NORTEL

Nortel Identity Engines Ignition Server

Release Notes

Release: 6.0.0
Document Revision: 01.01

www.nortel.com

NN47280-400

Nortel Identity Engines Ignition Server
Release: 6.0.0
Publication: NN47280-400
Document status: Standard
Document release date: July 2009

Contents

Contents

Customer service

Visit the Nortel Web site to access the complete range of services and support that Nortel provides. Go to www.nortel.com or go to one of the pages listed in te following sections.

Updated versions of documentation

You can download and print the latest versions of Nortel Identity Engines Ignition Server documents directly from the Internet at www.nortel.com/documentation.

Getting Help

If you purchased a service contract for your Nortel product from a distributor or authorised reseller, contact the technical support staff for that distributor or reseller for assistance

If you purchased a Nortel service program, you can get help by contacting one of the Nortel Technical Solutions Centers found at www.nortel.com/callus or visit our Technical Support site at www.nortel.com/support.

Express Routing Codes

An express routing code (ERC) is available for many Nortel products and services.

When you use an ERC, your call is routed to a technical support person who specializes in supporting that particular product or service. To locate an ERC for a product or service, go to www.nortel.com/erc.

Additional Information

Use the information in the following table to access other areas of the Nortel Web site.

For information about	Contact
Contact us	www.nortel.com/contactus
Documentation feedback	www.nortel.com/documentfeedback
products (marketing)	www.nortel.com/products
Partner Information Center (PIC)	www.nortel.com/pic
Register	www.nortel.com/register
Search	www.nortel.com/search
Services	www.nortel.com/services
Training	www.nortel.com/training

Nortel Identity Engines Ignition Server Release Notes

Nortel Identity Engines Ignition Server version 6.0.0 is the inaugural Nortel release. This product release consists of the Nortel Identity Engines Ignition Server firmware and Nortel Identity Engines Ignition Server Ignition Dashboard. Left unchanged is Nortel Identity Engines Ignition Server Guest Manager.

Contents

New in this release

The following sections details what's new in *Nortel Identity Engines Ignition Server Release Notes* NN47280-400.

- Features

- Other changes

Features

Ignition Server: Migration from hardware appliance to virtual appliance

Nortel Identity Engines Ignition Server version 6.0.0 adds the virtual appliance feature replacing the need to install and configure Ignition Server using hardware interfaces and is the only implementation supported by Nortel.

For more information about installing and configuring Ignition Server see the *Nortel Identity Engines Ignition Server Getting Started Guide Release 6.0.0.*

Ignition Server 6.0.0 supports backup and restore from Ignition Server 5.0. Customers currently running Ignition Server 4.2 are given an unsupported version of Ignition Server 5.0.0 for backup and restore functionality only. Customers will only be given Ignition 5.0 if they have purchased Ignition 6.0 from Nortel and have a valid maintenance contract.

Upon restoring the configuration, the user must enter a valid Virtual Appliance 6.0.0 license in order to use the functionality. This can be done by entering the license text onto Dashboard 6.0.0 -> Configuration -> site -> license.

Configuration Integrity

Configuration integrity prevents a customer from breaking the currently running access policies by deleting or renaming referred objects. For example, in a policy like "If user's group membership contains [sales] then Allow with sales-vlan", the customer can safely rename the sales group or the sales-vlan without fear of breaking their configuration; deleting the sales group or the sales-vlan will be prevented unless they update the policy first.

Custom LDAP

Custom LDAP user search filters allow the customer to specify the precise LDAP filter that Ignition will use to locate users in LDAP. This is particularly useful when the customer is using a non-standard LDAP objectclass for users, or when the customer would like to further filter the user population by another LDAP attribute.

Arbitrary RADIUS Provisioning

Arbitrary RADIUS provisioning attributes allow the customer to duplicate RADIUS attributes for the purposes of provisioning users or devices on the network. Also, the customer can reorder these attributes. Although there are many potential applications, this feature is important for sending IP or other ACLs to a sophisticated authenticator such as a VPN gateway, firewall, or portal.

Migration Logs

Migration logs will point the customer to automated fixes made to their policies during the migration process, and will also provide troubleshooting capability for migration problems.

NTLMv2 Support

Adding NTLMv2 support for MSCHAPv2 refers to providing compatiblity with Windows Server 2008 and other environments where NTLMv1 is disabled except for authentication applications such as Microsoft NPS.

