



USER GUIDE

AUG-10051-21

RNI System Administrator



Revision history

Rev No.	Date	Description
01	05-OCT-16	Initial release.
02	23-MAR-17	Updated for version 4.1.3.
03	31-JUL-17 / 06-NOV-17	Updated for version 4.2 / 4.2.1.
04 / 05	28-FEB-18 / 08-JUN-18	Updated for version 4.3 / 4.3.1.
06 / 07	28-AUG-18 / 26-OCT-18	Updated for version 4.4 / 4.4.1.
08 / 09	25-FEB-19 / 29-APR-19	Updated for version 4.5 / 4.5.1.
10 / 11	27-AUG-19 / 29-OCT-19	Updated for version 4.6.0 / 4.6.1.
12 / 13	26-FEB-20 / 23-APR-20	Updated for version 4.7.0 / 4.7.1.
14	28-AUG-20	Updated for version 4.8.
15	20-NOV-20	Additional updates for version 4.8 (4.8.1).
16	10-JUN-21	Updated for version 4.9.
17	25-OCT-21	Updated for version 4.10.
18	06-JUN-22	Updated for version 4.11.
19	05-DEC-22	Updated for version 4.12. Added information about password management for service accounts. Minor updates to User roles and System permissions sections.
20	16-JUN-23	Updated for version 4.13. Updates to customer information, configuration parameters, user roles, and system permissions.
21	15-NOV-23	Updated for version 4.14. Added technical information about how the email for RNI password expiration notification works and the template used for the email. Also noted that admins can now search for settings in the RNI's configuration and that columns related to password expiration were added to the Users page. Other misc. updates.

Copyright

This document, in whole or in part, ("Document") includes confidential and proprietary information belonging to Sensus USA Inc. and/or one of its subsidiaries or affiliates. Unauthorized use, reproduction, disclosure, distribution, or dissemination of this Document is strictly prohibited. No party may use, reproduce, disclose, distribute, or disseminate this Document for any purpose without express written authorization from Sensus USA Inc. Any use, reproduction, disclosure, distribution, or dissemination of this Document does not transfer title to, license, or grant any patent, copyright, trademark, or other intellectual property rights. This Document, and any copies or derivatives thereof, must be returned immediately on demand. This Document is subject to any applicable non-disclosure agreement(s). Information in this Document is subject to change without notice and does not represent a commitment on the part of Sensus.

© 2023, Sensus USA, Inc., a subsidiary of Xylem, Inc. All Rights Reserved.

Sensus, the Sensus logo, FlexNet® and associated logos are trademarks of Sensus and its subsidiaries and affiliates.

Sensus USA
637 Davis Drive
Morrisville, NC 27560

1-800-638-3748
www.sensus.com

Document: RNI System Administrator User Guide
Document Number: AUG-10051-21

Contents

1 System administration overview.....	6
2 Access the System Administration page.....	7
3 RNI user password settings.....	9
4 Multi-factor authentication.....	13
Tenant (customer) level multi-factor authentication.....	14
Active Directory and multi-factor authentication.....	14
Enroll and log in the RNI with multi-factor authentication.....	15
5 System Administration Software menu.....	19
Services tab.....	19
Components tab.....	19
6 System Administration Configuration menu.....	21
Customers tab	21
Add a customer.....	21
Networks tab.....	23
Add or edit a network.....	23
Sub-Networks tab.....	24
Configuration tab	25
Configuration parameters - Devices filter.....	26
Configuration parameters - Reads filter.....	35
Configuration parameters - Reporting filter.....	38
Configuration parameters - Interfaces filter.....	41
Configuration parameters - Communications filter.....	57
Configuration parameters - RNI filter.....	60
Key Management tab.....	62
7 System Administration Users menu.....	64
Users tab	64
Add or edit a user.....	64
Delete a user.....	66
Filter the Users tab and export the results.....	67
Roles tab.....	68
User roles.....	69
System permissions.....	80

Password Management tab.....	89
Password management for service accounts.....	90
Configure the password policy for service accounts.....	90
Apply the password policy to service accounts.....	92

1 System administration overview

Device Manager (DM) provides the primary means for the FlexNet® AMI system operator to monitor and report on device status, monitor device alerts, and manage device configuration information.

This User Guide presents instruction on functionality available to system administrators in the Sensus Device Manager (DM) application. The DM application supports large-scale FlexNet AMI systems, providing a single interface with which to manage system-wide jobs to any or all of their FlexNet devices.

The system administrator performs all functions within the DM web user interface. Users with this role can oversee the entire system, and monitor and configure system parameters. They can also perform potentially destructive functions. Examples include actions on a group or deletion of multiple devices.

The RNI does not limit the number of devices that a user can select to perform an action on. The normal workflow is to apply a series of filters to reduce the set of meters, and then take action on the smaller set.

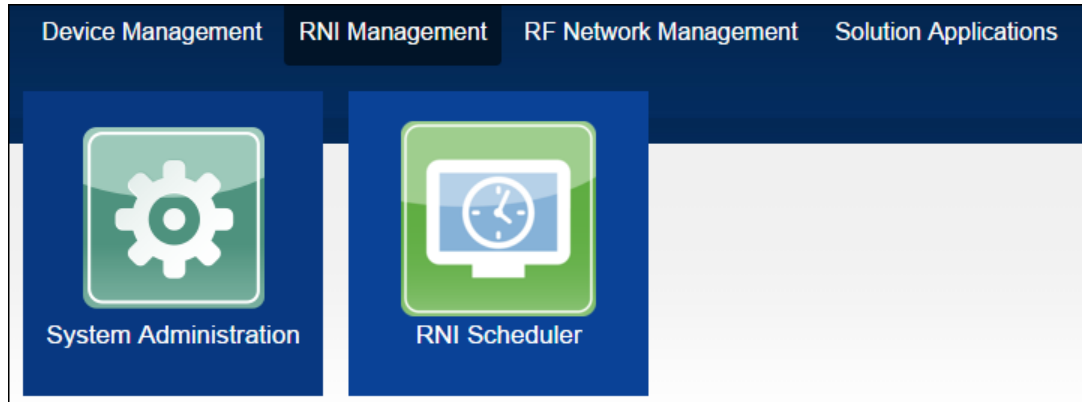


Note: For RNI 4.7.0 and later, a feature is available to prevent users from accidentally performing an action on the entire meter population. The system administrator can set a maximum number of devices on which an action can be performed. See the *DeviceManager.MaxDeviceActionsPerRequest* parameter in the Configuration parameters section for details.

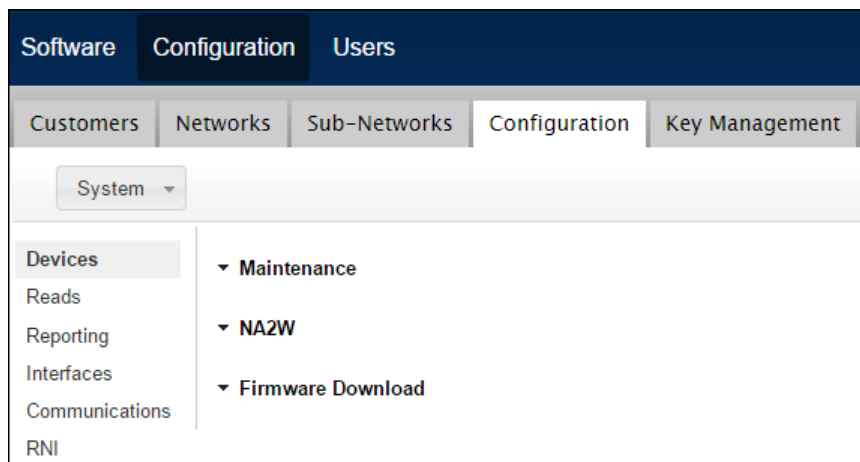
2 Access the System Administration page

From the **System Administration** page, you can manage the software, configuration, and users of the RNI system.

1. From the Launch Pad, select **RNI Management > System Administration**.



The **System Administration** page opens to the **Configuration** menu and tab by default.



2. On the **System Administration** page, select the tab and sub-tab, if applicable, that corresponds with the task you need to complete.

Tabs

- Software
 - Services
 - Components
- Configuration
 - Customers
 - Networks

- Sub-Networks
- Configuration
- Key Management
- Users
 - Users
 - Roles
 - Password Management
- SentryPoint Users



Note: This tab only displays for users with the SentryPoint application. Details about SentryPoint users are provided in the SentryPoint application online help.

3 RNI user password settings

Users can change their RNI user password from the Sensus Launch Pad.

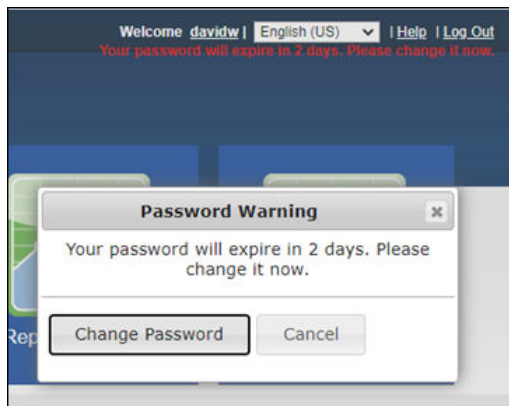
For RNI version 4.8 and later, if password notification is enabled in System Administration users will be notified via email if their RNI password is going to expire soon. Only users with a valid email address in their user profile will receive an email notification when their password expiration is approaching.

All users are required to enter an email address before their next password change. After adding an email address, users will receive an email when their password is getting ready to expire.

Additionally, a warning displays in red text in the upper-right corner of the Sensus Launch Pad if the user's password will expire soon. A pop-up warning similar to the following also displays when the user logs in the RNI. Both warnings display every time the user logs in the RNI during the warning period.



Note: The warning period is specified in the System Administration application. See *Password Management* in the *RNI System Administrator User Guide* for details.



The user needs to select **Change Password** to go to the User Profile page and change their password.



Note: System Administrators can enable and disable email notification of expiring passwords in the RNI System Administration software. This is accomplished by selecting **Configuration > Configuration > Communications > General**. Use the *Expiration.Notification.Enabled* parameter to enable or disable email notifications. Use the *Expiration.Notification.Intervals* parameter to specify when emails are sent. For example, the default value of 3w,2w,1w,5d,3d,2d,1d sends an email to users 3 weeks, 2 weeks, 1 week, 5 days, 3 days, 2 days, and 1 day before their password is due to expire.



Important: For customers with onsite/licensed RNI servers, an SMTP server must be configured to send the password expiration emails. After configuring the server, enable the User Password Expiration Notification job in the RNI Scheduler application.

For customers with RNI servers hosted in Sensus' Data Center, the RNI does not send the password expiration emails. The password expiration information is added to the user's Red Hat Directory Server (RHDS) policy and RHDS sends the emails.

If the Password Expiration Email Notification feature is enabled, users will receive an email similar to the following when it is time to change their RNI password:

Hello Bill Jones,

Your password for your RNI account "billj" on testmail_testserver.name.lab expires in 89 day(s), on December 17, 2023. Please change your password as soon as possible to avoid login problems.

You can change your password by following the link provided below:

testmail_testserver.name.lab/slp/user_profile

Thank you!

Please contact Sensus support if you have any issues.

The template for this email comes with default wording. However, RNI System Administrators can customize the wording of the email if necessary. The templates are located in the /templates directory within /opt/flexnet/usr-acct-notification.

The method of receiving email notifications and triggering the send notification job is the same as in prior RNI versions. The system uses flexnet.notification.properties in /opt/flexnet/usr-acct-notification/conf, and the notification intervals behave the same.



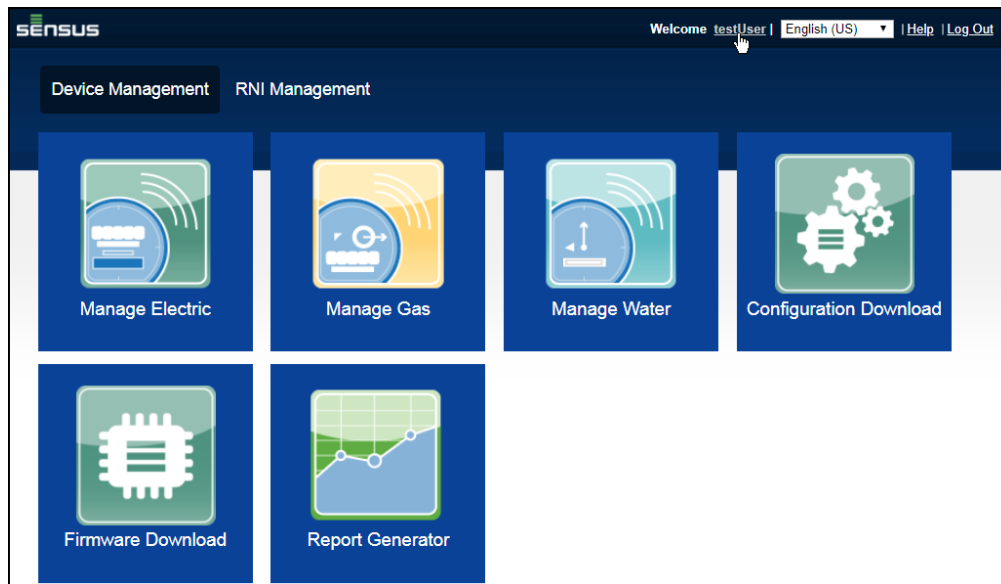
Note: These settings only work with LDAP. If the RNI is configured to use Active Directory, the administrators must manage these notifications within Active Directory.



Note: This email configuration can also be set via the RNI's installer, which sets properties in flexnet.local.properties with a prefix of email.

Follow the steps in this procedure to change your RNI password.

1. Select your user name in the upper-right corner of the page to open the User Profile page.



2. To add an email address to your user profile or to change the email associated with your profile, enter a valid email address in the **Email** field and select **Submit**.



Note: You must submit a valid email address before you can change your password.

User Profile

All fields *required.

User ID:

User Name:

Change Email Address

Email: *

Change Password

Current Password: *

New Password: *

Confirm New Password: *

or [Cancel](#)

3. Enter your current password in the **Current Password** field.
4. Enter your new password in the **New Password** field.
5. Confirm the new password by entering it in the **Confirm New Password** field.



Note: The passwords that you enter in the **New Password** and **Confirm New Password** fields must be identical.

6. Select **Submit**.

If your new password meets the complexity requirements (if any were specified by the RNI system administrator), the User Profile page closes and you are returned to the Sensus Launch Pad.



Note: An error message displays if the password entered in the **New Password** field does not match the password entered in the **Confirm New Password** field, or if the password does not match the complexity requirements set by the RNI system administrator. If the password change is unsuccessful due to complexity requirements, the exact reason is stated in the error message.

4 Multi-factor authentication

RNI version 4.10.1 and later include Multi-Factor Authentication (MFA). Xylem recommends the use of multi-factor authentication by all customers to add extra layers of security to Device Manager.

The RNI's implementation of MFA features a Time-based One-Time Password (TOTP) based solution allowing tokens from your mobile device as an additional authentication step. MFA can be enabled at a user level.

MFA works with multiple third-party TOTP-based applications. The following table lists several third-party tools that were tested and verified compliant with RNI version 4.10.1 and later.

Third-Party Mobile Application	Android	Apple
FreeOTP	✓	✓
Google Authenticator	✓	✓
LastPass Authenticator	✓	✓
2FAS Authenticator	✓	✓
Microsoft Authenticator	✓	✓
Duo Mobile	✓	✓
Okta Verify	✓	✓

You can enable MFA for an existing user, or enable it when creating a new user. See [Add or edit a user](#) for instructions to enable MFA at the user level. You can also enable MFA at the tenant (customer) level. See [Tenant \(customer\) level multi-factor authentication](#) on page 14 and [Add a customer](#) on page 21 for details.

After enabling MFA for a user, the MFA status for the user changes to Pending Enrollment. When the user logs in the RNI using MFA for the first time, and successfully completes enrollment using the third-party mobile application, then the MFA status changes to Enrolled on the User page.

Edit "testU"

Use the inputs below to edit User. Enter all *Required information.

[«Back to User List](#)

First Name:*

Test

Last Name:*

User

User ID:*

testU

Email:*

testuser@fakemail.com

Change Password

Customers:

Select Customer(s)
ACME
SNX08
SLCTD

Password Policy:

Select Policy
ACME
default
special

Multi-Factor Authentication

Customer	Status	Action to take
ACME	Enrolled	<input checked="" type="radio"/> None <input type="radio"/> Disable <input type="radio"/> Reset

System Administrators can also Disable MFA or Reset the MFA process for the user.

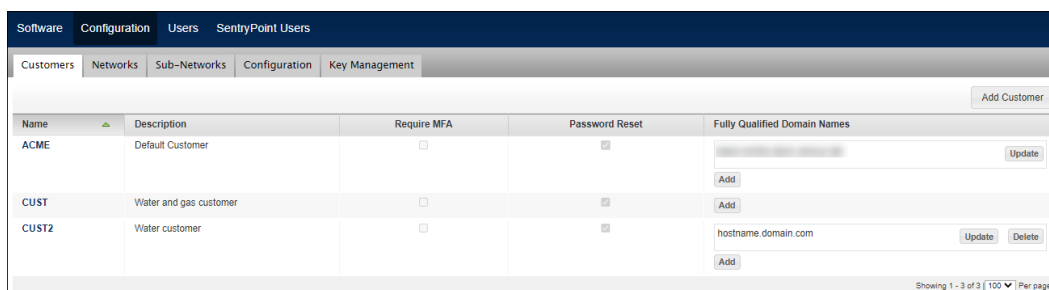
Tenant (customer) level multi-factor authentication

Tenant-level multi-factor authentication (MFA) administers MFA at the tenant, or customer level. Users with the TENANT_ADMIN and SERVICE_SYSTEM_ADMIN user roles can configure tenant-level MFA from the **Configuration > Customers** page.

Tenant-level MFA applies MFA to all LDAP and Active Directory users of a tenant/customer. When enabled, the RNI automatically applies MFA to new users added to the customer.

