeling. You can extend the existing remodeling. Table 1 contains the list of supported possible statement types in the **Autodiscover.cfg** file.

See "Customize Device Interface Name Modeling" for more information.

Table 1 Statement Types Supported in the Autodiscover.cfg File

Action	Description
Enterprise	The Enterprise type defines a vendor to the discovery system. The Enterprise type identifies the device as belonging to a particular vendor and defines how IP Service Activator can communicate with the device, and what paradigm IP Service Activator uses when we configure the device. The syntax is as follows: Enterprise:`<enterpriseNumber>;<enterpriseName>;<deviceDriver>;<supported>;<accessType>;<configLevel>;` For example: `Enterprise:9;Cisco;cisco;yes;TACACS;Interface;` See *Oracle Communications IP Service Activator User's Guide* website link below this table for more information on the parameter details.

Table 1 (Cont.) Statement Types Supported in the Autodiscover.cfg File

Action	Description

Main	The syntax for Main is as follows:
	`Main:<enterpriseNumber>;<highIfType>;<lowerIfType>;<regexp>;`
	
	The parameters for Main are similar to Subinterface.
	For this interface, if the enterprise number, interface pair, and optionally the regex match, treat it as a main interface in IP Service Activator.
	For example:
	`Main:9;32;39;îSerial.*;`
	
	This example would map Cisco Frame Relay interfaces on a SONET controller as main interfaces in IP Service Activator if the description matches the regular expression îSerial.*.

Ignore	The syntax for Ignore is as follows:
	`Ignore:<enterpriseNumber>;<highIfType>;<regexp>;`
	
	This means for the device matching the enterprise number, interfaces matching the high interface type number (and optionally matching the regex) are ignored. Discovery of matching interfaces will not be reported to IP Service Activator.
	For example:
	`Ignore:9;94;.*-adsl;`

Rename	The syntax for Rename is as follows:
	`Rename:<enterpriseNumber>;<ifType>;<string-to-match>;<string-to-replace>;`
	
	For this interface number, for this interface type, if you find an interface name that matches this pattern, use the substitute pattern to modify the name that is reported to IP Service Activator.
	For example:
	`Rename:9;134;-atm subif;;`
	
	In this example, ATM subinterfaces are renamed so that the text "-atm subif" is removed from the name (that is, it is replaced with nothing).

Subinterface	Network Integrity supports only the modeling related actions. This action is not supported.
Sublayer	Network Integrity supports only the modeling related actions. This action is not supported.
Vlan and Vlanport	Network Integrity supports only the modeling related actions. This action is not supported.
Ifname and Ifdesc	Network Integrity supports only the modeling related actions. This action is not supported.
Icmp	Network Integrity supports only the modeling related actions. This action is IPSA specific and is not supported.
Persistent	Network Integrity supports only the modeling related actions. This action is IPSA specific and is not supported.

Table 1 (Cont.) Statement Types Supported in the Autodiscover.cfg File

Action	Description
Volatile	Network Integrity supports only the modeling related actions. This action is IPSA specific and is not supported.
AtmVcInterfaceSource	Network Integrity supports only the modeling related actions. This action is IPSA specific and is not supported.
Host and Device	Network Integrity supports only the modeling related actions. This action is IPSA specific and is not supported.
Controller	Network Integrity supports only the modeling related actions. This action is IPSA specific and is not supported.

See *Oracle Communications IP Service Activator User's Guide* for more detailed information on these actions and their parameters at this website:

http://docs.oracle.com/cd/E61089_01/doc.73/e61091/usr_discovery.htm#IPSUS194

Discovering MIB II SNMP Action Changes

As part of this feature implementation, Discover MIB II SNMP action is added with following two new discovery processors:

- Device Interface Name Remodel Initializer Processor
- Device Interface Name Remodeler Processor

Device Interface Name Remodel Initializer Processor

This discovery processor initializes the "remodelerProperties" based on following MBean properties:

```
Discover MIB II SNMP:DI Name Remodel
Initializer:DeviceInterfaceNameModeling:PerformRemodeling

Discover MIB II SNMP:DI Name Remodel
Initializer:DeviceInterfaceNameModeling:LocationOfAutoDiscoverycfg
```

Device Interface Name Remodeler Processor

This discovery processor performs the remodeling of Logical Device hierarchy based on configuration information provided in **AutoDiscover.cfg** file. Table 2 provides the variable information for the processors.