Other changes

- Date & Time option to configure either NTP or manual has been removed since the appliance runs in the virtual environment. The appliance obtains the data & time from host. This info is displayed in the Data & Time tab.

- DHCP checkbox from port edit has been removed from port edit tab under node configuration, therefore the administrator/user must configure IP address manually.

- Removed Edit button for System Static Routing in Node configuration to fix an issue with edit option which is not correct.

Installing Ignition Server

To quickly install Ignition Server, follow the instructions in the *Nortel Identity Engines Ignition Server Getting Started Guide*. To connect Ignition to your switches, access points, and user data stores, see the *Nortel Identity Engines Ignition Server Configuration Guide*. To plan and carry out your enterprise installation of Ignition, consult Appendices A and B of the *Nortel Identity Engines Ignition Server Administrator's Guide*. To upgrade, see the section immediately below this.

Attention: The Dashboard installer will install a private copy of Sun's Java Runtime Environment (JRE) 1.6.0_u13. This installation will NOT be visible in the Add/Remove program control panel. When the Dashboard application is removed the private copy of JRE will also be removed from the users system.

Migrating from hardware appliance to Virtual Appliance

These instructions explain how to upgrade to version 6.0.0. The upgrade utility supports upgrades from 5.0.x. If your current firmware version is not listed here, contact your Nortel support representative for help.

⚠️ *Important!* Ignition server version 6.0.0 requires a *base license* in order to run. If you are upgrading from a pre-6.0 version, make sure you have your license(s) ready in the form of an e-mail or text file. If you do not have the required licenses, contact customer support now to get them (see "Customer service" on page 5). *Do not upgrade if you do not have your licenses!*

Upgrade Procedure:

1   Get the 6.0.0 Ignition Server software OVF folder and the 6.0.0 Ignition dashboard installer from Ignition Server software download site http://support.nortel.com (see page 5 for more details on customer support)

2   Back up your appliance data. You must do this to ensure that, if the need arises, you can reuse the backup file to restore the data onto the hardware appliance that you are currently using. Do the following:

•   *In Ignition Server 5.x:* Run Ignition Dashboard and click on your **Site** in the **Configuration** tree.

•   Select the command **Actions: Backup Data** to make a backup copy of the appliance's data and configuration. Be sure to make a note of the password for the backup file. See "Ignition Server Backup and Restore Procedures" in the *Nortel Identity Engines Ignition Server Administrator's Guide* for details.

3   If you have *log export* turned on for the Access and/or Audit channels, you must turn it off before you upgrade. You can turn it back on after the upgrade. Use your pre-upgrade Dashboard to turn off log export for these two channels. To do this:

•   *In Ignition Server 5.x:* In Dashboard, click on your **Site** in the **Configuration** tree. Click the **Logging** tab. Click **Export Logs**. Click **Edit**.

•   In the **Access** row, set the **Export Periodically** cell to *Never*.

- In the **Audit** row, set the **Export Periodically** cell to *Never*.
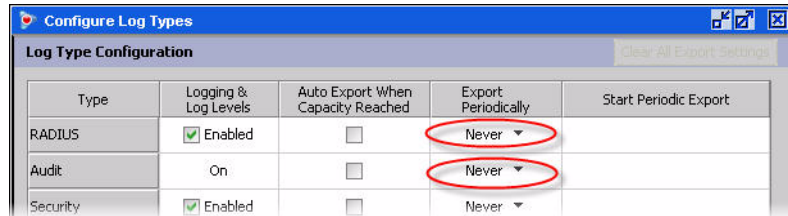
- Click **Save**.

4 Bring up virtual appliance with release 6.0.0 in VMWare ESX/ESXi platform by following instructions listed in the Nortel Identity Engines Ignition Server Getting Started Guide. Upgrade firmware option to release version 6.0 is not applicable in the hardware appliance that was purchased from Identity Engines. You also need new dashboard version 6.0 to be able to connect to virtual appliance.