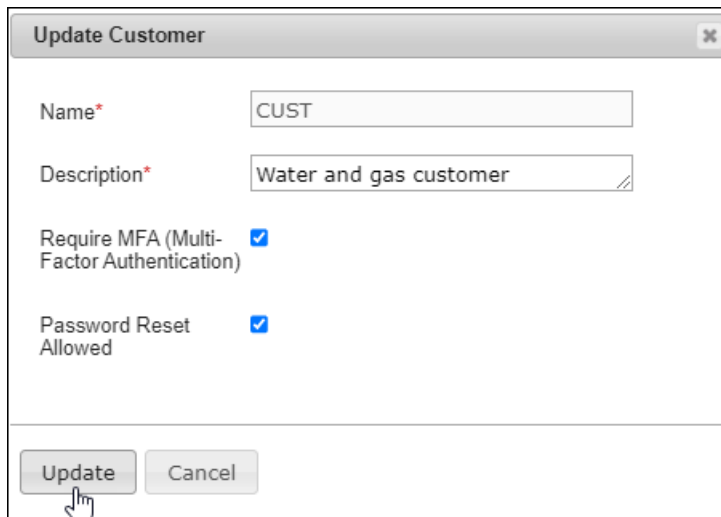
Tenant-level MFA excludes sensus-admin and service account users. For tenants/customers with MFA enabled, user-level MFA modification is not allowed.

See [Add a customer](#) on page 21 for instructions to add a new customer with multi-factor authentication. To enable MFA for an existing customer, select the customer name from the list of customers on the **Configuration > Customers** page.



Name	Description	Require MFA	Password Reset	Fully Qualified Domain Names
ACME	Default Customer	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/> <input type="button" value="Add"/> <input type="button" value="Update"/>
CUST	Water and gas customer	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/> <input type="button" value="Add"/>
CUST2	Water customer	<input type="checkbox"/>	<input checked="" type="checkbox"/>	hostname.domain.com <input type="button" value="Add"/> <input type="button" value="Update"/> <input type="button" value="Delete"/>

In the Update Customer dialog box that opens, select the **Require MFA (Multi-Factor Authentication)** option and then click **Update**.



Update Customer

Name*

Description*

Require MFA (Multi-Factor Authentication) ☒

Password Reset Allowed ☒

Active Directory and multi-factor authentication

For RNI systems integrated with Active Directory, the Active Directory users display on the Users page (for RNI version 4.10.1 and later). For previous versions of the RNI, the Users page was blank for Active Directory integrations.

This enhancement was made to enable Multi-Factor Authentication (MFA) for Active Directory integrations. From the Users page, an administrator can enable MFA at the

individual user level. Additionally, this also gives Active Directory administrators a way to view the roles that are assigned to each user.

Software Configuration Users SentryPoint Users				
Users Roles Password Management				
User ID	Name	Customer	Email	Filter
Automation	Auto Mation	GOTG	Automation@company.com	
guestAdmin	Guest Administrator	LF027 GOTG	guestAdmin@company.com	
pamiAdmin	Pami Admin	GOTG	pamiAdmin@company.com	
special&T	special test	GOTG	special&T@company.com	
s-special	Special User	GOTG	s-special@company.com	
tab T	tab Test	GOTG	tab T@company.com	

You can view the Active Directory users like any other user, but the User Roles are read-only as they are defined by Active Directory. An administrator can enable MFA for these users.

Edit "guestAdmin"

Use the inputs below to edit User. Enter all *Required information.

[Back to User List](#)

First Name:

Last Name:

User ID:

Email:

Multi-Factor Authentication

Customer	Status	Action to take
GOTG	Disabled	<input checked="" type="radio"/> None <input type="radio"/> Enable
LF027	Disabled	<input checked="" type="radio"/> None <input type="radio"/> Enable

User Role(s)

ACME_JGP

ACME_SF00809546

Enroll and log in the RNI with multi-factor authentication

After enabling multi-factor authentication (MFA) for a user, the next time the user attempts to log in the RNI they are prompted to enroll in MFA. Follow these steps to enroll and log in the RNI using MFA.



Note: MFA must be enabled for the user before they can follow this process and log in using MFA. See [Add or edit a user](#) for instructions. Additionally, the user must install one of the supported authenticator applications on their mobile device to enable this process. See [Multi-factor authentication](#) for a list of supported applications.

1. Install the supported authenticator application recommended by your System Administrator on your mobile device.
2. Enter your **Username** and **Password** for the RNI.

SENSUS

UTILITY ACME

Username

testU

Password

.....

Log In

This system may be accessed and used by authorized personnel only. Authorized users may only perform authorized activities and may not exceed the limits of such authorization. All activities on this system are subject to monitoring. Intentional misuse of this system can result in disciplinary action.

3. Select **Log In** and the following page displays with a barcode.



UTILITY ACME



You need to set up an external authenticator application to activate your account.

1. Install one of the supported authenticator applications. See system administrator.
2. Open the application and scan the barcode:



[Unable to scan?](#)

3. Enter the one-time code provided by the application and click Submit to finish the setup.

Provide a Device Name to help you manage your OTP devices.

Registration Code (Do not include spaces.) *

Device Name (Optional but recommended.)

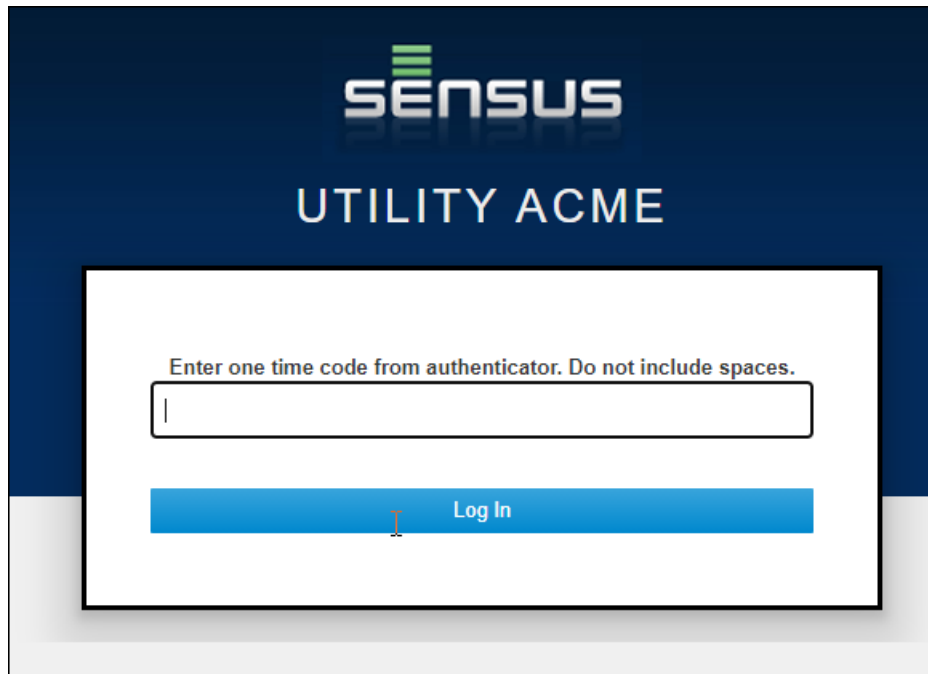
Submit

4. Scan the barcode using the third-party application installed on your mobile device. The third-party application displays a 6-digit code on your device.
5. Enter the 6-digit code from your mobile device in the **Registration Code** field on the RNI login page.
6. Optionally, enter a name to identify your mobile device in the **Device Name** field.
7. Select **Submit** and you are now enrolled in MFA for the RNI, and you are logged in the system.

Log in using MFA

8. The next time you log in, enter your Username and Password as usual (see Step 2 on page 15), and select **Log In**.

The following one time code page displays.



The screenshot shows a login interface for 'SENSUS UTILITY ACME'. The background is dark blue with the Sensus logo at the top. A white rectangular box in the center contains the text 'Enter one time code from authenticator. Do not include spaces.' above a text input field. Below the input field is a blue button labeled 'Log In'.

9. Enter the 6-digit code from the authentication application installed on your mobile device.
10. Select **Log In** and the Sensus Launch Pad opens. You are now logged in the RNI.

5 System Administration Software menu

Use the **Software** menu to view the services running on the RNI and the components that comprise it.

The **Software** menu consists of two tabs: Services and Components. Both tabs are read-only, and contain information about the Regional Network Interface (RNI). Select the headings to change the sort order of any column.

Services tab

The **Services** tab on the **Software** menu is an information-only page that lists the services that run on the RNI servers, and shows the status of each service.

Use the **Services** tab to view the service assigned to each RNI server, and the status of each service.

Software Configuration Users			
Services		Components	
Server		Service	Status
elara-combo		apps	Running
elara-combo		Auth	Running
elara-combo		Batch Engine	Running
elara-combo		Broker	Running
elara-combo		cce	Running
elara-combo		Config Download	Running
elara-combo		epclistener	Running
elara-combo		ESM	Running
elara-combo		ESM Bellwether	Running
elara-combo		Messaging	Running
elara-combo		FNP Server	Running
elara-combo		Firmware Download - Electric	Running
elara-combo		Firmware Download - NA2W	Running
elara-combo		Gateway	Running
elara-combo		HAN	Running
elara-combo		loadprofile-tools	Running

Components tab

The **Components** tab on the **Software** menu is an information-only page that shows RNI software component names, internal code names, and software versions.

Use the **Components** tab to view the code and software version assigned to each RNI software component.

Software Configuration Users		
Services	Components	
Name	Code	Version
ActiveMQ	activemq	0.0.0-323713
alarm-notification-service-v1	alarm-notification-service-v1	0.0.0-323713
alarm-rest-service-v1	alarm-rest-service-v1	0.0.0-323713
Apache HTTP server	flexnet-httpd	0.0.0-323713
App	flexnetapp	0.0.0-323713
Auth	flexnet-auth	0.0.0-323713
Batch Engine	flexnet-batch-engine	0.0.0-323713
CCE	flexnet-cce	0.0.0-323713
Config Download	flexnet-configdownload	0.0.0-323713
Coverage	flexnet-coverage	0.0.0-323713
Data Extraction	flexnet-dataextraction	0.0.0-323713
Db Builder	DbBuilder	0.0.0-3868
DM	flexnet-dm	0.0.0-323713
Environment	flexnet-environment	0.0.0-323713
Firmware Download	flexnet-fwdl	0.0.0-323713
Flexnet Hardening	flexnet-hardening	0.0.0-323713

6 System Administration Configuration menu

The **Configuration** menu enables you to configure customer, network, sub-network, system, and key management settings.

Customers tab

The **Customers** tab on the **Configuration** menu lists all current customers associated with the RNI, and enables you to add a customer or edit an existing customer description.

The listing on the **Customers** tab contains the customer name and description for each customer associated with the RNI. Additionally, it lists the fully qualified domain name (FQDN) if one has been provided, and enables you to update the FQDN. It also specifies whether multi-factor authentication (MFA) is required for the customer and whether password reset is enabled for the customer.

Software Configuration Users SentryPoint Users				
Customers Networks Sub-Networks Configuration Key Management				
				Add Customer
Name	Description	Require MFA	Password Reset	Fully Qualified Domain Names
ACME	Default Customer	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value=""/> Update
				Add
Showing 1 - 1 of 1 100 ▼ Per page				



Note: Access to the **Customers** tab is restricted to users with SYSTEM_ADMIN privileges or TENANT_ADMIN and SERVICE_SYSTEM_ADMIN privileges. Only users with full SYSTEM_ADMIN role access can add a new customer, and enable or disable password reset. Users with TENANT_ADMIN and SERVICE_SYSTEM_ADMIN roles can enable or disable MFA for an existing customer.

Add a customer

You can add a new customer (with or without multi-factor authentication) to the RNI using this process.

1. Select **Add Customer** and the **Add Customer** dialog box displays.

2. Enter the customer **Name**.



Note: The customer name must consist of 3 to 5 characters and start with an uppercase letter. It can contain uppercase letters and numbers.

3. Enter a **Description** for the customer.
4. To require multi-factor authentication (MFA) for the new customer, select the **Require MFA (Multi-Factor Authentication)** check box. If you do not want to use MFA for the new customer, do not select this option. See [Multi-factor authentication](#) on page 13 for information about using MFA.



Note: If you select the Require MFA option, the customer list shows the Require MFA status for this customer as Processing while the RNI is creating the customer. The Processing status changes to a check mark when MFA is enabled for the customer.

5. To enable the customer's users to reset their password if it expires or they cannot remember it, select the **Password Reset Allowed** check box. If you do not want the users to be able to reset their own password, do not select this option.
6. Optionally, enter a fully qualified domain name (for the customer's RNI web address) in the **FQDN** field.
7. Select one of the following **Security** options for the FQDN:
 - **Generate** to have the RNI generate a random certificate and private key for the FQDN. Continue with Step 8 on page 22.
 - **Provided** to upload your own certificate and private key.
 - a) If you chose **Provided**, select **Browse** and navigate to the folder containing your Certificate File.
 - b) If you chose **Provided**, select **Browse** and navigate to the folder containing your Private Key File.
8. To save changes, select **Add**. Select **Cancel** to exit without saving changes.

Immediately after adding a customer with a FQDN, the status of the FQDN will show as SUBMITTED. After the RNI accepts the FQDN, you will be able to update or delete it by selecting **Update** or **Delete**.

Customers
Networks
Sub-Networks
Configuration
Key Management

"CUST2" added successfully.
Close

Add Customer

Name	Description	Require MFA	Password Reset	Fully Qualified Domain Names
ACME	Default Customer	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/> Update
CUST	Water and gas customer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Add
CUST2	Water customer	<input type="checkbox"/>	<input type="checkbox"/>	Status: SUBMITTED hostname.domain.com

Customers
Networks
Sub-Networks
Configuration
Key Management

Add Customer

Name	Description	Require MFA	Password Reset	Fully Qualified Domain Names
ACME	Default Customer	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/> Update
CUST	Water and gas customer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Add
CUST2	Water customer	<input type="checkbox"/>	<input type="checkbox"/>	hostname.domain.com Update Delete

Add

Networks tab

The **Networks** tab on the **Configuration** menu enables you to add or edit networks that contain your base station groups.

A network represents a group of base stations in the system. When you create a base station in the user interface, you must include the network it will use to communicate. By creating a network here, you make it available to the rest of the system.

Software
Configuration
Users

Customers
Networks
Sub-Networks
Configuration
Key Management

Add Network

Network ID	Network Name	City	State
ACME	SimSetup Network	ACME City	CA
?	Unknown Network		

Showing 1 - 2 of 2 | 100 ▼ Per page

Add or edit a network

1. Select **Add Network** or a specific network ID, and the **Update Network** or **Add Network** dialog box displays.

Update Network

Network ID*

ACME

Network Name*

SimSetup Network

City

ACME City

State

CA

Update

Cancel

- If you are adding a network, enter the **Network ID**.



Note: When you update network information, the network ID cannot be changed.

- Enter the **Network Name**.
- Enter a **City** and **State** to indicate the network location.
- To save changes, select **Update** or **Add**.
- To cancel the changes and return to the **Networks** tab, select **Cancel**.

Sub-Networks tab

The **Sub-Networks** tab on the **Configuration** menu enables you to edit the sub-network name and customer affiliation.

A sub-network associates a network with a customer. Multiple customers can be associated with a network, and multiple networks can be associated with a customer.

Software Configuration Users

Customers Networks Sub-Networks Configuration Key Management

Save Changes

Sub-Network Name	Sub-Network ID	Network ID	Customer
Autogenerated Subnet	0	?	ACME
Autogenerated Subnet	0	ACME	ACME
Autogenerated Subnet	1	?	ACME
Autogenerated Subnet	2	?	ACME
Autogenerated Subnet	5	?	ACME
Autogenerated Subnet	6	?	ACME
Autogenerated Subnet	7	?	ACME
Autogenerated Subnet	9	?	GW
Autogenerated Subnet	9	ACME	GW
Autogenerated Subnet	12	?	ACME
Autogenerated Subnet	15	?	ACME

Showing 1 - 11 of 11 | 100 | Per page

To edit the name, highlight the current **sub-network name**, and enter a new name in the field. To change the associated customer, select from the **Customer** drop-down list.

To complete the changes, select **Save Changes**.

Configuration tab

The **Configuration** tab on the **Configuration** menu lists all system configuration parameters for various components of the RNI, and enables you to change the default values.

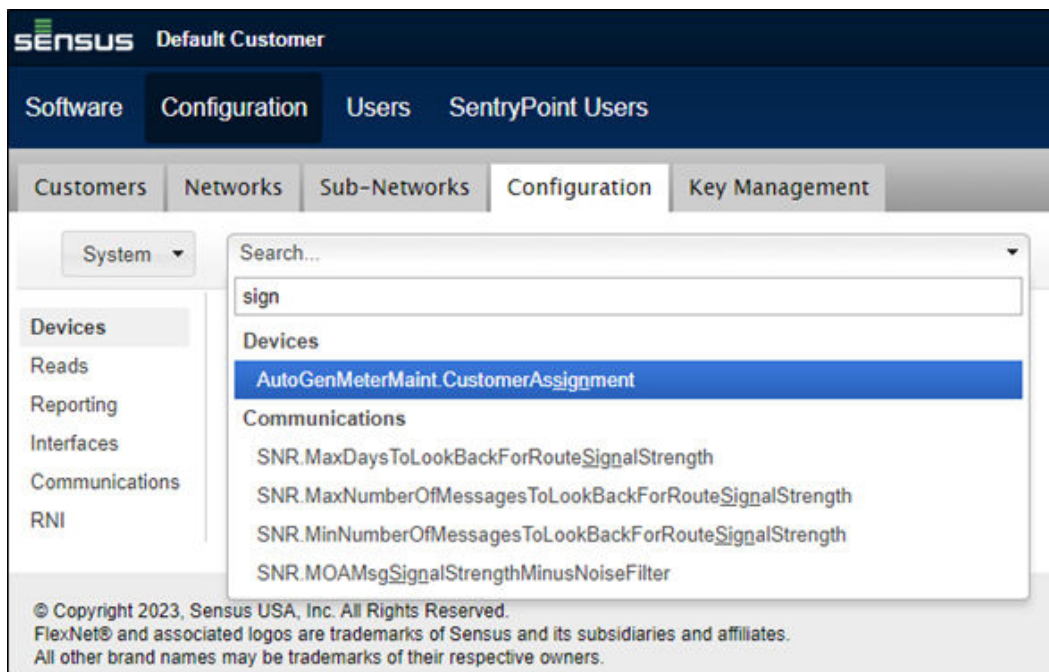
On the **Configuration** tab, you can work with parameters based on the filters list on the left side of the page. You can customize the parameter values for any customer.

If the defaults have never been changed:

1. Under **System**, select the company for which you need to make changes.
2. For each parameter to change, select **override for customer**.
3. Select or enter the new value.
4. Select **Save Changes**.

If the default values have been changed, skip Step 2.

For RNI 4.14 and later, administrators can search for settings within the RNI's configuration. Partial matches are used, so you only need to enter a few characters of the configuration setting you are looking for.