Table 2 Variables for Processors

Processor Name	Variable
Device Interface Name Remodel Initializer	Input: N/A Output: ■ remodelerProperties This contains the location of the **AutoDiscover.cfg** file, Default/Customized DI remodeler implementation class and a flag to set whether or not to perform remodeling.

Table 2 (Cont.) Variables for Processors

Processor Name	Variable
Device Interface Name Remodeler	Input: ▪ deviceInterfaceMap ▪ logicalDevice ▪ remodelerProperties ▪ snmpIfTypeMap ▪ snmpVendorNameMap Output: N/A

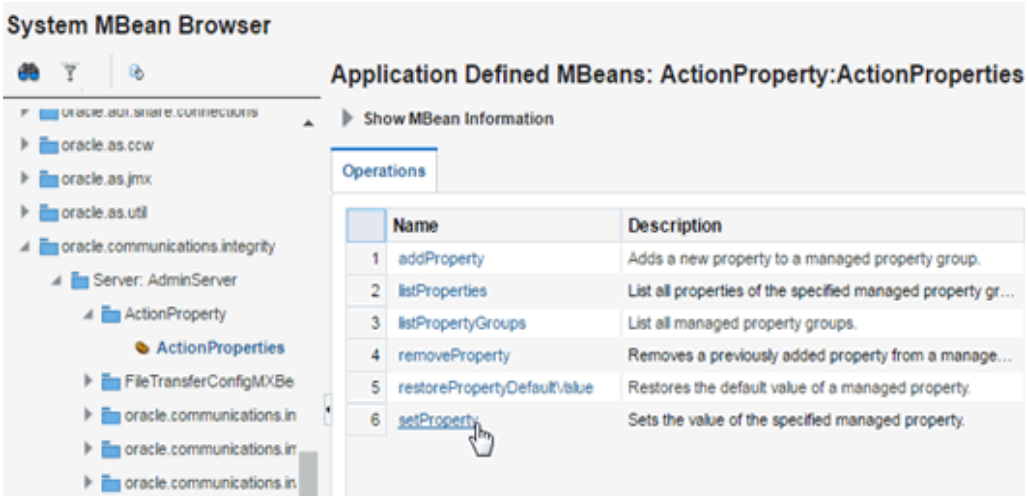
These new processor changes on the "Discover MIB II SNMP" action are also available in all the extended out-of-the-box actions, for example "Discover Generic Cisco SNMP" and "Discover Enhanced Cisco SNMP" to utilize this feature.

Enabling the Device Interface Name Remodeler

By default an SNMP scan does not run with the Device Interface Name Remodeler. To enable Device Interface Name Remodeler, you must set the "PerformRemodeling" property to true and provide the **AutoDiscovery.cfg** file location to "LocationOfAutoDiscoverycfg" for their specific SNMP scan. You do this using "System MBean Browser" in Oracle Weblogic Enterprise Manager.

Figure 2 shows the "System MBean Browser" in Oracle WebLogic Enterprise Manager for the Discover MIB II SNMP action.

Figure 2 Action Properties List in the Oracle Enterprise Manager



Customize Device Interface Name Modeling

To enhance or customize the Device Interface name modeling, perform the following:

- You must create a new Cartridge with a new Discovery Action extending MIB II / Cisco SNMP actions. This is because both the OOB MIB II and the Cisco cartridges are sealed and you do not modify them directly.

- Add all required dependencies cartridges to the new cartridge. For example, Address_Handler and MIB_II_SNMP_Cartridge and select “IPAddressHandler” as an Address Handler for a new discovery action.
- Create a CustomDINameRemodeler class by extending the DefaultDINameRemodeler class in the package:

  `oracle.communications.integrity.mibiisnmpcartridge.discoveryprocessors`

  In the CustomDINameRemodeler class override the performDINameRemodeler() method or any specific function of DefaultDINameRemodeler based on your new requirement.