5 Launch the *Ignition Dashboard installer* (the file you downloaded in) to install the new version of Dashboard.

A dialog box appears, offering you the option to uninstall the earlier version of Dashboard. Click **Yes** to have the installer remove the old version.
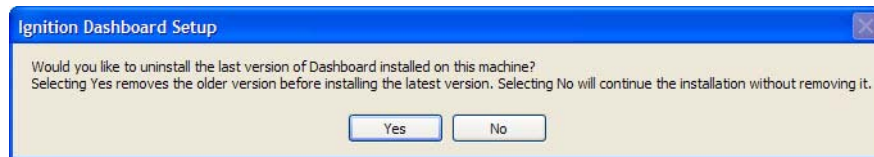
6 Follow the screens of the installer to install Dashboard. For additional details, see "Installing Ignition Dashboard" in the *Nortel Identity Engines Ignition Server Administrator's Guide.*

Attention: The Dashboard installer will install a private copy of Sun's Java Runtime Environment (JRE) 1.6.0_u13. This installation will NOT be visible in the Add/Remove program control panel. When the Dashboard application is removed the private copy of JRE will also be removed from the users system.

7 Run Ignition Dashboard version 6.0.0 to connect to the virtual appliance. Click the name or IP address of your **Node** in the **Configuration** tree, and click the **Status** tab. Under **Current Configuration**, check the **Software Version** to verify that the appliance is running the new firmware.

8 If you are upgrading from Ignition Server version 5.x, install your Ignition Server licenses:

- Get your Ignition Server licenses from Nortel customer support. *Note that you must have the FEATURE_BASE license in order to use Ignition's basic functionality.* Each license comes in the form of an e-mail or text file. The actual license starts with "BEGIN IGNITION LICENSE CERTIFICATE" and ends with "END IGNITION LICENSE CERTIFICATE".

- Install each Ignition Server license: In Dashboard's **Configuration** view, click your **Site** in the **Configuration** Hierarchy, click the **Licenses** tab, and click **Install**.

- Find the license and open it in your e-mail tool or text editor. Highlight and copy the text of your license. Copy the whole license including "BEGIN IGNITION LICENSE CERTIFICATE" and "END IGNITION LICENSE CERTIFICATE".

- Return to the License Installation window of Dashboard and click **Paste** to paste the license text there.

- Click **OK**.

9 Restore the saved configuration from the backup file that was obtained in Step 2 from Dashboard configuration > site > restore data. Detailed instructions are listed in *Nortel Identity Engines Ignition Server Administration Guide* section Appendix C.

10 If you turned off log exporting during the upgrade, re-enable it now. To do this, click your **Site** in Dashboard's **Configuration** tree. Click the **Logging** tab. Click **Export Logs**. Click **Edit**.

11 In the Configure Automated Log Export window, in the **Access** and/or **Audit** rows, set the **Export Periodically** setting to your desired frequency. Click **OK**.

12 Back up your appliance data again. This creates a version 6.0.0-compatible backup file that you can apply in the unlikely event that your appliance data becomes lost. Do the following:

- In Ignition Dashboard, click your **Site** in the **Configuration** tree.

- Select the command **Actions: Backup Data** to make a backup copy of the appliance's data and configuration.

Issues fixed in this release

ID	Summary
5130	FIXED: After installing TACACS+ and Guest Manager license, you must restart Dashboard
5303	FIXED: Editing an in-use Guest Manager provisioning group causes errors
5327	FIXED: Add support for NTLMv2 with MSCHAPv2
5238	FIXED: After reboot, default route missing from kernel routing tables
5598	FIXED: Setting node name does not stick (HA)
5895	FIXED: IGM SOAP call fails after 5.0.4 upgrade
5925	FIXED: RADIUS realm matching should be case-blind

Known limitations in this release

This section lists known bugs and a workaround if one is available.

Summary of Known Issues

ID	Summary	Page
4407	Date comparison in policy does not use time zone offset	page 12
3734	Creating an HA pair may fail, leaving secondary node in synching state	page 13
3616	Filtering the log view on a busy system may result in time-outs	page 13
3093	In HA pair, Monitor view displays data from VIP-master only	page 13
2168	Misleading "Duplicate IP Address" message in System Log	page 14
2058	Administrative actions in Dashboard may fail when Ignition Server is under heavy load	page 14
1771	Windows Update may uninstall Ignition Dashboard	page 14
1209	Delay in restoring broken AD connection	page 14
412	Renaming or deleting a virtual attribute or other Ignition Server data item may result in policy errors	page 15
Q02039685	TA:Outboud attributes in IPV4 type are displayed reversed in monitor log	page 15
Q02036078	RADIUS Session Times Out when authenticating Microsoft PEAP Supplicant.	page 16
Q02033497	System exception error message may appear in the appliance console.	page 16
Q02022316	Automatic Download of OPSWAT DLL files fails.	page 16
Q02036770	Both HA nodes become secondary	page 17
Q02024304	Could not delete Authentication Server in the Directory Services	page 17