Export the configuration settings

You can export all configuration settings for the system or a specific customer/RNI instance using the **Export** button in the upper-right corner of the **Configuration** tab. The exported files can then be compared using a third-party comparison tool to find any differences between the configuration settings. This is useful when a customer has two instances of the RNI. For example, a test system with the latest RNI version and a production system with an earlier RNI version.



Note: The Export Configuration feature is available for RNI versions 4.13.1 and later.

1. Select **System** or a specific customer/RNI instance from the drop-down menu in the upper-left corner of the **Configuration** tab.
2. Click the **Export** button and the system automatically downloads a CSV file that lists all RNI Configuration parameters for the System or the selected customer/RNI instance.

If System is selected from the drop-down menu, the configuration file that downloads is named `SYSTEM_properties.csv`. If a specific customer is selected, the configuration file is named `CUSTOMER_properties.csv`. The downloaded CSV file contains the following columns sorted in this order:

- Customer
- Category
- Sub-category
- Property
- Property value

Configuration parameters

The **Configuration** tab lists all system configuration parameters for various components of the RNI. The system configures these parameters with a set of default values, and the **Configuration** tab provides the opportunity to override the defaults. The following tables list the configuration parameters, a description of each parameter, and its default value.

The parameters are organized under six filters:

- [Devices](#)
- [Reads](#)
- [Reporting](#)
- [Interfaces](#)
- [Communications](#)
- [RNI](#)

Under each filter, parameters are further organized into sub-filters. The tables that follow are organized by the filters and sub-filters present on the **Configuration** tab.

Configuration parameters - Devices filter

Configuration Key	Description	System Default Settings
Maintenance Sub-filter		
RemoveSetupBindDataOnMeterDelete	Delete Setup and Bind message data (tblUniversalSetup, tblVersionInfo, and tblLastPosted) when deleting a meter from tblMeterMaint. Selections: True, False	False
MeterSerialNumber.Water.RemovePrependedValue	A CSV list of characters to be matched to remove the prepend character from a Water meter. If set to False, the key is not used.	False

Configuration Key	Description	System Default Settings
MeterSerialNumber.Water.RemoveAppendedValue	A CSV list of characters to be matched to remove the append character from a Water meter. If set to False, the key is not used.	False
MeterSerialNumber.Gas.RemovePrependedValue	A CSV list of characters to be matched to remove the prepend character from a Gas meter. If set to False, the key is not used.	False
MeterSerialNumber.Gas.RemoveAppendedValue	A CSV list of characters to be matched to remove the append character from a Gas meter. If set to False, the key is not used.	False
MeterSerialNumber.Electric.RemovePrependedValue	A CSV list of characters to be matched to remove the prepend character from an Electric meter. If set to False, the key is not used.	False
MeterSerialNumber.Electric.RemoveAppendedValue	A CSV list of characters to be matched to remove the append character from an Electric meter. If set to False, the key is not used.	False
MeterSerialNumber.AllowSpace	Allows spaces to be used in meter serial numbers.  Note: The meter setup and bind process removes any leading or trailing spaces added to the serial number. Only "internal" spaces are allowed.	False
MeterMaintHistory.Enabled	Controls if the MeterMaintHistory records can be created or updated. Selections: True, False	False
MeterLifecycle.AllowAddingRetiredMeterDays	Enables a meter in Retired status to be added back, using add meter operation after value days.	7
LifeCycle.IncludeUnknownLifecycle	Whether to include the Unknown lifecycle state to determine if a meter is installed. Selections: True, False	True
LifeCycle.AllowBypassInventoryState	Whether to let the system set a meter directly to the Installed state, bypassing the Inventory state. Selections: True, False	True
AutoGenMeterMaint.Enabled	Controls whether SmartPoint modules are created and maintained automatically. Selections: True, False	True


Configuration Key	Description	System Default Settings
AutoGenMeterMaint.CustomerAssignment	Controls the customer ID assignment policy during SmartPoint module installation. Selections: <ul style="list-style-type: none"> • <i>AbortIfUnknown</i> - Do not create a metermaint record if unable to find the customer ID based on the subnet ID. • <i>FallbackToDefault</i> - Set the customer ID based on the subnet ID. If unable to find the customer ID based on the subnet ID, set to DefaultCustomerId config key value. • <i>ForceDefault</i> - Set customer ID with the DefaultCustomerId config key value. 	FallbackToDefault
AutoGenMeterMaint.AutoGenGroup.Members	CSV list of devices that is auto-generated in tblmetermaint by the application. Always install, always overwrite fields for tblmetermaint.	81
Maintenance > Auto-create for Sub-filter		
AutoGenMeterMaint.Water.CreateNewRecord	Add a water SmartPoint module upon receipt of an installation message. Selections: True, False	True
AutoGenMeterMaint.LC.CreateNewRecord	Add a lighting SmartPoint module upon receipt of an installation message. Selections: True, False	True
AutoGenMeterMaint.Gas.CreateNewRecord	Add a gas SmartPoint module upon receipt of an installation message. Selections: True, False	True
AutoGenMeterMaint.DA.CreateNewRecord	Add a distribution automation SmartPoint module upon receipt of an installation message. Selections: True, False	True
AutoGenMeterMaint.AutoGenGroup.CreateNewRecord	Add a SmartPoint module upon receipt of an installation message.	True
Maintenance > Default Lifecycle Sub-filter		
AutoGenMeterMaint.Water.CreateNewRecord.InitialLifeCycleStateCode	Controls the initial lifecycle state for a water SmartPoint module installation. Selections: Install, Inventory	Install
AutoGenMeterMaint.LC.CreateNewRecord.InitialLifeCycleStateCode	Controls the initial lifecycle state for a lighting SmartPoint module installation. Selections: Install, Inventory	Install
AutoGenMeterMaint.Gas.CreateNewRecord.InitialLifeCycleStateCode	Controls the initial lifecycle state for a gas SmartPoint module installation. Selections: Install, Inventory	Install
AutoGenMeterMaint.DA.CreateNewRecord.InitialLifeCycleStateCode	Controls the initial lifecycle state for a distribution automation SmartPoint module installation. Selections: Install, Inventory	Install

Configuration Key	Description	System Default Settings
AutoGenMeterMaint.AutoGenGroup.CreateNewRecord.InitialLifeCycleState Code	Controls the initial lifecycle state for a SmartPoint module installation. Selections: Install, Inventory	Install
Maintenance > Overwrites > General Sub-filter		
AutoGenMeterMaint.AutoGenGroup.Overwrite.MeterId	Meter ID overwrite option during SmartPoint module installation. Selections: AllowSwap, DoNotOverwrite, Overwrite	Overwrite
AutoGenMeterMaint.AutoGenGroup.Overwrite.LatLong	Latitude and longitude overwrite option during SmartPoint module installation.	True
AutoGenMeterMaint.AutoGenGroup.Overwrite.DeviceTypeFields	Device type fields overwrite option during SmartPoint module installation.	True
Maintenance > Overwrites > Electric Sub-filter		
AutoGenMeterMaint.Electric.Overwrite.MeterId	Controls if fldMeterId in tblMeterMaint can be updated during electric SmartPoint module installation. Selections: True, False	True
AutoGenMeterMaint.Electric.Overwrite.LatLong	Controls if fldLat and fldLong in tblMeterMaint can be updated during electric SmartPoint module installation. Selections: True, False	True
AutoGenMeterMaint.Electric.Overwrite.DeviceTypeFields	Controls if fldDeviceType and fldMeterType in tblMeterMaint can be updated during electric SmartPoint module installation. Selections: True, False	True
Maintenance > Overwrites > Water Sub-filter		

Configuration Key	Description	System Default Settings
AutoGenMeterMaint.Water.Overwrite.MeterId	<p>Controls the water MeterId overwrite behavior during water SmartPoint module installation.</p> <p>Selections:</p> <ul style="list-style-type: none"> • <i>AllowSwap</i> - Applies only to Water and Gas meters. If the auto-generated meter ID already exists in tblMeterMaint tied to another endpoint_id, then set the duplicate record's meter ID to Repld:<repid_value> and then auto-generate with the new meter ID. Example for AllowSwap: The record to be auto-generated has Repld=12345, MeterId=12345M. But tblMeterMaint already has a record in the table for Repld=98765 and the same MeterId=12345M. First, change Repld 98765's meter ID to Repld:98765. Then, insert the new tblMeterMaint record with Repld=12345 and MeterId=12345M. • <i>DoNotOverwrite</i> - If the meter ID to be inserted or updated already exists in tblMeterMaint, abort the insert or update. • <i>Overwrite</i> - Replace the meter ID value in tblmetermaint with the meter ID value in the bind message. 	Overwrite
AutoGenMeterMaint.Water.Overwrite.LatLong	<p>Controls if fldLat and fldLong in tblMeter Maint can be updated during water SmartPoint module installation.</p> <p>Selections: True, False</p>	True
AutoGenMeterMaint.Water.Overwrite.DeviceTypeFields	<p>Controls if fldDeviceType, fldMeterType and fldDials in tblMeterMaint can be updated during water SmartPoint module installation.</p> <p>Selections: True, False</p>	True
Maintenance > Overwrites > Gas Sub-filter		

Configuration Key	Description	System Default Settings
AutoGenMeterMaint.Gas.Override.MeterId	<p>Controls the gas MeterId overwrite behavior during gas SmartPoint module installation.</p> <p>Selections:</p> <ul style="list-style-type: none"> • <i>AllowSwap</i> - Applies only to water and gas meters. If the auto-generated meter ID already exists in tblMeterMaint tied to another endpoint_id, then set the duplicate record's meterid to Repld:<repid_value> and then auto-generate with the new meter ID. Example for AllowSwap: The record to be auto-generated has Repld=12345, MeterId=12345M. But tblMeterMaint already has a record in the table for Repld=98765 and the same MeterId=12345M. First, update Repld 98765's meter ID to Repld:98765. Then, insert the new tblMeterMaint record with Repld=12345 and MeterId=12345M. • <i>DoNotOverwrite</i> - If the meter ID to be inserted or updated already exists in tblMeterMaint, abort the insert or update. • <i>Overwrite</i> - Replace the meter ID value in tblmetermaint with the meter ID value in the bind message. 	Overwrite
AutoGenMeterMaint.Gas.Override.LatLong	<p>Controls if fldLat and fldLong in tblMeter Maint can be updated during gas SmartPoint module installation.</p> <p>Selections: True, False</p>	True
AutoGenMeterMaint.Gas.Override.DeviceTypeFields	<p>Controls if fldDeviceType and fldMeterType in tblMeterMaint can be updated during gas SmartPoint module installation.</p> <p>Selections: True, False</p>	True
Maintenance > Overwrites > Lighting Sub-filter		

Configuration Key	Description	System Default Settings
AutoGenMeterMaint.LC.Overwrite. MeterId	<p>Controls the initial MeterId value when tblMeterMaint record is created during lighting SmartPoint module installation.</p> <p>Selections:</p> <ul style="list-style-type: none"> • <i>AllowSwap</i> - Applies only to water and gas meters. If the auto-generated meter ID already exists in tblMeterMaint tied to another endpoint_id, then set the duplicate record's meter ID to Repld:<repid_value> and then auto-generate with the new meter ID. Example for AllowSwap: The record to be auto-generated has Repld=12345, MeterId=12345M. But tblMeterMaint already has a record in the table for Repld=98765 and the same MeterId=12345M. First, update Repld 98765's meter ID to Repld:98765. Then, insert the new tblMeterMaint record with Repld=12345 and MeterId=12345M. • <i>DoNotOverwrite</i> - If the meter ID to be inserted or updated already exists in tblMeterMaint, abort the insert or update. • <i>Overwrite</i> - Replace the meter ID value in tblmetermaint with the meter ID value in the bind message. 	Overwrite
AutoGenMeterMaint.LC.Overwrite. LatLong	<p>Controls the initial LatLong field value when the tblMeterMaint record is created during lighting SmartPoint module installation.</p> <p>Selections: True, False</p>	True
AutoGenMeterMaint.LC.Overwrite. DeviceTypeFields	<p>Controls the initial DeviceTypeFields value when the tblMeterMaint record is created during lighting SmartPoint module installation.</p> <p>Selections: True, False</p>	True
Maintenance > Overwrites > DA Sub-filter		

Configuration Key	Description	System Default Settings
AutoGenMeterMaint.DA.Overwrite.MeterId	<p>Controls the initial Meter ID value when the tblMeterMaint record is created during distribution automation SmartPoint module installation.</p> <p>Selections:</p> <ul style="list-style-type: none"> • <i>AllowSwap</i> - Applies only to water and gas meters. If the auto-generated meter ID already exists in tblMeterMaint tied to another endpoint_id, then set the duplicate record's meter ID to Repld:<repid_value> and then auto-generate with the new meter ID. Example for AllowSwap: The record to be auto-generated has Repld=12345, MeterId=12345. But tblMeterMaint already has a record in the table for Repld=98765 and the same MeterId=12345M. First, update Repld 98765's Meter ID to Repld:98765. Then, insert the new tblMeterMaint record with Repld=12345 and MeterId=12345M. • <i>DoNotOverwrite</i> - If the meter ID to be inserted or updated already exists in tblMeterMaint, abort the insert or update. • <i>Overwrite</i> - Replace the meter ID value in tblmetermaint with the meter ID value in the bind message. 	Overwrite
AutoGenMeterMaint.DA.Overwrite.LatLong	<p>Controls the initial Latitude/Longitude value when the tblMeterMaint record is created during distribution automation SmartPoint module installation.</p> <p>Selections: True, False</p>	True
AutoGenMeterMaint.DA.Overwrite.DeviceTypeFields	<p>Controls the initial DeviceType field's value when the tblMeterMaint record is created during distribution automation SmartPoint module installation.</p> <p>Selections: True, False</p>	True
NA2W sub-filter		
Network.na2wMixedMPassModes	<p>Defines whether to enable or disable the mixed data rate mPass for NA2W devices.</p> <p>Selections: True, False</p>	False
Na2w.ValidUtilityCodes	<p>Only messages with these on-air utility codes (also known as customer id) will be processed for LAT and MOM (Middle of Minute).</p> <p> Note: Available for SYSTEM_ADMIN role only.</p>	0,2

Configuration Key	Description	System Default Settings
Na2w.MomBroadcastAttempts	Indicates the number of MOM broadcast attempts for FlexType 9. FlexType 9 applies to FlexNet V2 gas and water devices.	3
Na2w.MigrateWalkByDriveByToFixedBase	Indicates whether the RNI should auto-upgrade all WalkByDriveBy endpoints to use FixedBase communications. Selections: True, False	False
Na2w.MigrateOneWayToTwoWay	Indicates whether the RNI should auto-upgrade OneWay endpoints to TwoWay when possible. Selections: True, False	False
Na2w.MigrateMomToLat	Indicates whether the RNI should set endpoints in Middle of Minute (MOM) to fixed-base LAT. Selections: True, False	False
Na2w.MigrateFixedBaseListenAfterTalkToMiddleOfMinute	Indicates whether the RNI should attempt to maintain Middle of Minute (MOM) sync with endpoints. Selections: True, False	False
Na2w.GroupBroadcast.ResponseModulation	Response modulation to use for NA2W FlexNet version 2 (FNV2) group responses. Selections: _2SFSK, _2SFSK_8B, _2SFSK_HB, _4SFSK, _4SFSK_HB	_2SFSK_HB
Na2w.ExplicitTargetControlOnly	Ignore all default migration settings and only use explicit target_toplevel_state to drive commands.	False
Na2w.EnableCertCompression	Indicates whether security certificate compression is enabled. Selections: True, False	False
Na2w.DefaultTopLevelState	Default top level state. Selections: WalkBy/DriveBy, Fixed Base (LAT)	Fixed Base (LAT)
Firmware Download sub-filter		
firmwaredownload.smJobMaxJobCompletionCycles	The number of Job Completion cycles.	200
firmwaredownload.smJobCarouselIterations	Iterations per Carousel Ride.	4
firmwaredownload.phaselterationDelayMinutes	The time (in minutes) to wait before starting another Phase iteration.	35
firmwaredownload.missingBlockIterations	The number of times to iterate through Missing Block processing.	1
firmwaredownload.medJobMaxJobCompletionCycles	The number of Job Completion cycles.	100
firmwaredownload.medJobCarouselIterations	The number of iterations per Carousel Ride.	8
firmwaredownload.maxJobCompletionCycles	The number of Job Completion cycles.	50

Configuration Key	Description	System Default Settings
firmwaredownload.maxAttempt	The maximum attempts for Firmware Download phases.	7
firmwaredownload.loadStartBroadcast Iterations	The number of times to iterate through the Load Start phase.	50
firmwaredownload.lgJobMax.Job CompletionCycles	The number of Job Completion cycles.	100
firmwaredownload.lgJobCarousel Iterations	Iterations per Carousel Ride.	12
firmwaredownload.jobCompletion Threshold	Job completion threshold.	95
firmwaredownload.individualMessages PerHour	Individual messages per hour.	180
firmwaredownload.defaultBroadcast MessageChannel	Default Broadcast Message Channel.	0.0
firmwaredownload.carouselIterations	The number of iterations per Carousel Ride.	7
firmwaredownload.broadcastMessages PerHour	Broadcast messages per hour.	180
firmwaredownload.autoRefreshTime	The time (in milliseconds) to Auto-Refresh pages in the FWDL GUI.	300000

Configuration parameters - Reads filter

Configuration Key	Description	System Default Settings
General sub-filter		
MeterReading.IncludeDemandReset	When True, demand resets are included in latest readings.	True
ESM sub-filter		
esm.suppressMetaPing	Suppresses metadata ping from the RNI. This is provided so that metadata pings can be avoided when replaying messages to sync up a parallel system. Turn off during replay. Selections: True, False	False
ESM.ProcessingModelForUnknown Dataset	Controls the Processing Model for undefined dataset; defaults to ignore.	0
esm.maxBackfillDays	The maximum number of days the ESM will backfill to (or the oldest metadata change time, whichever is closer).	30
esm.backfillPeriod	Maximum number of days to backfill.	30