  The following is an example of a CustomDINameRemodeler class:

```
public class CustomDINameRemodeler extends DefaultDINameRemodeler {
    @Override
    public void performDINameRemodeler(LogicalDevice logicalDevice,
                                       DINameRemodelerProperties properties)
                                       throws ProcessorException {
       // Custom Remodeling goes here.
    }
}
```

- Create a new discovery processor “DI Name Remodeler Customizer” and move it above the “DI Name Remodeler” processor in processor list and select “remodelerProperties” as the input parameter.

  Figure 3 shows the result after you move the “DI Name Remodeler Customizer” above the “DI Name Remodeler” processor. Figure 4 shows the selection of the “remodelerProperties” as the input parameter for the “DI Name Remodeler Customizer”.

Figure 3 Processors Related to this Action

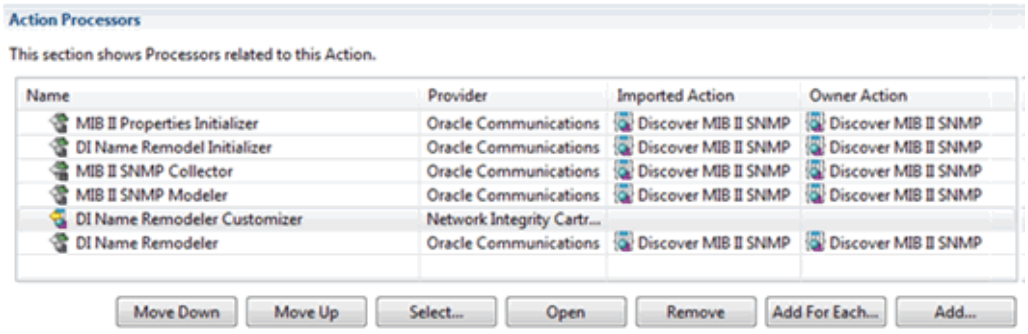
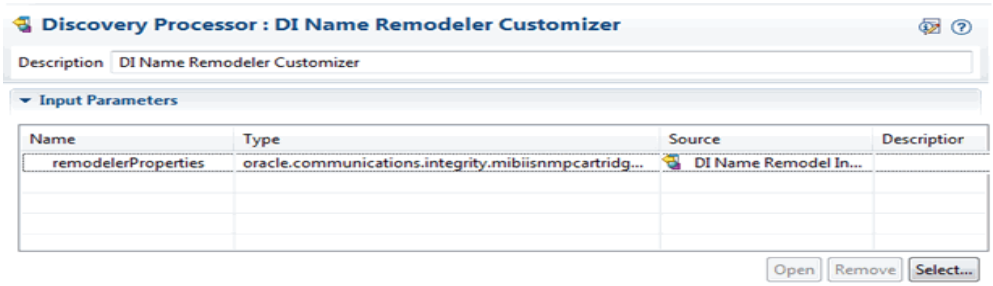


Figure 4 Discovery Processor Properties



- Create an implementation class for a new “DI Name Remodeler Customizer” processor. For example, create the following class:

  `DINameRemodelerCustomizerProcessorImpl`

  You set the instance of CustomDINameRemodeler to “remodelerProperties” using the setNameRemodeler() method.

- Set the implementation class for the “DI Name Remodeler Customizer” with the package and implementation class name.

Example 1 provides code for a sample implementation class DINameRemodelerCustomizerProcessorImpl.

Example 1 Sample Implementation Class Code

```
public class DINameRemodelerCustomizerProcessorImpl implements
             DINameRemodelerCustomizerProcessorInterface {
   @Override
   public void invoke(DiscoveryProcessorContext context,
                      DINameRemodelerCustomizerProcessorRequest request)
                          throws ProcessorException {
     DINameRemodelerProperties remodelerProperties =
           request.getRemodelerProperties();
     if(remodelerProperties.isPerformRemodeling()){
         CustomDINameRemodeler customRemodeler = new CustomDINameRemodeler();
         remodelerProperties.setNameRemodeler(customRemodeler);
      }
   }
}
```

Documentation Updates

There are no new documents provided in this release. The *Network Integrity Installation Guide* has been updated for Release 7.3.5.