Date comparison in policy does not use time zone offset

Bug Id 4407

Problem Description The Ignition Server may incorrectly allow or deny an authorization because the Ignition Server uses GMT/UTC time zone even though the rule (as configured in Dashboard) is set to use a different time zone, such as

America/Los Angeles. This error occurs because, when your authorization rule enforces time restrictions using the *Date* inbound attribute type, Ignition Server ignores the time zone set in the rule. This error occurs only when you use an attribute type of *Date*. In fact, there are two problems: (1) Ignition Server ignores the time zone setting when you use the *Date* attribute type with any comparator; and (2) the *between* comparison operator does not allow you to specify a time zone in your rule.

Workaround Do not use the *Date* attribute type in your policies. Instead, use the *Date and Time* attribute type. When using *Date and Time*, Ignition Server applies time zones correctly.

Creating an HA pair may fail, leaving secondary node in synching state

Bug Id 3734

Problem Description Identity Engines quality assurance has observed rare instances in which, during the creation of an HA pair, the secondary node becomes inoperable. When this occurs, Dashboard shows the secondary node in a synching state for a long period of time (typically more than four minutes).

Workaround If your secondary node becomes inoperable, do the following:
- Break the HA pair from the command line on both boxes as explained in the section, "Breaking an HA Pair Using the CLI," in the *Nortel Identity Engines Ignition Server Administrator's Guide*.
- Re-create the HA pair as explained in the section, "Run the HA Wizard," in the *Administrator's Guide*. **Important:** When re-creating the HA pair, use the server that was previously **Database Primary** as the new primary node. That is, run the HA Wizard from the machine you plan to use as the primary node.

Filtering the log view on a busy system may result in time-outs

Bug Id 3616

Problem Description In Dashboard's Log Viewer window, applying a filter while the Ignition Server is busy may result in a time-out. If a time-out occurs, the filter is not applied.

Workaround Apply a filter that will return a smaller set of results. For example, if your attempt to retrieve the last eight hours' worth of records failed, try loading four hours' worth of records, instead.

In HA pair, Monitor view displays data from VIP-master only

Bug Id 3093

Problem Description In an installation composed of an HA pair of Ignition Servers, the Monitor panel in Ignition Dashboard displays the latest records *from only the Server that is currently the VIP-master for the RADIUS port*. This applies only to installations where a VIP has been activated on the Ignition Server and the RADIUS

service has been placed on the VIP. This situation could cause confusion for an administrator in the time immediately after a failover, when the most recent user authentication records (logged on the Server that is now no longer VIP-master) disappear from view, replaced with the most recent records from the Server that is newly appointed VIP-master. These records may be older records.

Misleading "Duplicate IP Address" message in System Log

Bug Id 2168

Problem Description The System Log of the Ignition Server may contain misleading "duplicate IP address" error messages. These messages are written to the System Log during initiation of an HA pair. You may safely ignore these messages. They do not indicate an error; they are a normal part of the VIP initiation. The messages look like:

Error. duplicate IP address 173.168.19.12 sent from link address 00:18:22:bb:2c:32

Administrative actions in Dashboard may fail when Ignition Server is under heavy load

Bug Id 2058

Problem Description When the Ignition Server is serving a heavy load of administrative requests, it may fail to respond to actions that the administrator attempts to perform in Dashboard.

Workaround Retry the failed action in Dashboard.

Windows Update may uninstall Ignition Dashboard

Bug Id: 1771

Problem Description: Performing a Windows Update may cause Ignition Dashboard to become disabled. When this occurs, the user sees an error dialog when he tries to launch Dashboard: "Could not find the main class. Program will exit."

Workaround: Reinstall Ignition Dashboard.

Delay in restoring broken AD connection

Bug ID 1209

Problem Description If the network connection between Ignition Server and the Active Directory is interrupted, there may be a delay before Ignition Server reconnects to Active Directory and resumes servicing RADIUS requests. If the Ignition-AD connection is a non-SSL connection, re-connection is possible in 1-2 minutes. For an SSL connection, re-connection may take up to ten minutes.