Configuration Key	Description	System Default Settings
esm.backfillGapFactor	<p>This is a multiplier on the intervals-per-supervisory message that determines the maximum number of intervals in a backfill request.</p> <p>Because meters are supposed to put as many intervals in a single 0x5C supervisory message as possible, you should always backfill equal or less than the interval count in the supervisory message. A bigger than 1 factor would most likely cause MPT packets and more on-air traffic than savings.</p>	1
Parsers sub-filter		
parsers.validation.water.mrf	<p>Set MRF based on the parameters MRF or MRF non-numeric for water meters.</p> <p>Selections: True, False</p>	False
parsers.validation.PowerRestore	<p>Controls the power restore flag validation step.</p> <p>Selections: LogOnly, SilentValidate, Skip, Validate</p>	SilentValidate
parsers.validation.PhysicalCapacity	<p>Controls the physical capacity validation step.</p> <p>Selections: LogOnly, SilentValidate, Skip, Validate</p>	Validate
parsers.validation.OverlapMismatch	<p>Controls the overlap mismatch validation step.</p> <p>Selections: LogOnly, SilentValidate, Skip, Validate</p>	Validate
parsers.validation.MeterReadFail	<p>Controls the meter read fail flag validation step.</p> <p>Selections: LogOnly, SilentValidate, Skip, Validate</p>	SilentValidate
parsers.validation.HistoryLength Mismatch	<p>Controls the validation step that compares the parsed history depth with the passed-in history depth.</p> <p>Selections: LogOnly, SilentValidate, Skip, Validate</p>	Validate
parsers.validation.HalfInterval	<p>Controls the half interval validation step.</p> <p>Selections: LogOnly, SilentValidate, Skip, Validate</p>	Validate
parsers.validation.ElsterBug. Embedded55IsCorrupt	<p>Controls the Elster (Honeywell) high-res bug workaround validation step.</p> <p>Selections: LogOnly, SilentValidate, Skip, Validate</p>	SilentValidate
parsers.validation.EliminateNegatives	<p>Controls the Eliminate negative values parser behavior.</p> <p>Selections: LogOnly, SilentValidate, Skip, Validate</p>	Validate

Configuration Key	Description	System Default Settings
parsers.validation.Backwards Progression	Controls the backwards progression validation step. This includes <i>reads cannot be less than nearest older</i> and <i>reads cannot be more than nearest newer</i> checks. Selections: LogOnly, SilentValidate, Skip, Validate	Validate
parsers.PostToMessageRaw	Indicates if the message_raw table should have data inserted into it. This can be turned off to save disk space and to improve performance. Selections: True, False	False
parsers.PostOnAirMessages	Indicates whether on-air messages should be parsed and posted. This is only applicable if message type 96 is also turned on. This can be turned off to save disk space and to improve performance. Selections: True, False	False
parsers.PostIdleMessages	Indicates whether idle messages should be parsed and posted. This is only applicable if message type 96 is also turned on. This can be turned off to save disk space and to improve performance. Selections: True, False	True
Engine sub-filter		
ReadEngine.Water.SamplePointModel	Override calculation of sample point from sample time. Selections: round.to.hour.max, round.to.sample.rate	round.to.sample.rate
ReadEngine.Water.RollDetection.Tolerance	Percentage value used to detect rollover or rollunder in the biz rules so that reads are not mistakenly quarantined after a register rollover occurs.	1.0
ReadEngine.Water.PrecisionModel	Override option for the Read Summation Precision Model. Valid values: summation.precision.preserve, summation.precision.reduce	summation.precision.preserve
ReadEngine.Model.BuildAcrossXmit Gap	Invalidated intervals derived from anchors. Selections: True, False	True
ReadEngine.Gas.SamplePointModel	Override calculation of sample point from sample time. Selections: round.to.hour.max, round.to.sample.rate	round.to.sample.rate
ReadEngine.Gas.RollDetection.Tolerance	Percentage value used to detect rollover or rollunder in the biz rules so that reads are not mistakenly quarantined after a register rollover occurs.	1.0

Configuration Key	Description	System Default Settings
ReadEngine.Gas.PrecisionModel	Override option for the Read Summation Precision Model. Valid values: summation.direct.derivation, summation.precision.preserve, or summation.precision.reduce	summation.precision. preserve
ReadEngine.ElectricResidential.Roll Detection.Tolerance	Percentage value used to detect rollover or rollunder, which prevents residential electric reads from being incorrectly quarantined after a register rollover occurs.	1.0
ReadEngine.ElectricCI.RollDetection. Tolerance	Percentage value used to detect rollover or rollunder, which prevents commercial electric reads from being incorrectly quarantined after a register rollover occurs.	1.0
ReadEngine.Electric.SamplePointModel	Override calculation of sample point from sample time. Selections: round.to.hour.max, round.to.sample.rate	round.to.sample.rate
Permalog.MeterId.Identifier	Check the meter ID on a per-reas basis to determine if the device is a Permalog device.	False
LPv2.CollectionFrequency	Number of hours before initiating a current block ping. Selections: 00, 08, 12, 16	00
Backfill sub-filter		
backfill.EnableByDefault	Specifies whether endpoints are automatically backfilled by default. Selections: True, False	False
backfill.BackfillPeriodDays	The number of days after which missing reads will no longer be backfilled.	0

Configuration parameters - Reporting filter

Configuration Key	Description	System Default Setting
General sub-filter		
Reports.Water.RescaleReads	Rescales the reads to match 2x behavior for MDM.	1
Reports.sql.MeasurementResolution-W	Specifies the reading presentation in reports for water. As of RNI 4.3.1, this configuration option is no longer applicable on some reports. See the <i>RNI Reports Operation Reference Manual</i> for details.	False
Reports.sql.MeasurementResolution-L	Specifies the reading presentation in reports for lighting. As of RNI 4.3.1, this configuration option is no longer applicable on some reports. Please see the <i>RNI Reports Operation Reference Manual</i> for details.	False

Configuration Key	Description	System Default Setting
Reports.sql.MeasurementResolution-G	Specifies the reading presentation in reports for gas. As of RNI 4.3.1, this configuration option is no longer applicable on some reports. Please see the <i>RNI Reports Operation Reference Manual</i> for details.	False
reports.meterlist.timezone	Default time zone value for meters.	-1
Reports.IgnoreGenericMeterId	Used to ignore generic meter ID.	False
reports.iee_events_xml.Collection SystemId	The value is reported as the collection SystemId attribute in the Itron Enterprise Edition Events XML file.	AMDS
reports.iconatoudatatypefilter	CSV list to control the iConA TOU data set to look for while reporting. Selections: 0-Current, 1-Midnight, 2-Last DemandReset, 4-LastSeason	1,2
Reports.HighFlowThreshold	Default threshold for high flow.	750
Reports.EnhancedDemandReset	If enabled, the SelfReport and TOUReport include the time and value of peak demand, and the count.	False
Reports.Debug	Debugging reports.	False
Reporting.ScaleReadDigits	Enable this setting to display what the meter dials show, or disable (clear the check box) to display the full value.	False
NormalizedSampleTime	If set to True, the report uses fldSamplePoint. Otherwise, it uses fld-SampleTime. Selections: True, False	False
MeterRead.Model.Interval	The meter read model. Selections: derived, transmitted	transmitted
MeterIdSource	Defined the location from which FlexNet retrieves the meter ID. Selections: FlexNetIdForMeter, MeterIdAsReportedByMeter, MeterIdFromMdmif	MeterIdAsReportedByMeter
ITron.LocalizeTimestamps	Set to False to report time in UTC. Selections: True, False	True
IntervalReportMaxRows	Maximum number of matrix detail rows to process. If greater than this, the report is aborted.	250000000
hhfimport.LoadDirectory	The HHF import process folder.	/opt/hhf/file-load
hhfimport.DPMInstallDirectory	The default directory for HHF to find the DPM.	C:\Program Files (x86)\Sensus\Database Builder SDB\Reporting
HHF.LocalizeTimestamps	Set to True to report time in local time. Selections: True, False	False
HHF.DeleteMissingIntervals	Determines if missing intervals should be included or excluded in the load profile HHF report.	False
DeliveryPath	Base path of the Delivery folder.	/var/opt/flexnet/data-extracts


Configuration Key	Description	System Default Setting
CMEP sub-filter		
MLA01	Defines what flexible data fields will be used by the MLA01 report.	FlexNetIdForMeter, MeterIdFromMdmif, Unused,Unused, Unused,Unused
MEPMD02	Defines what flexible data fields will be used by the MEPMD02 report.	FlexNetIdFor Meter,MeterIdFrom Mdmif,Unused, Unused,TOU DataType,Unused
MEPMD01	Defines what flexible data fields will be used by the MEPMD01 report.	FlexNetIdFor Meter,MeterIdFrom-Mdmif,Unused, Unused, Unused, Unused
MEPEC01	Defines what flexible data fields will be used by the MEPEC01 report.	FlexNetIdFor Meter,MeterIdFrom-Mdmif,Unused, Unused, Unused, Unused
loadprofile.maxhistorydays	The maximum number of days that can be read.	30
Cmep.Water.ValueTruncate	Set to True to perform truncation instead of rounding on values with larger scale than the format. Selections: True, False	False
Cmep.Water.ValueFormat	C# format string that controls meter reading value formatting.	0.###
Cmep.TOU-NonTierIncludeSummation	Controls whether to include summation reads with peak demand reads in TimeOfUseReport non-tier. Selections: True, False	True
Cmep.SenderCustomerIdOverride	Configurable SenderCustomerId value to override default behavior.	Default
Cmep.SelfReadReportAppCodes	A CSV list to control the app codes to look for while reporting.	25,31,46,48,93
Cmep.SelfRead.RegisterRead.Quantity TypeId.Filter	The quantity type IDs to exclude from the report. Examine the quantity_type table for quantity_type_id definitions.	
Cmep.RunIntervalReportIn2xWater Format	Set to True to generate an interval report in 2x format for water customers.	False
Cmep.ReceiverIdOverride	Configurable ReceiverId value to override default behavior.	Default
Cmep.LPIntervalReportIncludeN32in RRR	Controls whether to exclude missing reads from ReferenceReadRow in LoadProfileIntervalReport for ESM.	True
Cmep.LPIntervalReportChannelList	A list to control which LP channels to include for publishing in CMEP. For example, All indicates all channel data exported, and 1,2 indicates channels 1 and 2.	All
Cmep.LocalizeTimestamps	Set to True to convert local time stamps using tblMeterMaint.fldUSTZ and tblMeterMaint.fldFollowsDST. Selections: True, False	False



Configuration Key	Description	System Default Setting
Cmep.LatLongDecimalPlaces	The number of decimal places when displaying Latitude and Longitude.	6
CMEP.IntervalReportOnlyR0inRRR	If True, only R0 summation values are to be included in ReferenceReadRow.	False
Cmep.IncludeQuarantinedIntervals	If True, include quarantined intervals in the CMEP reports.	False
Cmep.IgnoreSendIntervalData	Controls whether to include the filter based on tblMeterMaint.fldsendintervaldata. Selections: True, False	False
Cmep.Gas.ValueTruncate	Set to True to perform truncation instead of rounding on values with larger scale than the format. Selections: True, False	False
Cmep.Gas.ValueFormat	C# format string that controls meter reading value formatting.	0.###
Cmep.EnhancedReferenceReadRow	Set to True to report midnight values on read reference row. Selections: True, False	False
Cmep.Electric.ValueTruncate	Set to True to perform truncation instead of rounding on values with larger scale than the format. Selections: True, False	False
Cmep.Electric.ValueFormat	C# format string that controls meter reading value formatting.	0.###
Cmep.DefaultRateLabel.Tier7	Used when rate codes are not used.	RATE_G
Cmep.DefaultRateLabel.Tier6	Used when rate codes are not used.	RATE_F
Cmep.DefaultRateLabel.Tier5	Used when rate codes are not used.	RATE_E
Cmep.DefaultRateLabel.Tier4	Used when rate codes are not used.	RATE_D
Cmep.DefaultRateLabel.Tier3	Used when rate codes are not used.	RATE_C
Cmep.DefaultRateLabel.Tier2	Used when rate codes are not used.	RATE_B
Cmep.DefaultRateLabel.Tier1	Used when rate codes are not used.	RATE_A
Cmep.DefaultRateLabel.Tier0	Used when rate codes are not used.	TOTAL
Cmep.ApplyTransformerMultipliers	Specify as True to apply PT/CT multipliers to meter reading values. Selections: True, False	False
Cmep.Alarms.ExcludeEventStatus History	Exclude details found only in event_status_history. Selections: True, False	False

Configuration parameters - Interfaces filter


Configuration Key	Description	System Default Settings
Device Manager sub-filter		
SoftAlarm.Stales.5dayThreshold	The limit of stale meters for 5 days before raising the soft alarm.	1000


Configuration Key	Description	System Default Settings
SoftAlarm.Stales.1dayThreshold	The limit of stale meters for 1 day before raising the soft alarm.	1000
SoftAlarm.ReportTracking.10dayThreshold	The limit of meters in a report over 10 days before raising the soft alarm.	1000
DeviceManager.ThrottlingDurationForDisconnectCommands	Sets the Service Switch > Disconnect action time length in hours. This spreads the disconnect commands over the selected number of hours instead of fulfilling all of the disconnect commands as fast as possible. Options include 1, 2, 4, 8, 12, 16, 20, 24, and 48 hours. Select 0 to disable this feature.	0
DeviceManager.Publish.CDStateChange	If True, the RemoteLoadShedAcknowledgement orchestration event distributor will post asynchronous state change notifications to the Device Manager CDStateChange queue.	False
MDMIF sub-filter		
MDMIF.MaxFileTransactionsPendingResumeSize	File input transactions will resume when the pending size falls to this number.	0
MDMIF.MaxFileTransactionsPendingPauseSize	The maximum number of pending file input transactions that can be active.	100
MDMIF.FileInputPath	The Flat File input path.	/opt/mdmif/file-input
MDMIF.FileArchivePath	The Flat File archive path.	/opt/mdmif/file-archive
MultiSpeak > Version3 > Connect-Disconnect (CD) Sub-filter		
Multispeak.CDCB.GetCDSupportedMeters.MaxResults	The maximum number of results retrieved from a database query for the CD->CB GetCDSupportedMeters web service call.	300
Multispeak.CD.GetCDSupportedMeters.FetchSize	The maximum number of meters returned in a response to GetCDSupportedMeters.	500
Multispeak.CBCD.DestinationUserId	The userid for logging in at the destination URL on the customer utility box that will support the FlexNet CBCD web service calls.	
Multispeak.CBCD.DestinationURL	The destination URL on the customer utility box that will support the FlexNet CBCD web service calls.	
Multispeak.CBCD.DestinationPassword	The password for logging in at the destination URL on the customer utility box that will support the FlexNet CBCD web service calls.	

Configuration Key	Description	System Default Settings
Multispeak.CBCD.DestinationEnabled	This key controls if the FlexNet CBCD web service calls will use the matching tblConfigValues.fldMember and their values in Multispeak.CBCD.Destination URL, Multispeak.CBCD.Destination UserId, Multispeak.CBCD.Destination Password. Set to False if you do not want to send to this URL, set to True if you do want to send to this URL. Selections: True, False	False
MultiSpeak > Version3 > Meter Reading (MR) Sub-filter		
Multispeak.MRCB.GetAMRSupportedMeters.MaxResults	The maximum number of results retrieved from a database query for the MR->CB GetAMRSupportedMeters web service call.	300
Multispeak.MRCB.ForceTOU	Controls whether to force including the tier reads for a meter or let the rate code determine if they are returned. If set to True, then the tier reads are included regardless of the rate code. If set to False, then the tier reads are only included if a valid TOU rate code has been assigned to the meter. A meter must have a TOU rate code in order to return TOU data. Selections: True, False	False
Multispeak.CBMR.ReadingChangedNotification.RetryInterval	Waiting period (in milliseconds) between ReadingChangeNotification SOAP message retries.	30000
Multispeak.CBMR.ReadingChangedNotification.RetryCount	Number of resend retries upon transmission error during ReadingChangedNotification SOAP message delivery.  Note: SOAP fault responses from DestinationURLs are not considered transmission errors.	5
Multispeak.CBMR.ReadingChangedNotification.MaxCacheCount	Maximum number of caches that the notification client should keep in play. A higher number of caches provides a better tolerance to slow consumers and event floods, because the notification client has a bigger capacity for processing events. This value should be bounded depending on the available memory on the server. Recommend that the value in a production system be 2 or higher. Changes to this parameter take effect after gateway restart.	100
Multispeak.CBMR.ReadingChangedNotification.MaxAutoRecoveries	Controls maximum number of gateway cache recovery attempts before a data purge (-1 is unlimited).	32

Configuration Key	Description	System Default Settings
Multispeak.CBMR.ReadingChangedNotification.BatchTime	<p>Length of time, in milliseconds, that a partial batch is retained. Upon expiry, SOAP messages containing outages in the partial batch will be sent. Changes to this parameter take effect after gateway restart.</p> <p> Note: Even if batching is primarily being controlled with the batchSize property, a non-zero value should always be specified for the batch time property so that readings are not buffered in the MR system indefinitely.</p>	100
Multispeak.CBMR.ReadingChangedNotification.BatchSize	<p>The number of ReadingChanged events included in a single SOAP message that is bound for the notification server. For example, a value of 100 means that MR will wait until it receives 100 readings for that destination, and will then forward them on in one ReadingChanged Notification message. If both batch size and batch time are specified, then either condition may trigger the SOAP message to be sent. Changes to this parameter take effect after gateway restart.</p>	5
Multispeak.CBMR.ReadingChangedNotification.AutoRecoveryInterval	Sets the time interval between gateway cache auto recovery attempts (in milliseconds).	900000
Multispeak.CBMR.DestinationUserId	The userid for logging in at the destination URL on the customer utility CB box that will support the FlexNet CB->MR web service calls.	
Multispeak.CBMR.DestinationURL	<p>The destination URL on the customer utility CB box that will support the FlexNet CB->MR web service calls, such as GetAllMeters, GetAllServiceLocations.</p> <p> Note: MultiSpeak says CB->MR is CB serving MR.</p>	https://www.myhost.com/multispeak/cbmr
Multispeak.CBMR.DestinationPassword	The password for logging in at the destination URL on the customer utility that supports the FlexNet CB->MR web service calls.	
Multispeak.CBMR.DestinationEnabled	<p>When True, FlexNet CB->MR web service calls use the matching tbl-ConfigValues.fldMember and their values in Multispeak.CBMR.DestinationURL, Multispeak.CBMR.DestinationUserId, Multispeak.CBMR.DestinationPassword. Set to False if you do not want to send to this URL.</p> <p>Selections: True, False</p>	False+
MultiSpeak > Version3 > Outage Detection (OD) Sub-filter		