Known Problems in Network Integrity 7.3.5

Table 3 lists and describes the known issues in this release.

Table 3 Known Problems for Release 7.3.5

Bug Number	Notes
25406312	**Issue** Detect Discrepancy text is partially visible after up taking Alta skin in the “Manage scans” search result table. **Workaround** Drag the column in the manage scan result table to read the entire label.
25413622	**Issue** After upgrade to 7.3.5 version, multi cartridge re-deployment is not working properly. **Workaround** Re-deploy each cartridge at a time.

Table 3 (Cont.) Known Problems for Release 7.3.5

Bug Number	Notes
13087174	**Issue** Cartridge deployment fails in a clustered environment when the Cartridge Deployment Tool is configured to use SSL and the keystore location is provided. **Workaround** Do the following: 1. In the WebLogic Server Administration Console, enable the non-SSL port for the managed server (for example, networkintegrity01) on which the CMWS application is deployed. 2. Restart all the managed servers in the cluster. 3. Redeploy the CMWS application on networkintegrity01. 4. Deploy the cartridges using the Cartridge Deployment Tool. 5. After you have deployed the cartridges, disable the non-SSL port for networkintegrity01 in the WebLogic Server Administration Console.
11676449	**Issue** When a scan action is configured to use the file transfer processor when the Source File Management is set to Rename or Delete, the scan status of a running scan may change from Running to Completed, even though other processes are still running. This issue occurs when Network Integrity incorrectly changes the scan status to Completed after the processor has finished its processing and modeling, instead of changing the status to Completed after the intended file has been renamed and deleted. You may observe this issue in situations where the remote file operation is required to delete or rename a large number of files or when the network connection is slow. Failures related to the remote file rename or delete operations are not reported by the Network Integrity user interface. **Workaround** None.
11071255	**Issue** Manage Scans page is not displayed properly when you log in to Network Integrity again after the session times out in Internet Explorer. **Workaround** Refresh your browser if you are using Internet Explorer, or use Firefox.
10065856	**Issue** If the **Correct in UIM** operation fails due to a session time out, no error message is displayed. **Workaround** None.
19940521	**Issue** If you create new roles or policies using Oracle Enterprise Manager, the changes are not propagated to the managed servers unless the managed servers are restarted. **Workaround** After you create the roles and policies, you must restart the managed servers. Doing so enables the managed servers to receive updates related to the local LDAP server from the Administration server, and subsequently the new policies and roles are propagated to the managed servers.

Network Integrity 7.3.2 Release Notes

This section includes the Release Notes content for Network Integrity 7.3.2.

New Features

The following sections provide information on the new features of Network Integrity 7.3.2.

Support for Single Sign-On Authentication

Network Integrity now includes support for single sign-on (SSO) authentication. Network Integrity implements the SSO authentication solution using Oracle Access Manager, which enables you to seamlessly access multiple applications without being prompted to authenticate for each application separately. The main advantage of SSO is that you are authenticated only once, which is when you log in to the first application; you are not required to authenticate again when you subsequently access different applications within the same web browser session.

Network Integrity also supports single logout (SLO). If you access multiple applications using SSO within the same web browser session, and then if you log out of any one of the applications, you are logged out of all the applications.

See "Setting Up Network Integrity for Single Sign-On Authentication" in *Network Integrity Installation Guide* for more information.

Support for CPU Utilization-enabled Discovery

The Cisco Router and Switch SNMP cartridge and Cisco Router and Switch UIM Integration cartridge have been enhanced to support CPU utilization-enabled discovery. These cartridges now enable you to discover devices based on their CPU utilization by setting a threshold value (in percentage) in the discovery scan.

See *Network Integrity Cisco Router and Switch SNMP Cartridge Guide* and *Network Integrity Cisco Router and Switch UIM Integration Cartridge Guide* for more information.

If the CPU utilization value of a device exceeds the user-specified threshold value, the scan for that device is skipped. The discovery scans are run only for those devices whose CPU utilization value is less than the user-specified threshold value.