Renaming or deleting a virtual attribute or other Ignition Server data item may result in policy errors

Bug Id 412

Problem Description A previously working authorization policy may fail if you rename or delete a virtual group, virtual attribute, or other piece of Ignition Server data used in the policy. Policies refer to virtual attributes, groups, and other objects by name; if you change a name or delete an item, the reference is broken. An authorization policy may use data associated with the following elements:

- authenticator
- authenticator bundle
- authenticator hierarchy (container)
- service category
- directory service in a directory set
- virtual group
- virtual attribute

Workaround If possible, do not rename or delete any data item of the types listed above if you think those items might have been used in your authorization policies. If you have renamed or cannot avoid renaming an item, then use the following workaround to fix broken authorization policies if you have renamed or deleted one of the elements listed above.

1. Open the Policy Management Window.
2. Select a service category from the drop down **Service Category** list.
3. Highlight a rule in the displayed list of Rule Names, and:
   - × **For virtual attribute errors:** Check each policy for the string, "Invalid reference". Where you find this string, edit the policy so that it uses the updated name.
   - × **For errors related to other data elements:** Edit the rule to use a replacement data item.

   Repeat this for each rule in the service category.
4. Repeat Step 3 for each service category listed in the drop down list called **Service Category**.

TA:Outboud attributes in IPV4 type are displayed reversed in monitor log

Bug Id Q02039685

Problem Description The outbound attributes in IPv4 address is displayed in reverse order.

Workaround there is no work around; it is a display issue.

RADIUS Session Times Out when authenticating Microsoft PEAP Supplicant.

Bug Id Q02036078

Problem Description When authenticating Microsoft PEAP Supplicant the request timeout for unauthenticated request.

Workaround With Microsoft PEAP supplicant DO NOT enable "Enable Unauthenticated RADIUS Authorization parameter in the policy" from Dashboard->site->Access Policies ->RADIUS policy the authorization policy tab".

System exception error message may appear in the appliance console.

Bug Id Q02033497

Problem Description If you do not wait for Dashboard to connect to the appliance to confirm system is ready and then login from CLI, the following error message may appear from in the appliance console "system exception, ID 'IDL:omg.org/CORBA/TRANSIENT:1.0'OMG minor code (2), described as 'No usable profile in IOR.',completed = NO"

Workaround Wait for Dashboard to connect to the appliance to confirm system is ready, at that time you can login from CLI.

Automatic Download of OPSWAT DLL files fails.

Bug Id Q02022316

Problem Description Automatic Download of Posture Metadata Configuration fails as is evident by a similar entry in the system logs viewable by the Dashboard: Posture Metadata Update: One or more Opswat file downloads failed (visible in the system logs) The metadata refresh failed because the system was unable to retrieve the data (GUI popup message)

Workaround This is a known issue for the 6.0 release of Nortel Ignition Server. Automatic scheduled downloads of posture metadata will be available in a future release but for this release these metadata files must be manually downloaded. Nortel will publish these 'Opswat' metadata files on a monthly basis and the operator can manually download these updates and load them onto the Ignition Server. The files can be downloaded from Nortel by visiting www.nortel.com/identity and selecting the Software Downloads link. To manually load the updates within Configuration mode in the Dashboard, right-click on the Site root, select Posture Metadata Configuration, select Manual upload and then browse to the location where the metadata files were downloaded.

Both HA nodes become secondary

Bug Id Q02036770

Problem Description Nortel quality assurance has observed one instance in which the RADIUS request packets are not working when both nodes in the HA pair becomes secondary. The node DB role is displayed in configuration->site->High Availability.

Workaround 1) Break the HA pair from the dashboard configuration->site->Break HA Link (select by right clicking site) and then re-create the HA pari as explained in the section, "Run the HA Wizard" in the Administrator's Guide.

If the above work around fails to rectify the problem then a reboot of primary node in the HA pair is needed.

Could not delete Authentication Server in the Directory Services

Bug Id Q02024304

Problem Description This issue is found in Nortel internal QA lab. Ignition server experiences a timeout when trying to delete Authentication server which has more than 4000 groups in the directory services. With 4000 groups the deletion operation succeeds even though the dashboard shows timeout. Between 4500-5000 the delete operation fails.

Workaround Break HA and perform the operation and recreate HA.

Nortel Identity Engines Ignition Server
Release Notes

NORTEL