Configuration Key	Description	System Default Settings
Multispeak.OAOD.RetryInterval	The waiting period between ODEventNotification SOAP message retries.	30000
Multispeak.OAOD.RetryCount	<p>Upon transmission errors during ODEventNotification SOAP message delivery, this indicates the number of times to attempt resend.</p> <p> Note: SOAP fault responses from the DestinationURL are not considered transmission errors.</p>	60
Multispeak.OAOD.MaxCaches	<p>Maximum number of gateway OA > OD caches that the notification client should keep in play. A higher number of caches provide a better resistance to slow consumers and event floods because the notification client has a bigger sandbox for processing events.</p> <p>This value should be bounded depending on the available memory on the server.</p>	10
Multispeak.OAOD.MaxAutoRecoveries	Controls the maximum number of gateway cache recovery attempts before a data purge (-1 is unlimited).	8
Multispeak.OAOD.DestinationUserId	The UserId for logging in at the destination URL on the customer utility OA box that will support the FlexNet OA->OD web service calls.	
Multispeak.OAOD.DestinationURL	<p>The destination URL on the customer utility OA box that will support the FlexNet OA->OD web service calls, such as ODEventNotification.</p> <p> Note: Multispeak says OA->OD is OA serving OD.</p>	https://www.myhost.com/multispeak/oaod
Multispeak.OAOD.DestinationPassword	The password for logging in at the destination URL on the customer utility OA box that will support the FlexNet OA->OD web service calls.	
Multispeak.OAOD.DestinationEnabled	<p>This key controls if the FlexNet OA->OD web service calls will use the matching tblConfigValues.fldMember and their values in Multispeak.OAOD.Destination URL, Multispeak.OAOD.Destination UserId, Multispeak.OAOD.Destination Password. Set to False if you do not want to send to this URL.</p> <p>Selections: True, False</p>	False
Multispeak.OAOD.BatchTime	The length of time a partial batch is retained. Upon expiry, the SOAP message containing outages in the partial batch will be sent.	3000

Configuration Key	Description	System Default Settings
Multispeak.OAOD.BatchSize	The number of outage events to include in a single MultiSpeak ODEventNotification SOAP message that is bound for the Outage Notification Server.	100
Multispeak.OAOD.AutoRecovery Interval	Sets the interval between gateway cache auto recovery attempts (in milliseconds).	900000
MultiSpeak > Version4 > Customer Billing (CB) Sub-filter		
Multispeak.CB.TimezoneCompliant	Set to True for MultiSpeak standard compliant mode. Set to False to accept zone information. Selections: True, False	False
Multispeak.CB.DestinationUserID	The user ID for logging in to the destination URL on the customer utility CB box that supports FlexNet CB web service calls.	
Multispeak.CB.DestinationURL	The URL to access the customer utility CB box that supports FlexNet CB web service calls.	
Multispeak.CB.DestinationPassword	The password for logging in to the destination URL on the customer utility CB box that supports FlexNet CB web service calls.	
Multispeak.CB.DestinationEnabled	When True, FlexNet CB web service calls use matching tblConfigValues.fldMember and their values in Multispeak.CB.DestinationURL, Multispeak.CB.DestinationUserId, Multispeak.CB.DestinationPassword. Set to False if you do not want to use this destination. Selections: True, False	False
MultiSpeak > Version4 > Connect-Disconnect (CD) Sub-filter		
Multispeak.CD.SD.MaxAttempts	Number of resend retries upon transmission error during Scheduled Disconnect notification SOAP message delivery.  Note: SOAP fault responses from destination URLs are not considered transmission errors.	5
Multispeak.CD.SD.MaxAge	Maximum Scheduled Disconnect notification event age in milliseconds. Notifications with creation timestamps older than this age will be discarded.	
Multispeak.CD.SD.DestinationUserId	The User ID to access the customer notification server that will receive Scheduled Disconnect notifications.	
Multispeak.CD.SD.DestinationURL	The URL to access the customer notification server that will receive Scheduled Disconnect notifications.	

Configuration Key	Description	System Default Settings
Multispeak.CD.SD.Destination Password	The password for logging into the destination URL on the customer utility box supporting Scheduled Disconnect notifications web service calls.	
Multispeak.CD.SD.DestinationEnabled	When True, FlexNet Scheduled Disconnect notifications will be sent to Multispeak.CD.SD.DestinationURL with Multispeak.CD.SD.DestinationUserId and Multispeak.CD.SD.DestinationPassword. Set to False if you do not want to use this destination.	
Multispeak.CD.SD.BatchTime	Length of time in milliseconds that a partial batch is retained. SOAP messages containing Scheduled Disconnect notification events in the partial batch are sent upon expiration.	3000
Multispeak.CD.SD.BatchSize	Number of Scheduled Disconnect events included in a single MultiSpeak Scheduled Disconnect notification SOAP message bound for the notification server.	1
Multispeak.CD.SD.AttemptInterval	Waiting period in milliseconds between Scheduled Disconnect notification SOAP message attempts.	30000
Multispeak.CD.MaxAttempts	<p>Number of resend retries upon transmission error during CD notification SOAP message delivery.</p> <p> Note: SOAP fault responses from DestinationURLs are not considered transmission errors.</p>	5
Multispeak.CD.MaxAge	Maximum CD event age in milliseconds.	
Multispeak.CD.GetCDSupportedMeters.FetchSize	Fetch size for CD supported meters.	500
Multispeak.CD.DestinationUserId	The userid for logging in at the destination URL on the customer utility box that will support the FlexNet CD web service calls.	
Multispeak.CD.DestinationURL	The destination URL on the customer utility box that will support the FlexNet CD web service calls.	
Multispeak.CD.DestinationPassword	The password for logging in at the destination URL on the customer utility box that will support the FlexNet CD web service calls.	

Configuration Key	Description	System Default Settings
Multispeak.CD.DestinationEnabled	This key controls if the FlexNet CD web service calls will use the matching tblConfigValues.fldMember and their values in Multispeak.CD.DestinationURL, Multispeak.CD.DestinationUserId, Multispeak.CD.DestinationPassword. Set to False if you do not want to send to this URL, set to True if you do want to send to this URL. Selections: True, False	False
Multispeak.CD.BatchTime	Length of time that a partial batch is retained. Upon expiration, SOAP messages containing outages in the partial batch will be sent.	3000
Multispeak.CD.BatchSize	Number of CD events to include in a single Multispeak CD Notification SOAP message that is bound for the CD notification server.	1
Multispeak.CD.AttemptInterval	Waiting period between CD Notification SOAP message attempts.	30000
MultiSpeak > Version4 > Demand Response (DR) Sub-filter		
Multispeak.DR.DestinationUserId	User ID for Demand Response Gateway Notification Client.	
Multispeak.DR.DestinationURL	Destination URL of Demand Response Gateway Notification Client.	
Multispeak.DR.DestinationPassword	Password for Demand Response Gateway Notification Client.	
Multispeak.DR.DestinationEnabled	Turn on or off notifications for Demand Response. Selections: True, False	False
MultiSpeak > Version4 > Home Area Network (HAN) Sub-filter		
Multispeak.HAN.HANRegistrationNotification.DestinationUserId	User ID in HAN Registration notifications.	
Multispeak.HAN.HANRegistrationNotification.DestinationURL	Destination URL for HAN Registration notifications.	
Multispeak.HAN.HANRegistrationNotification.DestinationPassword	Password in HAN Registration notifications.	
Multispeak.HAN.HANRegistrationNotification.DestinationEnabled	Turn on or off notifications for HAN Registration. Selections: True, False	False
Multispeak.HAN.HANCommissionNotification.DestinationUserId	User ID in HAN Commissioning notifications.	
Multispeak.HAN.HANCommissionNotification.DestinationURL	Destination URL for HAN Commissioning notifications.	
Multispeak.HAN.HANCommissionNotification.DestinationPassword	Password in HAN Commissioning notifications.	
Multispeak.HAN.HANCommissionNotification.DestinationEnabled	Turn on or off notifications for HAN Commissioning. Selections: True, False	False


Configuration Key	Description	System Default Settings
Multispeak.HAN.DestinationUserId	Destination UserID of HAN Gateway Notification Client.	
Multispeak.HAN.DestinationURL	Destination URL of HAN Gateway Notification Client.	
Multispeak.HAN.DestinationPassword	Destination Password of HAN Gateway Notification Client.	
Multispeak.HAN.DestinationEnabled	Determines whether the HAN Gateway Notification Client destination is enabled. Selections: True, False	False
MultiSpeak > Version4 > Meter Reading (MR) Sub-filter		
Multispeak.MR.TimezoneCompliant	Set to True for MultiSpeak standard compliant mode. Set to False to accept no information. Selections: True, False	False
Multispeak.MR.ReadingChanged Notification.MaxAttempts	The RNI entry should not be used; add a customer-specific value. Enter the maximum number of delivery attempts to send a SOAP message to the subscriber. A null value indicates there is no limit.	
Multispeak.MR.ReadingChanged Notification.MaxAge	The RNI entry should not be used; add a customer-specific value. Enter the maximum permitted age of deliverable meter events in milliseconds. A null value indicates there is no age limit.	
Multispeak.MR.ReadingChanged Notification.BatchTime	Length of time, in milliseconds, that a partial batch is retained. Upon expiry, SOAP messages containing ReadingChangedNotifications in the partial batch will be sent. Changes to this parameter take effect after gateway restart.	100
Multispeak.MR.ReadingChanged Notification.BatchSize	The number of outage events included in a single MultiSpeak ReadingChangedNotification SOAP message that is bound for the outage notification server. For example, a value of 100 means that MR will wait until it receives 100 readings for that destination, and will then forward them on in one ReadingChangedNotification message. If both batch size and batch time are specified, then either condition may trigger the SOAP message to be sent.	5
Multispeak.MR.ReadingChanged Notification.AttemptInterval	The RNI entry should not be used; add a customer-specific entry. Enter the waiting period in milliseconds between ReadingChangedNotification message send attempts.	150,000

Configuration Key	Description	System Default Settings
Multispeak.MR.PublishDerivedSummation.WATER	Publish derived Water summations as EndReadings. Selections: True, False	False
Multispeak.MR.MeterEventsReset.DestinationUserId	The RNI entry should not be used; add a customer-specific entry. Enter the destination server MeterEventReset userid.	
Multispeak.MR.MeterEventsReset.DestinationURL	The RNI entry should not be used; add a customer-specific entry. Enter URL where MeterEventReset will be delivered, in the form http://<hostname.meterreading>:<port> / <MR_Soap_Service>	
Multispeak.MR.MeterEventsReset.DestinationPassword	The RNI entry should not be used; add a customer-specific entry. Enter the destination server MeterEventReset password.	
Multispeak.MR.MeterEventsReset.DestinationEnabled	The RNI entry should not be used; enter a customer-specific entry. Enables MeterEventReset to the configured DestinationURL. Selections: True, False	False
Multispeak.MR.MeterEventNotification.DR.DestinationUserId	The RNI entry should not be used; add a customer-specific entry. Enter the destination server MeterEventNotification DR userid.	
Multispeak.MR.MeterEventNotification.DR.DestinationURL	The RNI entry should not be used; add a customer-specific entry. Enter URL where MeterEventNotification DR will be delivered, in the form http://<hostname.meterreading>:<port> / <MR_Soap_Service>	
Multispeak.MR.MeterEventNotification.DR.DestinationPassword	The RNI entry should not be used; add a customer-specific entry. Enter the destination server MeterEventNotification DR password.	
Multispeak.MR.MeterEventNotification.DR.DestinationEnabled	The RNI entry should not be used; enter a customer-specific entry. Enables MeterEventNotification DR to the configured DestinationURL. Selections: True, False	False
Multispeak.MR.MeterEvent.MaxAttempts	Number of resend retries upon transmission error during MR MeterEvent SOAP message delivery.  Note: SOAP fault responses from Destination URLs are not considered transmission errors.	
Multispeak.MR.MeterEvent.MaxAge	The RNI entry should not be used; add a customer-specific entry. Enter the maximum permitted age of deliverable meter events in milliseconds. A null value indicates there is no age limit.	

Configuration Key	Description	System Default Settings
Multispeak.MR.MeterEvent.Destination UserId	The RNI entry should not be used; add a customer-specific entry. Enter the destination server MR userid.	
Multispeak.MR.MeterEvent.Destination URL	The RNI entry should not be used; add a customer-specific entry. Enter URL where MR MeterEvent will be delivered, in the form http://<hostname.meterreading>:<port> / <MR_Soap_Service>	
Multispeak.MR.MeterEvent.Destination Password	The RNI entry should not be used; add a customer-specific entry. Enter the destination server MR password.	
Multispeak.MR.MeterEvent.Destination Enabled	The RNI entry should not be used; enter a customer-specific entry. Enables MeterEvent Notification to the configured DestinationURL. Selections: True, False	False
Multispeak.MR.MeterEvent.BatchTime	Length of time a partial batch is retained. SOAP messages containing outages in the partial batch are sent upon expiration.	100
Multispeak.MR.MeterEvent.BatchSize	Number of MeterEvents included in a single SOAP message bound for the notification server.	5
Multispeak.MR.MeterEvent.Attempt Interval	Waiting period (in milliseconds) between MR MeterEvent SOAP message retries.	150,000
Multispeak.MR.IntervalDataNotification. MaxAttempts	The RNI entry should not be used; add a customer-specific entry. Enter the maximum number of delivery attempts.	5
Multispeak.MR.IntervalDataNotification. MaxAge	The RNI entry should not be used; add a customer-specific entry. Enter the maximum permitted age of deliverable IntervalDataNotification.	
Multispeak.MR.IntervalDataNotification. DestinationUserId	The RNI entry is not used; add a customer-specific entry for the MR UserId.	
Multispeak.MR.IntervalDataNotification. DestinationURL	The RNI entry is not used add a customer-specific entry. Enter URL where IntervalDataNotification will be delivered, in the form http://<host-name.meterreading>:<port>/<MR_Soap_Service>.	
Multispeak.MR.IntervalDataNotification. DestinationPassword	The RNI entry is not used; add a customer-specific entry. Enter the destination server MR password.	
Multispeak.MR.IntervalDataNotification. DestinationEnabled	The RNI entry should not be used; add a customer-specific entry. Enables IntervalDataNotification to the configured DestinationURL. Selections: True, False	False

Configuration Key	Description	System Default Settings
Multispeak.MR.IntervalDataNotification.BatchTime	Length of time a partial batch is retained. SOAP messages containing outages in the partial batch are sent upon expiration.	120000
Multispeak.MR.IntervalDataNotification.BatchSize	The number of IntervalData notifications included in a single SOAP message that is bound for the notification server. For example, a value of 100 means that MR will wait until it receives 100 blocks for that destination and then forward them on in one message.	1000
Multispeak.MR.IntervalDataNotification.AttemptInterval	The RNI entry should not be used; add a customer-specific entry. Enter the waiting period between IntervalDataNotification message send attempts, in milliseconds.	150000
MultiSpeak.MR.HistoryLogChangedNotification.DestinationUserId	The RNI entry should not be used; add a customer-specific entry. Enter the destination server HistoryLogChangedNotification UserId.	
MultiSpeak.MR.HistoryLogChangedNotification.DestinationURL	The RNI entry should not be used; add a customer-specific entry. Enter the URL from which the HistoryLogChangedNotification will be delivered as http://<hostname.meterreading>:<port>/<MR_Soap_Service> url.	
MultiSpeak.MR.HistoryLogChangedNotification.DestinationPassword	The RNI entry should not be used; add a customer-specific entry. Enter the destination server HistoryLogChangedNotification password.	
MultiSpeak.MR.HistoryLogChangedNotification.DestinationEnabled	The RNI entry should not be used; add a customer-specific entry. Enables HistoryLogChangedNotification for the configuration destination URL.	
Multispeak.MR.GetIntervalData.MaxReadingsCount	Maximum number of Readings returned in Interval Data. A block is demarcated by a register reading from the meter; the granularity of a block depends on the transmissions received from the meter. In general one block will contain multiple actual readings.	2000
Multispeak.MR.GetEventHistory.MaxEventsCount	Maximum number of rows returned for event history gateway calls.	1000
Multispeak.MR.GetAMRSupportedMeters.FetchSize	Fetch size for AMRSupported Meters.	500

Configuration Key	Description	System Default Settings
Multispeak.MR.ForceTOU	Whether to force including the tier reads for a meter or let the rate code determine if they are returned. If True, then tier reads are included regardless of the rate code (assuming the meter is reporting tier reads). If False, then tier reads are only included if a valid Time of Use (TOU) rate code has been assigned in the RNI for this meter. Selections: True, False	False
Multispeak.MR.EventLogNotification.MaxCacheCount	Maximum Cache count for Event Log Notification.	50
Multispeak.MR.EndpointConfigurationChangedNotification.DestinationUserId	The RNI entry is not used; add a customer-specific entry for the MR EndpointConfigurationChanged Notification userid.	
Multispeak.MR.EndpointConfigurationChangedNotification.DestinationURL	The RNI entry is not used; add a customer-specific entry in the form http:// <hostname.meterreading>:<port> / <MR_Soap_Service>	
Multispeak.MR.EndpointConfigurationChangedNotification.DestinationPassword	The RNI entry is not used; add a customer-specific entry for the MR EndpointConfigurationChanged Notification password.	
Multispeak.MR.EndpointConfigurationChangedNotification.DestinationEnabled	The RNI entry is not used. Selections: True, False	False
Multispeak.MR.DestinationUserId	The RNI entry is not used. Add a customer specific entry for the MR UserId.	
Multispeak.MR.DestinationURL	The RNI entry is not used. Add a customer specific entry in the form http://<host-name.customerbilling>:<port>/ <MR_Soap_Service>.	
Multispeak.MR.DestinationPassword	The RNI entry is not used. Add a customer specific entry for the MR password.	
Multispeak.MR.DestinationEnabled	An on and off switch for the MR notification client in the RNI. This should be set to True when the subscribing service is ready to receive notifications. Selections: True, False	False
Multispeak.MR.BW.DestinationUserId	The RNI entry should not be used; add a customer-specific entry for the MR Streaming userid.	
Multispeak.MR.BW.DestinationURL	The RNI entry should not be used; add a customer-specific entry in the form http://<hostname.streaming>:<port> / <MR_Soap_Service>	
Multispeak.MR.BW.DestinationPassword	The RNI entry should not be used; add a customer-specific entry for the MR Streaming password.	