To support the discovery of devices based on CPU utilization, a new scan parameter group, **CPU Utilization Parameters**, has been added in the NetworkIntegritySDK cartridge. This scan parameter group adds the **CPU Utilization %** field to the Network Integrity UI Scan Configuration screen. The **CPU Utilization %** field accepts a value between 1 to 99.

See *Network Integrity Developer's Guide* for more information.

New CLI Cartridge Introduced

The Command Line Interface (CLI) cartridge allows you to build deployable cartridges that connect to devices and retrieve information using CLI commands over Telnet or Secure Shell (SSH) protocol.

The CLI cartridge provides the following key features:

- Telnet protocol and SSH communication with CLI devices
- Record and playback of CLI communication

The CLI cartridge is an abstract cartridge, meaning that Design Studio is used to configure and assemble the run time cartridge against devices before deploying it into Network Integrity.

The CLI cartridge ZIP file contains a reference implementation cartridge for discovering Cisco devices running the IOS XR operating system and retrieves information about virtual private LAN services (VPLSs) on the Cisco IOS XR devices.

See *Network Integrity CLI Cartridge Guide* for more information.

Extended Oracle Communications Information Model Support

Network Integrity now enables you to model packet connectivity entities in Design Studio to enhance the integration with Oracle Communications Unified Inventory Management (UIM).

> **Note:** Network Integrity 7.3.2 supports Oracle Communications Information Model 7.3.0. For specific technical details about the Oracle Communications Information Model and the Network Integrity information model, see *Oracle Communications Information Model Reference* and *Network Integrity Information Model Reference*.

To support packet connectivity, Network Integrity adds support to additional Oracle Communications Information Model (OCIM) entities in the following entity categories:

- Connectivity Entities
- Logical Device Entities
- Signal Structure Entities
- Capacity Consumption Pattern Entities

Connectivity Entities You can now define Connectivity specifications in Design Studio and classify entities based on those specifications in Network Integrity. In addition, when you define a Connectivity specification, you can designate its connectivity type.

Network Integrity now supports three types of Connectivity entities, each of which is designed for use with particular technologies. When you define a Connectivity specification, you specify one of the following connectivity types:

- **Multiplexed:** Multiplexed (or Channelized) connectivities support technologies such as E-Carrier, T-Carrier, J-Carrier, SDH, and SONET, and WDM.
- **Packet:** Packet connectivities support technologies such as Ethernet, DSL, Frame Relay, ATM, and MPLS. See "Logical Device Entities" for additional information.

- **Service:** Service connectivities deliver services to end customers. Service connectivity consumes other types of connectivity and resources, but cannot be consumed itself. Service connectivities are used as part of service arrangements involving packet technology, such as Carrier Ethernet.

Connectivity entities take advantage of pre-defined rate codes and technologies that are provided by Oracle in the ora_uim_basemeasurements and ora_uim_basetechnologies cartridges.

See the Design Studio Modeling Inventory Help for more information.

Logical Device Entities Network Integrity now includes Logical Device entities to support networking technologies that are based on packet connectivity, including Ethernet, Frame Relay, Asynchronous Transfer Mode (ATM), and Multiprotocol Label Switching (MPLS).

Network Integrity now includes flow interfaces and flow identifiers that are used in packet scenarios. See "Flow Interfaces" and "Flow Identifiers" for more information.

Flow Interfaces

To support packet connectivity, Network Integrity now includes Flow Interface entities.

Flow interfaces partition media interfaces (device interfaces at the top of their hierarchies) into virtual channels based on bit rate. Flow interfaces are similar to the sub-device interfaces used to terminate channelized connectivity, but are used to terminate packet connectivity only. They have configurations that capture their attributes.

When you define a Flow Interface specification, you specify one of four termination types:

- **Access:** Indicates that the purpose of an interface is to terminate connectivity that provides access to a service provider network, such as Ethernet UNI connectivity.
- **Internetwork:** Indicates that the purpose of an interface is to terminate connectivity that interconnects two service provider networks, such as Ethernet E-NNI connectivity.
- **Trunk:** Indicates that the purpose of an interface is to terminate connectivity that connects equipment and devices in the same network, such as Ethernet I-NNI connectivity.
- **Unknown:** Indicates that the purpose of the interface is unknown. Used to support scenarios not covered by the Access, Internetwork, and Trunk termination types.