Configuration Key	Description	System Default Settings
Multispeak.MR.BW.DestinationEnabled	The RNI entry should not be used; enter a customer-specific entry for the MR Streaming. Selections: True, False	False
MultiSpeak > Version4 > Outage Detection (OD) Sub-filter		
OutageDetection.ping.retryInterval	The time in seconds between successive meter alarm ping retries in the case where there is already an outstanding higher priority meter request.	10
OutageDetection.ping.preemptExisting Transactions	Whether the outage detection fast ping can pre-empt existing lower priority meter requests. Selections: True, False	True
OutageDetection.ping.pingResult ConfidenceThreshold	The minimum confidence threshold to be reached before an outage detection response can be returned.	1.0
OutageDetection.ping.pingPriority	The priority to set for outage detection fast pings.	11
OutageDetection.general.totalTime Allowed	The total time, in seconds, allowed for a request before the best possible response is returned.	60
OutageDetection.general.requestLimit	The maximum number of outage detection requests that can be in progress at a time.	30
OutageDetection.db.usePrevious Messages	Whether the last message on air recorded in the database can be used to determine the occurrence of a meter outage. Selections: True, False	True
OutageDetection.db.previousMessage TrustPowerOnFlag	Whether to trust the last message on air recorded in the database if it indicates a "power on" state. Selections: True, False	True
OutageDetection.db.previousMessage TrustPowerOffFlag	Whether to trust the last message on air recorded in the database if it indicates a "power off" state. Selections: True, False	True
OutageDetection.db.previousMessage MaxAge	The maximum age, in seconds, that the last message on air can be in order to be considered for outage detection.	300
Multispeak.OD.MaxAttempts	Number of resend retries upon transmission error during ODEventNotification SOAP message delivery.  Note: SOAP fault responses from DestinationURLs are not considered transmission errors.	
Multispeak.OD.MaxAge	Maximum event age in milliseconds.	

Configuration Key	Description	System Default Settings
Multispeak.OD.DestinationUserId	The RNI entry is not used; add a customer-specific entry for the OD userid.	
Multispeak.OD.DestinationURL	The RNI entry is not used; add a customer-specific entry in the form http://<host-name.outagedetection>: <port>/<OD_Soap_Service>	http://<host-name. outage detection>: <port>/<OD_Soap_Service>
Multispeak.OD.DestinationPassword	The RNI entry is not used; add a customer-specific entry for the OD Password.	
Multispeak.OD.DestinationEnabled	When True, FlexNet OD web service calls use matching tblConfigValues.fldMember and their values in Multispeak.OD.DestinationURL, Multispeak.OD.DestinationUserId, Multispeak.OD.DestinationPassword. Set to False if you do not want to use this destination. Selections: True, False	False
Multispeak.OD.BatchTime	Length of time that a partial batch is retained. Upon expiry, SOAP messages containing outages in the partial batch will be sent.	3000
Multispeak.OD.BatchSize	Number of outage events to include in a single Multispeak ODEventNotification SOAP message that is bound for the outage notification server.	100
Multispeak.OD.AttemptInterval	Waiting period between ODEventNotification SOAP message attempts.	30000
Gateway sub-filter		
Notifications.StoreAndForward.Reads	Enables store and forward function for unsolicited meter reads to be stored to and distributed from read-notifications.dat. Selections: True, False	False
Notifications.StoreAndForward.Non IntervalReads	Enables store and forward function for unsolicited meter sensor reads to be stored to and distributed from read-notifications.dat. Selections: True, False	False
Notifications.StoreAndForward.Events	Enables store and forward function for unsolicited meter events to be stored to and distributed from event-notifications.dat. Selections: True, False	False
Notifications.StoreAndForward.Event ConfigurationChanged	Enables store and forward function for unsolicited meter event configuration changes to be stored to and distributed from event-notifications.dat. Selections: True, False	False

Configuration Key	Description	System Default Settings
Notifications.StoreAndForward.DeviceConfigurationChanged	Enables store and forward function for unsolicited meter device configuration changes to be stored to and distributed from event-notifications.dat. Selections: True, False	False
Notifications.StoreAndForward.CD	Enables application layer publishing of connect/disconnect events. Selections: True, False	False
Ms3.Gateway.Publish.OutageDetection	Enables application layer publishing of outage detection events. Selections: True, False	False
Ms3.Gateway.Publish.CDStateChange	Enables application layer publishing of connect/disconnect events. Selections: True, False	False
Gateway.Publish.SLC	Enables publications of the SLC (lighting) reads. Selections: True, False	False
Gateway.Publish.BellwetherMeterRead	Controls whether to publish reads from bellwether meters. Selections: True, False	False
Gateway.MinTimeZone	The minimum Time Zone value.	3
Gateway.MinLongitude	The minimum Longitude value.	-180.0
Gateway.MinLatitude	The minimum Latitude value.	-90.0
Gateway.MaxTransactionResponseLength	The maximum length of a Transaction Response.	100
Gateway.MaxTransactionIdLength	The maximum length of a TransactionId.	16
Gateway.MaxTimeZone	The maximum time zone value.	11
Gateway.MaxRepld	The maximum value of a REP ID.	268435455
Gateway.MaxPodLength	The maximum length of a POD.	25
Gateway.MaxMeterIdLength	The maximum length of a MeterId.	25
Gateway.MaxMeterFormLength	The maximum length of a Meter Form.	3
Gateway.MaxLongitude	The maximum Longitude value.	180.0
Gateway.MaxLatitude	The maximum Latitude value.	90.0
Gateway.MaxFlexNetId	The maximum value of a FlexNetId.	268435455
Gateway.MaxDials	The maximum number of dials for a meter.	8
Gateway.MaxCycle	The maximum daily billing cycle.	21
Cathodic.Protection.Publish.MeterRead	Switches on or off notification of cathodic protection reading.	False
MLC Sub-filter		
Mlc.DO.DestinationUserId	The username for logging in at the destination URL on the MLC app that will support the MLC Notification calls.	<destinationusername>

Configuration Key	Description	System Default Settings
Mlc.DO.DestinationURL	The destination URL on the MLC application that will support the Gateway Notification calls.	<destinationURL>
Mlc.DO.DestinationPassword	The password for logging in at the destination URL on the MLC app that will support the MLC Notification calls.	<destinationPassword>
Mlc.DO.DestinationEnabled	Controls if the MLC web service calls will use the matching tblConfigValues.fldMember and their values in Mlc.DO.DestinationURL, Mlc.DO.DestinationUserId, Mlc.DO.DestinationPassword. Set to False if you do not want to send to this URL; set to True if you do want to send to this URL. Selections: True, False	True
SLC Sub-filter		
AutoGenMeterMaint.SLC.Overwrite.MeterId	Controls the lighting control meter ID overwrite behavior. Selections: AllowSwap, DoNotOverwrite, Overwrite	Overwrite
AutoGenMeterMaint.SLC.Overwrite.LatLong	Controls the lighting control latitude and longitude overwrite behavior.	True
AutoGenMeterMaint.SLC.Overwrite.DeviceTypeFields	Controls the lighting control device type fields overwrite behavior.	True
AutoGenMeterMaint.SLC.CreateNewRecord.InitialLifeCycleStateCode	This key sets the lighting control lifecycle state code for a new record. Selections: Install, Inventory	Install
AutoGenMeterMaint.SLC.CreateNewRecord	Creates a new record upon receipt of a setup/binding message from a new lighting device.	True

Configuration parameters - Communications filter

Configuration Key	Description	System Default Settings
Communications > General sub-filter		
ustats.NumOfDays	Number of Days to include in the UStats run (going back from local midnight).	30
ustats.IgnoreEndGapDays	Ignore missing reads and transmissions if no communication received for x days.	4
TGB.58BytePayload.Support	Controls whether the 58-byte payload support feature is enabled. Selections: True, False	False
SNR.MOAMsgSignalStrengthMinusNoiseFilter	Filter used to avoid bad signal strength and noise values caused from iAbort and previous message data.	6
SNR.MinNumberOfMessagesToLookBackForRouteSignalStrength	The minimum number of messages that must exist for the route in order for data to be stored in the direct_route_signal_strength table.	3



Configuration Key	Description	System Default Settings
SNR.MaxNumberOfMessagesToLookBackForRouteSignalStrength	The maximum number of messages for the route to include for signal strength totals.	10
SNR.MaxDaysToLookBackForRouteSignalStrength	The maximum number of days of messages to look for signal information for the particular route.	30
SNR.MaxDaysToLookBackForCurrentChannel	The maximum number of days of messages to look for getting current physical channel per channel type.	7
SNR.IncludeMOANoiseInAverageNoise	Indicates whether or not to average MOA and TGB idle noise values (True) or use TGB idle noise values only (False).	False
SNR.HoursToLookBackForIdleNoise	The number of hours to look back for calculating average noise per TGB physical channel.	24
Expiration.Notification.Intervals	Password expiration email notification intervals. Determines when a specific user receives an email notification, by using the number of password days remaining.	3w,2w,1w,5d,3d,2d,1d
Expiration.Notification.Enabled	Enables password expiration email notifications.	Enabled
DeviceManager.MaxDeviceActionsPerRequest	Maximum number of devices that can be applied in an action. This limits the number of devices that a user can select for actions in Device Manager. (This parameter does not apply to MultiSpeak functions.)	0 (this parameter is disabled by default)
ConnectDisconnect.ThrottlingDurationForDisconnectCommands	Sets the Service Switch > Disconnect action time length in hours.	0 (this parameter is disabled by default)
ConnectDisconnect.ScheduledDisconnectPastDaysAllowed	Maximum number of days in the past that the scheduled disconnect/reconnect can be scheduled. Enter 0 to disable this parameter. Negative numbers are not allowed.	1
ConnectDisconnect.ScheduledDisconnectFutureDaysAllowed	Maximum number of days in the future that the scheduled disconnect/reconnect can be scheduled. Enter 0 to disable this parameter. Negative numbers are not allowed.	7
ConnectDisconnect.MaxDevicesScheduledDisconnectAndDemandReset	Maximum number of devices that can be applied in Schedule Disconnect Reconnect and Demand Reset actions. Enter 0 to disable this parameter. Negative numbers are not allowed.	10000
Communications > Stale sub-filter		

Configuration Key	Description	System Default Settings
StaleMeterDetection.StartTime	Start Time for the stale meter detection process on any given day. A time of 00:00:00 would re-initiate the process every Midnight and run the stale-detection zero or more times based on RepeatInterval. Format: hh:mm:ss Range: 00:00:00 to 23:59:59	00:00:00
StaleMeterDetection.RepeatInterval	Repeat frequency (in hours) for the stale detection process on any given day. A value of 4 enables stale-detection to run every four hours, depending on OperationDays and OperationHours.	4
StaleMeterDetection.OperationHours	If this configuration is specified, the stale detection job is only run during the hours defined by this configuration. For example, 8-12: means the job will be run between 8:00AM and 12:00PM.	All
StaleMeterDetection.OperationDays	If this configuration is specified, the stale detection job will only run on the days defined by this configuration. For example, MON-FRI: means the job will be run from Monday to Friday. MON,WED: means the job will only be run on Monday and Wednesday.	All
StaleMeterDetection.MinDuration	Configuration for the stale time window (in hours). A value of 8 means that any meter missing reads for the last eight or more hours to the value of <StalemeterDetection.MaxDuration> hours are included.	12
StaleMeterDetection.MaxPing AttemptsPerDay	If not empty, this configuration can be used to limit the number of stale pings to the meter. If the value is set to 3, a maximum of only 3 stale pings will be sent to the meter on any given day.	6
StaleMeterDetection.MaxDuration	Configuration for the stale time window (in hours). A value of 36 means any meter missing reads for the last <StaleMeterDetection.MinDuration> hours to 36 hours will be included. Range: 0 to 36	24
StaleMeterDetection.Enabled	Enable or disable the stale meter detection background process. Selections: True, False	False
Communications > Twoway sub-filter		
twoway.timeping.TxMsgPriority	Specifies the transmit priority level of the time ping command.	15
twoway.timeping.BatchPriority	Specifies the batch priority level of the time ping command.	6
twoway.loadprofile.TxMsgPriority	Specifies the transmit priority level of the load profile command.	13
twoway.backfill.TxMsgPriority	Specifies the transmit priority level of the backfill command.	13

Configuration Key	Description	System Default Settings
Communications > CommStats sub-filter		
CommStats.NumOfDays	Number of days to include in the etl_rf_facts run (going back from local midnight).	30
CommStats.ETLLookBackDays	System-wide setting only; customer level will be ignored. Set number of days to look back for late arriving data.	2
CommStats.Batches	Number of batches used in the etl_rf_facts run.	1

Configuration parameters - RNI filter

Configuration Key	Description	System Default Settings
RNI > General sub-filter		
web.routeanalyzer.priority.highest	Base station priority to use when Highest is selected in Route Analyzer.	7
web.routeanalyzer.mapping.showmaps	Indicates whether mapping should be used by the Route Analyzer. Selections: True, False	False
RateCodeToggle.Enabled	Only applicable to electric meters. Show the Rate Code toggle in the Latest Reads, Load Profile, Snapshot Data, and TOU tabs. Selections: True, False	False
EnableConfigLogForWaterMDM	Create a value for RNI/RNI and set to True if MDM 2.29 or older is in use. Selections: True, False	False
DefaultUSTZ	Default time zone for the customer.	274
DefaultQuadrant	Quadrant to validate latitude/longitude sign. 0 is off, 1 is +/- (North and West), 2 is +/+ (North and East), 3 is -/+ (South and East), and 4 is -/- (South and West).	0
DefaultFollowsDST	Default indicator of whether or not to apply daylight savings time. Selections: True, False	True
DefaultCustomerId	Default customer ID for the RNI.	<customerid>
RNI > Database sub-filter		
web.sql.ScaleReadDigits	Indicates whether to modify the number of digits in a read based on the fldDials setting in tblMeterMaint. Selections: True, False	True
web.sql.RequireconfigToDisplay	Indicates whether Setup/Bind message should have been received to display on the web. Selections: True, False	False
web.sql.MeasurementResolution-W	Indicates whether MeasurementResolution needs to be used for Water meters to display on the web. Selections: True, False	False

Configuration Key	Description	System Default Settings
web.sql.MeasurementResolution-G	Indicates whether MeasurementResolution needs to be used for Gas meters to display on the web. Selections: True, False	False
web.sql.DisplayUnregisteredMeters	Whether to display meters that have setup or binding information but no row in tblMeterMaint. Selections: True, False	False
RetentionDays	Number of days to retain data. No rows should be autopurged short of this limit.	60
fldCityCase	Controls the alphabetic case in which city data will be stored in the database. Selections: INITCAP, LOWER, NONE, UPPER	NONE
endpoint_info.MaxRowCount	Row limit for full count.  Note: Setting to -ve value or very large will impact performance.	100000
DBPartition.MSSQL.ShrinkFiles	Shrink MSSQL Database Future Partition files to default size. Selections: True, False	False
DBPartition.MSSQL.FuturePartitionDays	Creates Future Partition Days based on the value.	10
RNI > Security sub-filter		
KeyManagement.Passphrase.MinUpper CaseChars  Note: All KeyManagement.Passphrase parameters are RNI system-wide settings. They are not configurable on a tenant/customer level.	Minimum number of uppercase characters for the passphrase when generating an encryption file with Key Management.	1
KeyManagement.Passphrase.Min SpecialChars	Minimum number of special characters for the passphrase when generating an encryption file with Key Management.	1
KeyManagement.Passphrase.MinLower CaseChars	Minimum number of lowercase characters for the passphrase when generating an encryption file with Key Management.	1
KeyManagement.Passphrase.MinLength	Minimum password length when generating an encryption file with Key Management.	12
KeyManagement.Passphrase.MinDigits Chars	Minimum number of digits for the passphrase when generating an encryption file with Key Management.	1
KeyManagement.MaximumKey PerRequest	Maximum number of keys allowed per request for a given customer.	-1
crypto.UniqueKeyRotationPeriodDays	The number of days between unique key rotations (0 = do not rotate).	0

Configuration Key	Description	System Default Settings
crypto.SharedKeyRotationPeriodDays	The number of days between shared key rotations (0 = do not rotate).	0
crypto.Na2wDefineOldRecordsIn Minutes	How often to retry encryption action for NA2W devices (indicates the the number of minutes between retries).	4320
crypto.GetEncryptedMeterKeys	If set to True, the RNI will attempt to retrieve endpoint keys from the Central Key Server when meters are installed. Selections: True, False	False
crypto.ExtractKeyRotationPeriodHours	Specifies key rotation extraction period in hours.	0
crypto.EncryptByDefault	If set to True, all encryption-enabled endpoints will be scheduled for encryption. Selections: True, False	False
crypto.ElectricDefineOldRecordsIn Minutes	How often (in minutes) to retry encryption action for FlexNet V1 electric devices.	15
crypto.AsymmetricDefineOldRecordsIn Minutes	How often (in minutes) to retry encryption action for FlexType 1 devices. FlexType 1 applies to North American line-powered devices.	15
crypto.AllowUniqueKeyRotation	Specifies whether unique key rotation is allowed.	True
crypto.AllowKeyExtraction	Specifies whether key extraction is allowed.	False
RNI > Logging sub-filter		
LOGGING_LEVEL	Maximum error level to save in the error_log table.	2
ErrLogging.PostReadData.Level	The level of errors to report in the error_log table. Selections: -1 none, 0 fatal, 1 error, 2-4 warnings	-1

Key Management tab

The **Key Management** tab generates encryption keys that enable the FlexNet Utility to communicate with a meter.

Use the **Key Management** tab to create and download an encrypted file of endpoint encryption keys for use by the FlexNet Utility or other compatible methods.

Software
Configuration
Users

Customers
Networks
Sub-Networks
Configuration
Key Management

Generate Encryption File

Upload IDs

ID Type:
FlexNetId

FlexNet/Meter ID File:
Choose File
No file chosen
Upload a comma delimited file containing ID's

or copy and paste one or many comma delimited ID's in the field below

Passphrase:

Re-enter Passphrase:

Submit

ID Type

Specify the type of IDs you are using in your request – FlexNet IDs or Meter IDs.

FlexNet/Meter ID File

Browse your computer for a comma-delimited file containing the FlexNet IDs or Meter IDs.

ID Text Field

As an alternative to importing a comma-delimited ID file, you can paste one or more IDs into this field. Multiple IDs must be separated by commas.

Passphrase

Enter the password to use to protect the created file. This password needs to be entered when accessing the file upon use.

Re-enter Passphrase

This entry must match the original Passphrase entry.

Submit

To create and download an encrypted file of endpoint encryption keys for the endpoints selected, select **Submit**.

7 System Administration Users menu

Using the tabs on the **Users** menu, you can manage users, roles and permissions, and passwords.

The following default user accounts are created during the RNI installation process:

- guestAdmin
- cpService
- gatewayUser



Note: See [User roles](#) for a complete list of default user roles that are available upon system installation.

Users tab

Use the **Users** tab to add, edit, and delete users.

The Users page lists the user ID, the user's name, the customer to which the user belongs, the user's email, the roles assigned to the user, the date the user last changed their password, the date the user's password will expire, how many days remain until the user's password expires, and whether the user is a service account (an RNI-managed non-human service used to log in the RNI).

As a system administrator, you have permission to manage users. Your view contains a column on the right side of the page that enables you to delete users.

Software Configuration Users SentryPoint Users										
Users Roles Password Management										
Add User Export										
User ID	Name	Customer	Email	Password Changed Date	Password Expiration Date	Days Left until Password Expiration	Roles	Service Account	Filter	
acmeadmin	Acme Customer	ACME		October 3, 2023				<input type="checkbox"/>	Delete	
actionGuideUser	Action Guide	ACME	Action.Guide@fakemail.com	October 3, 2023	January 1, 2024	83	ACTION_GUIDE	<input type="checkbox"/>	Delete	
admin	admin admin	ACME	admin.admin@fakemail.com	October 3, 2023	January 1, 2024	83	DM_ADMIN, DM_SERVICE_ELECTRIC, DM_SERVICE_GAS, DM_SERVICE_WATER	<input type="checkbox"/>	Delete	
Automation	Auto Motion	ACME	Auto.Motion@fakemail.com	October 3, 2023	January 1, 2024	83	CATHODIC_ADMIN, DM_ADMIN, DM_SERVICE_ELECTRIC, DM_SERVICE_GAS, DM_SERVICE_WATER, FWDL, FWDL_ADMIN, NMS_ADMIN, PERFORM_CONFIG_DL, PERFORM_TOU_CONFIG, SCHEDULE_ADMIN, SERVICE_BATCH_VIEWER, SERVICE_CATHODIC, SERVICE_CONFIG_DL, SERVICE_FWDL, SERVICE_NETWORK_METRICS, SERVICE_NMS, SERVICE_REPORT_GEN, SERVICE_SCHEDULER, SERVICE_SYSTEM_ADMIN, SERVICE_TOU_CONFIG, SYSTEM_ADMIN	<input type="checkbox"/>	Delete	

Add or edit a user

Use this procedure to update user information.

1. Select **Add User** to create a new user, or select a specific user ID to edit an existing user.



Note: In order for a user to access a specific application, the applicable service roles must be assigned to that user. For example, to access and manage electric meters, a user must be assigned SERVICE_SYSTEM_ADMIN and DM_SERVICE_ELECTRIC roles.

The **Create User** or **Edit User** page displays.

Edit "testUser"

Use the inputs below to edit User. Enter all ***Required** information.

[«Back to User List](#)

First Name:*

Last Name:*

User ID:*

Email:*

Service Account:☐

[Change Password](#)

Customers:

Select Customer(s)
ACME

Password Policy:

Select Policy
ACME
default
special

Multi-Factor Authentication

Customer	Status	Action to take
ACME	Enrolled	<input checked="" type="radio"/> None <input type="radio"/> Disable <input type="radio"/> Reset

Add User Role(s)

Current Roles

DM_SERVICE_ELECTRIC

DM_SERVICE_GAS

DM_SERVICE_WATER

SERVICE_SYSTEM_ADMIN

Add Roles

ACTION_GUIDE

CATHODIC_ADMIN

CATHODIC_USER

CATHODIC_VIEWER

2. Enter all required information: **First Name**, **Last Name**, **User ID**, and **Email**.
3. If the user is a service account—an RNI-managed non-human service used to log in in the RNI—select the **Service Account** option.



Note: Service accounts do not support multi-factor authentication (MFA).

4. To assign or change a password for the user, select **Create Password** or **Change Password**.
5. Enter the new password, and then re-enter it to confirm it.
6. Select the customers to which the user belongs. The **Customers** field lists the current customer RNIs to which the administrator has access.
7. Select the appropriate **Password Policy** from the list.



Note: For a Service Account user, select the `CUSTOMER_SERVICE` password policy. See [Password management for service accounts](#) on page 90 for details about the password policy for service accounts.

8. Choose to enable or disable **Multi-Factor Authentication** for a new user by selecting **Disable** to disable (default action) or **Enable** to use multi-factor

authentication for this user. The options for editing a user are **None** to disable and **Enable** to enable MFA.



Note: For existing users, MFA can be enabled by a System Administrator. The following roles can manage MFA: SYSTEM_ADMIN, DM_SYSTEM_OPERATOR, TENANT_ADMIN, and USER_ADMIN.

- Under **Add User Roles**, select the Add icon for each role to assign to the user.



Note: A user with the role of TENANT_ADMIN cannot edit the privileges of a SYSTEM_ADMIN user, cannot create a SYSTEM_ADMIN user, and cannot give system administrator privileges to themselves or to another tenant.

- After roles have been assigned and are displayed under **Current Roles**, select the Delete icon next to any role you want to delete.
- To save changes, select **Create User** or **Save User**.
- To cancel the changes and return to the **Users** tab, select **Cancel**.

Delete a user

Use this procedure to delete a user from the RNI system software.

- From the **Users** menu, select the **Users** tab.
A list of all RNI system users and their associated information displays.

Software Configuration Users SentryPoint Users										
Users Roles Password Management										
Add User Export										
User ID	Name	Customer	Email	Password Changed Date	Password Expiration Date	Days Left until Password Expiration	Roles	Service Account	Filter	
acmeadmin	Acme Customer	ACME		October 3, 2023				<input type="checkbox"/>		
actionGuideUser	Action Guide	ACME	Action Guide@fakemail.com	October 3, 2023	January 1, 2024	83	ACTION_GUIDE	<input type="checkbox"/>		
admin	admin admin	ACME	admin.admin@fakemail.com	October 3, 2023	January 1, 2024	83	DM_ADMIN, DM_SERVICE_ELECTRIC, DM_SERVICE_GAS, DM_SERVICE_WATER	<input type="checkbox"/>		
Automation	Auto Motion	ACME	Auto.Motion@fakemail.com	October 3, 2023	January 1, 2024	83	CATHODIC_ADMIN, DM_ADMIN, DM_SERVICE_ELECTRIC, DM_SERVICE_GAS, DM_SERVICE_WATER, FLOW, FLOW_ADMIN, NMS_ADMIN, PERFORM_CONFIG_OIL, PERFORM_TOU_CONFIG, SCHEDULE_ADMIN, SERVICE_BATCH_VIEWER, SERVICE_CATHODIC, SERVICE_CONFIG_OIL, SERVICE_FLOW, SERVICE_NETWORK_METRICS, SERVICE_NMS, SERVICE_REPORT_GEN, SERVICE_SCHEDULER, SERVICE_SYSTEM_ADMIN, SERVICE_TOU_CONFIG, SYSTEM_ADMIN	<input type="checkbox"/>		

- Scroll through the list of users until you locate the user to delete.

systemb	system billing	ACME	system.billing@fakemail.com	October 3, 2023	January 1, 2024	83	DM_BILLING_MANAGER, SERVICE_SYSTEM_ADMIN	<input type="checkbox"/>		
systemc	system customer	ACME	system.customer@fakemail.com	October 3, 2023	January 1, 2024	83	DM_CUSTOMER_SUPPORT, SERVICE_SYSTEM_ADMIN	<input type="checkbox"/>		
systems	system system	ACME	system.system@fakemail.com	October 3, 2023	January 1, 2024	83	DM_SYSTEM_OPERATOR, SERVICE_SYSTEM_ADMIN	<input type="checkbox"/>		
testUser	Test User	ACME	testuser@fakemail.com	October 9, 2023	October 9, 2023	Won't Expire	DM_ADMIN, DM_SERVICE_ELECTRIC, DM_SERVICE_GAS, DM_SERVICE_WATER, DM_SYSTEM_OPERATOR, SERVICE_NETWORK_METRICS, SERVICE_SYSTEM_ADMIN, SERVICE_TOU_CONFIG	<input type="checkbox"/>		

- Select **Delete** in the row for the user you want to remove.
A message displays prompting you to confirm the deletion.

Confirm Delete

User "Test User" will be deleted from the system.

Delete

Cancel

- Select **Delete**, and the user is removed from the system.
- A *User deleted successfully* message displays at the top of the page.
Select **Close** to dismiss the message.

Filter the Users tab and export the results

The **Users** tab can be filtered by one or more columns in the table: User ID, Name, Customer, Email, Roles, and Service Account. After applying any filters, you can export the resulting list of users with their associated roles. If the list is not filtered, a list of all RNI users and their associated roles is displayed and can be exported.

Use the following process to filter the list of users for the RNI software, and to export the filtered list to a .csv file (Excel spreadsheet).

1. On the **Users** tab, select the **Filter** button. This displays a new row above the existing rows, where you can enter a value to use to filter each column in the table.



Note: For RNI versions 4.14 and later, three columns were added to the Users page: Password Changed Date, Password Expiration Date, and Days Left until Password Expiration. The purpose of these columns is to help administrators track users with passwords that are going to expire soon. You can use these new columns to sort the table entries.

Software Configuration Users SentryPoint Users										
Users Roles Password Management										
Add User Export										
User ID	Name	Customer	Email	Password Changed Date	Password Expiration Date	Days Left until Password Expiration	Roles	Service Account	Filter	
Search User ID	Search Name	Search Customer	Search Email				Search Roles		Reset	
acmeadmin	Acme Customer	ACME		October 3, 2023					Delete	
actionGuideUser	Action Guide	ACME	Action.Guide@fakemail.com	October 3, 2023	January 1, 2024	83	ACTION_GUIDE		Delete	
admin	admin admin	ACME	admin.admin@fakemail.com	October 3, 2023	January 1, 2024	83	DM_ADMIN, DM_SERVICE_ELECTRIC, DM_SERVICE_GAS, DM_SERVICE_WATER		Delete	
Automation	Auto Motion	ACME	Auto.Motion@fakemail.com	October 3, 2023	January 1, 2024	83	CATHODIC_ADMIN, DM_ADMIN, DM_SERVICE_ELECTRIC, DM_SERVICE_GAS, DM_SERVICE_WATER, FWDL, FWDL_ADMIN, NMS_ADMIN, PERFORM_CONFIG_DL, PERFORM_TOU_CONFIG, SCHEDULE_ADMIN, SERVICE_BATCH_VIEWER, SERVICE_CATHODIC, SERVICE_CONFIG_DL, SERVICE_FWDL, SERVICE_NETWORK_METRICS, SERVICE_NMS, SERVICE_REPORT_GEN, SERVICE_SCHEDULER, SERVICE_SYSTEM_ADMIN, SERVICE_TOU_CONFIG, SYSTEM_ADMIN		Delete	

2. Enter the value by which to filter one or more of the columns and click **Filter**. The list in the following example was filtered by the **ACTION_GUIDE** role.

Software Configuration Users SentryPoint Users										
Users Roles Password Management										
Add User Export										
User ID	Name	Customer	Email	Roles			Service Account		Filter	
Search User ID	Search Name	Search Customer	Search Email	ACTION_GUIDE					Reset	
actionGuideUser	Action Guide	ACME	Action.Guide@fakemail.com	ACTION_GUIDE					Delete	
guestAdmin	Guest Administrator	ACME	Guest.Administrator@fakemail.com	ACTION_GUIDE, CATHODIC_ADMIN, DM_ADMIN, DM_SERVICE_ELECTRIC, DM_SERVICE_GAS, DM_SERVICE_WATER, FWDL, FWDL_ADMIN, NMS_ADMIN, PERFORM_CONFIG_DL, PERFORM_TOU_CONFIG, SA_COMM_STATS, SCHEDULE_ADMIN, SERVICE_CATHODIC, SERVICE_CONFIG_DL, SERVICE_FWDL, SERVICE_NETWORK_METRICS, SERVICE_NMS, SERVICE_REPORT_GEN, SERVICE_SCHEDULER, SERVICE_SYSTEM_ADMIN, SERVICE_TOU_CONFIG, SYSTEM_ADMIN, MANAGE_SCHED_DISC						

3. To export the filtered list of users and their associated properties to an Excel spreadsheet, select **Export**.

The .csv file automatically downloads to your computer.

Roles tab

Use the **Roles** tab to create new roles, change the permissions for current roles, and delete user-defined roles.

All of the currently defined roles are listed in alphabetical order. When you select a role, the system lists the users who are currently assigned to that role, and it shows the permissions associated with the role.

The screenshot shows the 'Roles' tab in a system administration interface. At the top, there are tabs for 'Software', 'Configuration', and 'Users'. Below these, there are sub-tabs for 'Users', 'Roles', and 'Password Management'. The 'Roles' sub-tab is active. On the left, there is a list of roles: 'CATHODIC_ADMIN' (highlighted), 'CATHODIC_USER', 'CATHODIC_VIEWER', 'DM_ADMIN', 'DM_BILLING_MANAGER', 'DM_CUSTOMER_SUPPORT', 'DM_SERVICE_ELECTRIC', 'DM_SERVICE_FWDL', 'DM_SERVICE_GAS', 'DM_SERVICE_SYSTEM_ADMIN', 'DM_SERVICE_WATER', 'DM_SYSTEM_OPERATOR', 'FWDL', 'FWDL_ADMIN', and 'FWDL_VIEWER'. On the right, there are fields for 'Role' (containing 'CATHODIC_ADMIN') and 'Description' (containing 'Cathodic Administrator'). Below these, there is a section for 'Users' showing two users: 'Glaucielly De Santi' and 'Guest Administrator', each with a red 'X' icon. At the bottom, there is a 'Permissions' section with three checkboxes: 'View/ export device list & device detail', 'View system-wide data: Alerts tab, reports', and 'View device firmware download job status'.

Add a custom role

1. To add a new role, select the **Add** button at the top of the page.
2. Enter a name and a description for the role.
3. Select the customer for the role.
4. Specify permissions for the selected role.
5. Select **Save** to save your changes, or choose **Cancel** to exit without saving.

Assign users to a new role

1. To assign users to a new role, go to the **Users** tab.
2. Click the **User ID** for the user.
3. On the **Edit** page that opens, add the role.
4. Select **Save User**.

Delete a role



Note: You can only delete user-defined roles. System roles cannot be deleted.

1. To delete a user-defined role, select the role from the list on the **Roles** page.
2. Select **Delete** and a **Confirm Delete** prompt opens.
3. Click the **Delete** button on the prompt, and a *Role deleted successfully* message displays at the top of the page.

User roles

Role name	Associated permissions	Role description
ACTION_GUIDE	Modify radio configuration over-the-air	Provides access to the Action Guide REST service in the RNI API Engine. This service connects the Sensus RNI to Sensus Analytics applications and is generally configured during setup by Sensus when that product is ordered. This allows the upstream application access to NA2W stats, firmware download, and endpoint information. This interface is not used by any other system and is not intended to interface with end customer systems. The Modify radio configuration over-the-air permission is for the Sensus Analytics Pressure Profile application and it is used to remove water pressure sensor thresholds.
CATHODIC_ADMIN	Open the SentryPoint application, manage groups, edit devices, export (hard-coded)	Cathodic Administrator
CATHODIC_USER	Open the SentryPoint application, edit devices (hard-coded)	Cathodic User
CATHODIC_VIEWER	Open the SentryPoint application, view devices with specific permissions granted to this role (hard-coded)	Cathodic Viewer
DM_ADMIN	<div>View and export device list and device detail</div> <div>View system-wide data: Alerts tab and reports</div> <div>View device firmware download (FWDL) job status</div> <div>View system-wide settings</div> <div>Modify radio configuration over-the-air</div> <div>Modify sensor configuration over-the-air</div> <div>Initiate demand response events</div> <div>Initiate demand reset events</div> <div>Initiate service switch operations</div> <div>Initiate endpoint pings</div> <div>Initiate device import</div> <div>Initiate device FWDL</div> <div>Edit system-wide behavior parameters</div> <div>Clear alarms and configure smart alarms</div> <div>Modify HAN devices and FlexNet Load Control Module (LCM) relays</div>	Device Manager Administrator. This role must be paired with one of the services for electric, gas, or water.

Role name	Associated permissions	Role description
DM_ADMIN (continued)	Add, edit, and delete base station records Modify device lifecycle state Modify device operational mode Enable, disable, and suspend device encryption Create and edit groups and tags	Device Manager Administrator. This role must be paired with one of the services for electric, gas, or water.
	Manage MultiSpeak dynamic registration Create and edit user information within a tenant Modify DB attributes of a device Manage job execution and lifecycle in scheduler Add a new meter in the RNI	
	Start usage monitoring for a meter Arm a meter for connect Perform a billing ping Clear meter alarms Configure and cancel load limit Delete a meter from the RNI	
	Stop usage monitoring for a meter Perform and cancel a demand reset Disconnect power for the meter	
	Set up, initiate, and cancel demand response events Manage dynamic registration Get a meter record from the RNI Get meter readings from the RNI Get system configurations for the RNI	
	Join, leave, and commission HAN devices Create and delete HAN devices Send and cancel display messages to HAN devices Configure meters Change a meter's lifecycle information	
	Reconnect power for the meter Ping (on-air message) a meter for status Set remote shutoff valve to trickle Update an existing meter in the RNI Create and edit group types	


Role name	Associated permissions	Role description
DM_ADMIN (continued)	Configure reading units and resolution Access experimental features Perform key management and generate encryption files Enable, disable, and configure shutoff alarms Shut off valve Control the display of sub 1hr MSR Synchronize meter and related data from the Customer Billing system to the RNI Change alert severity	Device Manager Administrator. This role must be paired with one of the services for electric, gas, or water.
DM_BILLING_MANAGER	View and export device list and device detail View system-wide data: Alerts tab and reports Create and edit groups and tags	Device Manager Billing Manager
DM_CUSTOMER_SUPPORT	View and export device list and device detail View system-wide data: Alerts tab and reports Create and edit groups and tags	Device Manager Customer Support
DM_SERVICE_ELECTRIC	Not Applicable*	Enables access to the Device Manager Electric application. It controls the display of the Manage Electric icon on the Sensus Launch Pad.
DM_SERVICE_GAS	Not Applicable*	Enables access to the Device Manager Gas application. It controls the display of the Manage Gas icon on the Sensus Launch Pad.
DM_SERVICE_WATER	Not Applicable*	Enables access to the Device Manager Water application. It controls the display of the Manage Water icon on the Sensus Launch Pad.
DM_SYSTEM_OPERATOR	View and export device list and device detail View system-wide data: Alerts tab and reports View device FWDL job status View system-wide settings Modify radio configuration over-the-air Modify sensor configuration over-the-air Initiate demand response events Initiate demand reset events Initiate service switch operations Initiate endpoint pings	Device Manager System Operator

Role name	Associated permissions	Role description
DM_SYSTEM_OPERATOR (continued)	Initiate device import Initiate device FWDL Clear alarms and configure smart alarms Modify HAN devices and FlexNet LCM relays Add, edit, and delete base station records	Device Manager System Operator
	Modify device lifecycle state Modify device operational mode Enable, disable, and suspend device encryption Create and edit groups and tags Manage MultiSpeak dynamic registration	
	Create and edit user information within a tenant Modify DB attributes of a device Manage job execution and lifecycle in scheduler Add a new meter in the RNI Start usage monitoring for a meter	
	Arm a meter for connect Clear meter alarms Configure and cancel load limit Delete a meter from the RNI	
	Stop usage monitoring for a meter Perform a demand reset Cancel a demand reset Disconnect power for the meter Set up, initiate, and cancel demand response events	
	Manage dynamic registration Get a meter record from the RNI Get meter readings from the RNI Get system configurations for the RNI Join, leave, and commission HAN devices	
	Create and delete HAN devices Send and cancel display messages to HAN devices Configure meters Change a meter's lifecycle information Reconnect power for the meter	
	Ping (on-air message) a meter for status Set remote shutoff valve to trickle Update an existing meter in the RNI Create and edit group types Configure reading units and resolution	

Role name	Associated permissions	Role description
DM_SYSTEM_OPERATOR (continued)	Access experimental features Perform key management and generate encryption files Enable, disable, and configure shutoff alarms Shut off valve Control the display of sub 1hr MSR	Device Manager System Operator
FWDL	Not Applicable*	Required role for FWDL_ADMIN and FWDL_VIEWER roles. This role is used in conjunction with the SERVICE_FWDL role to perform firmware downloads in the Firmware Download (FWDL) application on the Sensus Launch Pad. This application manages NA2W FWDL and Electric FWDL.
FWDL_ADMIN	View device FWDL job status Initiate device FWDL	FWDL Administrator; this role must be paired with FWDL service.
FWDL_VIEWER	View device FWDL job status	FWDL Viewer
GATEWAY	<div>Modify device operational mode</div> <div>Create and edit groups and tags</div> <div>Add a new meter in the RNI</div> <div>Start usage monitoring for a meter</div> <div>Arm a meter for connect</div> <div>Perform a billing ping</div> <div>Clear meter alarms</div> <div>Configure and cancel load limit</div> <div>Delete a meter from the RNI</div> <div>Stop usage monitoring for a meter</div> <div>Perform and cancel a demand reset</div> <div>Disconnect power for the meter</div> <div>Set up, initiate, and cancel demand response events</div> <div>Manage dynamic registration</div> <div>Get a meter record from the RNI</div> <div>Get meter readings from the RNI</div> <div>Get system configurations for the RNI</div> <div>Join, leave, and commission HAN devices</div> <div>Create and delete HAN devices</div> <div>Send and cancel display messages to HAN devices</div> <div>Configure meters</div> <div>Change a meter's lifecycle information</div> <div>Reconnect power for the meter</div> <div>Ping (on-air message) a meter for status</div> <div>Set remote shutoff valve to trickle</div>	Used for access to MultiSpeak. Not a GUI access role.