Flow Identifiers

To support packet connectivity, Network Integrity now includes Flow Identifier entities. Flow identifiers are defined by specifications in Design Studio. Flow identifiers are used to represent the ways that various packet network technologies identify and distinguish network traffic. Flow Identifier specifications support technologies such as Ethernet, Frame Relay, ATM, and MPLS.

See the Design Studio Modeling Inventory Help for more information.

Signal Structure Entities You can now define the following entity in Design Studio:

- Pipe Signal Termination Point

Pipe Signal Termination Point

You can now define Pipe Signal Termination Point specifications in Design Studio. You can associate Pipe Signal Termination Point specifications to either Connectivity specifications or Pipe specifications to define channelized facilities. You use Pipe Signal Termination Point specifications to define signal structures. A signal structure defines a multiplexing hierarchy where data streams are separated into multiple lower data communication links.

See the Design Studio Modeling Inventory Help for more information.

Capacity Consumption Pattern Entities You can now define the following entities in Design Studio:

- Inventory Unit Of Measure
- Measurement Type

Inventory Unit Of Measure

Units of measure define the units used to measure a type of capacity. A unit of measure is a quantity or increment by which something is divided, counted, or described. For example, Kbps (kilobits per second) is a unit that measures a bit rate.

Measurement Type

A measurement type classifies related groups of units of measure. For example, a bit rate measurement type classifies units of measure, such as bits per second (bps), kilobits per second (kbps), and so on. Other possible measurement types include weight and amperage.

See the Design Studio Modeling Inventory Help for more information.

Documentation Updates

This section provides information about the Network Integrity documentation set.

Network Integrity CLI Cartridge Guide Introduced

The Network Integrity 7.3.2 documentation set includes a new guide entitled *Network Integrity CLI Cartridge Guide*. This guide explains the functionality and design of the Oracle Communications Network Integrity CLI cartridge.

Known Problems in Release 7.3.2

Table 4 lists the known problems in the 7.3.2 release.

Table 4 Known Problems

Bug Number	Notes
13087174	**Issue** Cartridge deployment fails in a clustered environment when the Cartridge Deployment Tool is configured to use SSL and the keystore location is provided. **Workaround** Do the following: 1. In the WebLogic Server Administration Console, enable the non-SSL port for the managed server (for example, networkintegrity01) on which the CMWS application is deployed. 2. Restart all the managed servers in the cluster. 3. Redeploy the CMWS application on networkintegrity01. 4. Deploy the cartridges using the Cartridge Deployment Tool. 5. After you have deployed the cartridges, disable the non-SSL port for networkintegrity01 in the WebLogic Server Administration Console.
11676449	**Issue** When a scan action is configured to use the file transfer processor when the Source File Management is set to Rename or Delete, the scan status of a running scan may change from Running to Completed, even though other processes are still running. This issue occurs when Network Integrity incorrectly changes the scan status to Completed after the processor has finished its processing and modeling, instead of changing the status to Completed after the intended file has been renamed and deleted. You may observe this issue in situations where the remote file operation is required to delete or rename a large number of files or when the network connection is slow. Failures related to the remote file rename or delete operations are not reported by the Network Integrity user interface. **Workaround** None.
11071255	**Issue** Manage Scans page is not displayed properly when you log in to Network Integrity again after the session times out in Internet Explorer. **Workaround** Refresh your browser if you are using Internet Explorer, or use Firefox.
10065856	**Issue** If the **Correct in UIM** operation fails due to a session time out, no error message is displayed. **Workaround** None.

Table 4 (Cont.) Known Problems

Bug Number	Notes
19940521	**Issue** If you create new roles or policies using Oracle Enterprise Manager, the changes are not propagated to the managed servers unless the managed servers are restarted. **Workaround** After you create the roles and policies, you must restart the managed servers. Doing so enables the managed servers to receive updates related to the local LDAP server from the Administration server, and subsequently the new policies and roles are propagated to the managed servers.

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.

Oracle Communications Network Integrity Release Notes, Release 7.3.5
E81519-01

Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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