Role name	Associated permissions	Role description
GATEWAY (continued)	Update an existing meter in the RNI Enable, disable, and configure shutoff alarms Shut off valve Synchronize meter and related data from the Customer Billing system to the RNI Manage broadcast groups View broadcast group information	Used for access to MultiSpeak. Not a GUI access role.
METER_SHOP_TECHNICIAN	<div>View and export device list and device detail</div> <div>View system-wide data: Alerts tab, reports</div> <div>View device firmware download job status</div> <div>View system-wide settings</div> <div> Modify radio configuration Over-The-Air Modify Sensor configuration Over-The-Air </div> <div> Initiate Demand Response events Initiate Demand Reset events Initiate Service Switch operations Initiate endpoint Pings Initiate device import Initiate device firmware download </div> <div> Clear alarms, configure smart alarms Modify HAN devices and FlexNet LCM relays Modify device life cycle state Modify device Operational Mode Enable, Disable, and Suspend Device Encryption </div> <div> Create and Edit groups and tags Modify DB attributes of a device Add a new meter into the RNI Start usage monitoring for a meter Perform a Billing Ping </div> <div> Clear meter alarms Delete a meter from the RNI Stop usage monitoring for a meter Perform a Demand Reset Cancel a Demand Reset </div> <div> Disconnect power for the meter Setup, initiate, and cancel Demand Response events Get a meter record from the RNI Get meter readings from the RNI </div>	Meter shop technician. Enables access typically required for the meter shop. Meter shop staff need to download meter keys for the field technicians to service FNV2 meters, but do not need access to other admin functions in the System Administration application. This role provides only the specific permissions needed, without including additional admin functions.

Role name	Associated permissions	Role description
METER_SHOP_TECHNICIAN (continued)	Join, leave, and commission HAN devices Create and delete HAN devices Send and cancel display messages to HAN devices Configure Meters Change a meter's lifecycle information Reconnect power for the meter Ping (on-air message) a meter for status Set remote shutoff valve to trickle Update an existing meter in the RNI Create and Edit group types Configure Reading Units and Resolution Key management, generate encryption files Remote Deactivation Enable, disable, and configure shutoff alarms Shutoff valve	Meter shop technician. Enables access typically required for the meter shop. Meter shop staff need to download meter keys for the field technicians to service FNV2 meters, but do not need access to other admin functions in the System Administration application. This role provides only the specific permissions needed, without including additional admin functions.
NETMET_READ_ONLY	This role can only view data within Network Metrics and manage sets. This role cannot create or delete alarms, base stations, radios, frequency mappings, or soft alarms.	<ul style="list-style-type: none"> VIEW_RADIOS VIEW_DEVICES VIEW_ALARMS VIEW_SYS_HISTORY VIEW_TOWERS VIEW_SYS_PREFS VIEW_FREQUENCY_MAPPINGS VIEW_USERS VIEW_METRICS
NETMET_CORE	This role can only view data within the Network Metrics application. Includes all the permissions of the NETMET_READ_ONLY role. This role can also download CSV files, create soft alarms, and manage alarms.	All the permissions of the NETMET_READ_ONLY role plus: <ul style="list-style-type: none"> MANAGE_ALARMS MANAGE_DEVICES MANAGE_TOWERS MANAGE_RADIOS MANAGE_ALARMS MANAGE_DEVICES MANAGE_TOWERS MANAGE_RADIOS

Role name	Associated permissions	Role description
NETMET_ADMIN	Includes all the permissions necessary for performing administrative activities in Network Metrics.  Note: Deleting towers or radios from within the Network Metrics application does not remove them from the RNI—only from Network Metrics.	All the permissions of the NETMET_CORE role plus: <ul style="list-style-type: none">• MANAGE_FREQUENCY_MAPPINGS• DELETE_TOWERS• DELETE_RADIOS
NMS_ADMIN	Not Applicable*	NMS Administrator
NMS_USER	Not Applicable*	NMS User
NOTIF_SUBSCRIPTION_MANAGEMENT	Not Applicable*	Used for the MultiSpeak Interface, not a GUI role. Authenticates the MultiSpeak and RNI API to access the Notifications service (for example, Subscribe and Unsubscribe).
PERFORM_CONFIG_DL	Not Applicable*	Meter Configuration Download Administrator. Enables the user to perform configuration download.
PERFORM_TOU_CONFIG	Not Applicable*	TOU Configuration Administrator. Provides access to the TOU (Time of Use) Configurator application for Electric Device Manager.
SA_COMM_STATS	Modify radio configuration over-the-air	Enables access to communication statistics for NA2W endpoints from the RNI API. The Modify radio configuration over-the-air permission is for the Sensus Analytics Pressure Profile application and it is used to remove water pressure sensor thresholds.
SCHEDULE_ADMIN	Not Applicable*	Scheduler Administrator. Enables access to the Scheduler application. Membership in this role confirms Admin status and conditionally enables actions in the application. Scheduler is an advanced application that enables an Administrator to schedule autonomous actions (for example, Scheduled Reports).
SCHEDULE_VIEWER	Not Applicable*	Scheduler Viewer. This role enables access to the Scheduler application with view-only permissions. A user can view the scheduled jobs, but not create, update, or delete any scheduled jobs.

Role name	Associated permissions	Role description
SCS_PROXY_USER	Not Applicable*	Enables access to the Secure Command Server application.
SERVICE_AMC	Not Applicable*	Provides access to the Advanced Meter Config application on the Sensus Launch Pad. This is a Sensus Professional Services application available for specific Device Types (DT-23 and DT-50).
SERVICE_BATCH_VIEWER	Not Applicable*	Enables access to the Batch Job Viewer (Available to internal Sensus personnel only)
SERVICE_CATHODIC	Not Applicable*	Enables access to the Cathodic Protection application (SentryPoint). It controls the display of the SentryPoint icon under Solution Applications on the Launch Pad.
SERVICE_CONFIG_DL	Not Applicable*	Enables access to the Configuration Download application. It controls the display of the Configuration Download icon under on the Sensus Launch Pad.
SERVICE_FWDL	Not Applicable*	Enables access to the Firmware Download icon on the Sensus Launch Pad.
SERVICE_NETWORK_METRICS	Not Applicable*	Enables access to the Network Metrics application. It controls the display of the Network Metrics icon under RF Network Management on the Sensus Launch Pad. This role should be coupled with one of the other Network Metrics roles for specific access levels within Network Metrics.
SERVICE_NMS	Not Applicable*	Enables access to Network Management System. Must be set to access the Network Management application if the application is installed.
SERVICE_REPORT_GEN	Not Applicable*	Enables access to Report Generator. Must be set to access the Report Generator application.
SERVICE_SCHEDULER	Not Applicable*	Enables access to Scheduler. Must be set to access the Scheduler application.

Role name	Associated permissions	Role description
SERVICE_SYSTEM_ADMIN	Not Applicable*	Enables access to the System Administration application under RNI Management on the Sensus Launch Pad. This role must be paired with a functional role assignment, such as DM_SERVICE_WATER, which enables the user to view the Manage Water icon on the Sensus Launch Pad. This enables an Admin user to have administrative level access to that functional role.
SERVICE_TOU_CONFIG	Not Applicable*	Enables access to the TOU Configurator application. It controls the display of the TOU Configurator icon under Download Configuration on the Sensus Launch Pad.
SYSTEM_ADMIN	Edit system-wide behavior parameters Create and edit tenants and tenant user admins Create and edit user information within a tenant Perform key management and generate encryption files Manage the maximum number of devices that can be included in an action Synchronize meter and related data from the Customer Billing system to the RNI	System Administrator; this role must be set to the administrator of the system and must be paired with other service roles.
TENANT_ADMIN	View and export device list and device detail View system-wide data: Alerts tab and reports View device FWDL job status View system-wide settings Modify radio configuration over-the-air <hr/> Modify sensor configuration over-the-air Initiate demand response events Initiate demand reset events Initiate service switch operations Initiate endpoint pings <hr/> Initiate device import Initiate device FWDL Edit system-wide behavior parameters Clear alarms and configure smart alarms Modify HAN devices and FlexNet LCM relays	Tenant Administrator; this role is intended to manage access for users at a tenant level.

Role name	Associated permissions	Role description
TENANT_ADMIN (continued)	<div> Add, edit, and delete base station records Modify device lifecycle state Modify device operational mode Enable, disable, and suspend device encryption Create and edit groups and tags </div> <div> Manage MultiSpeak dynamic registration Create and edit user information within a tenant Modify DB attributes of a device Manage job execution and lifecycle in scheduler Add a new meter in the RNI </div> <div> Start usage monitoring for a meter Arm a meter for connect Perform a billing ping Clear meter alarms Configure and cancel load limit Delete a meter from the RNI </div> <div> Stop usage monitoring for a meter Perform and cancel a demand reset Disconnect power for the meter Set up, initiate, and cancel demand response events </div> <div> Manage dynamic registration Get a meter record from the RNI Get meter readings from the RNI Get system configurations for the RNI Join, leave, and commission HAN devices </div> <div> Create and delete HAN devices Send and cancel display messages to HAN devices Configure meters Change a meter's lifecycle information Reconnect power for the meter </div> <div> Ping (on-air message) a meter for status Set remote shutoff valve to trickle Update an existing meter in the RNI Create and edit group types Configure reading units and resolution </div>	Tenant Administrator; this role is intended to manage access for users at a tenant level.

Role name	Associated permissions	Role description
TENANT_ADMIN (continued)	Access experimental features Perform key management and generate encryption files Enable, disable, and configure shutoff alarms Shut off valve Manage the maximum number of devices that can be included in an action Control the display of sub 1hr MSR Synchronize meter and related data from the Customer Billing system to the RNI	Tenant Administrator; this role is intended to manage access for users at a tenant level.
USER_ADMIN	Create and edit user information within a tenant	User Administrator

*Not Applicable – Permission is hard-coded

System permissions

The following table contains each permission and its associated roles.

Permission name	Detailed definition (if needed)	Associated roles
View and export device list and device detail		DM_ADMIN DM_BILLING_MANAGER DM_CUSTOMER_SUPPORT DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
View system-wide data: Alerts tab and reports		DM_ADMIN DM_BILLING_MANAGER DM_CUSTOMER_SUPPORT DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
View device firmware download (FWDL) job status		DM_ADMIN DM_SYSTEM_OPERATOR FWDL_ADMIN FWDL_VIEWER METER_SHOP_TECHNICIAN TENANT_ADMIN
View system-wide settings		DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
Modify radio configuration over-the-air		ACTION_GUIDE DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN SA_COMM_STATS TENANT_ADMIN


Permission name	Detailed definition (if needed)	Associated roles
Modify sensor configuration over-the-air		DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
Initiate demand response events		DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
Initiate demand reset events		DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
Initiate service switch operations		DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
Initiate endpoint pings		DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
Initiate device import		DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
Initiate device firmware download		DM_ADMIN DM_SYSTEM_OPERATOR FWDL_ADMIN METER_SHOP_TECHNICIAN TENANT_ADMIN
Edit system-wide behavior parameters		DM_ADMIN SYSTEM_ADMIN TENANT_ADMIN
Clear alarms and configure smart alarms		DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
Modify HAN devices and FlexNet Load Control Module (LCM) relays		DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
Add, edit, and delete base station records		DM_ADMIN DM_SYSTEM_OPERATOR TENANT_ADMIN

Permission name	Detailed definition (if needed)	Associated roles
Modify device lifecycle state		DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
Modify device operational mode		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Enable, disable, and suspend device encryption		DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
Create and edit groups and tags		DM_ADMIN DM_BILLING_MANAGER DM_CUSTOMER_SUPPORT DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Manage MultiSpeak dynamic registration		DM_ADMIN DM_SYSTEM_OPERATOR TENANT_ADMIN
Create and edit user information within a tenant		DM_ADMIN DM_SYSTEM_OPERATOR SYSTEM_ADMIN TENANT_ADMIN USER_ADMIN
Create and edit tenants and tenant user admins		SYSTEM_ADMIN
Modify DB attributes of a device		DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
Manage job execution and lifecycle in scheduler		DM_ADMIN DM_SYSTEM_OPERATOR TENANT_ADMIN
Add a new meter in the RNI		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN

Permission name	Detailed definition (if needed)	Associated roles
Start usage monitoring for a meter		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Arm a meter for connect		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY TENANT_ADMIN
Perform a billing ping	Used in MultiSpeak. See section 2.1.1.2 of the <i>MultiSpeak v3.0 Meter Reading Integration Guide</i> for more details. This enables the user to initiate a meter reading by meterID via MultiSpeak.	DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Clear meter alarms		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Configure and cancel load limit		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY TENANT_ADMIN
Delete a meter from the RNI		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Stop usage monitoring for a meter		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Perform a demand reset		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Cancel a demand reset		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN

Permission name	Detailed definition (if needed)	Associated roles
Disconnect power for the meter		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Set up, initiate, and cancel demand response events		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Manage dynamic registration	Used in MultiSpeak. See the <i>MultiSpeak v4.1 Overview Integration Guide</i> and section 2.1.1.2 of the <i>MultiSpeak v4.1 Meter Reading Integration Guide</i> and for more details. This enables the MultiSpeak user to call the following methods: <ul style="list-style-type: none"> • RequestRegistrationID • RegisterForService • UnregisterForService • GetRegistrationInfoByID 	DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY TENANT_ADMIN
Get a meter record from the RNI	Used in MultiSpeak. See the MultiSpeak integration guide for more details. This is used to get meter reads from the database via the MultiSpeak interface. The "record" in this context is a returned row from the database structures.	DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Get meter readings from the RNI	Used in MultiSpeak. This permission applies to a collection of methods defined in section 2.1.1.2 of the <i>MultiSpeak v4.1 Meter Reading Integration Guide</i> .	DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Get system configurations for the RNI		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY TENANT_ADMIN
Join, leave, and commission HAN devices		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Create and delete HAN devices		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN

Permission name	Detailed definition (if needed)	Associated roles
Send and cancel display messages to HAN devices		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Configure meters		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Change a meter's lifecycle information		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Reconnect power for the meter		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Ping (on-air message) a meter for status		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Set remote shutoff valve to trickle		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Update an existing meter in the RNI	Used in MultiSpeak. See section 2.1.1.2 of the <i>MultiSpeak v4.1 Meter Reading Integration Guide</i> and for more details. This enables the MultiSpeak user to call the following methods: <ul style="list-style-type: none"> • MeterChangedNotification • ServiceLocationChanged Notification • MeterRemoveNotification • InitiateMeterExchange • InitiateMeterInstallation 	DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN NMS_USER PERFORM_TOU_CONFIG TENANT_ADMIN
Create and edit group types		CATHODIC_ADMIN DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN

Permission name	Detailed definition (if needed)	Associated roles
Configure reading units and resolution		DM_ADMIN DM_SYSTEM_OPERATOR METER_SHOP_TECHNICIAN TENANT_ADMIN
Debug information	Used in Device Manager when the user needs to see more details regarding any failed actions (listed in the Communication Summary dialog box).	Not assigned to any user roles by default. Exposes the <i>action criteria</i> used against a specific action that failed in Device Manager. For example, an installation audit command against a batch of devices failed for some devices. In this example, the criterion not met is Product Type (it was not 20), and therefore, the command did not pass. This information is listed in red in the Action Rules field.
Advanced Scheduled Events	Used in Electric Device Manager. It enables the user to schedule Advanced Events. This permission displays the Schedule Advanced Event button next to the Schedule Event button. Advanced Events are items like static configuration, where a user can adjust <i>more actions</i> than standard Scheduled Events, like Boost Mode Frequency, Transmit Channel Mask, and so on. There is also a user interface enhancement with this permission that creates a link/shortcut on the Dashboard page. When this link is selected, the System Intelligence > Scheduled Events page opens.  Note: This link only displays when Advanced Events are scheduled.	Not assigned to any user roles by default. DM Advanced Functionality. Relaxes the page requirements for entering a Scheduled Job ID and Device Family, and offers more programming options (including the sensitive radio frequency settings).
Perform key management and generate encryption files		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN SYSTEM_ADMIN TENANT_ADMIN

Permission name	Detailed definition (if needed)	Associated roles
Enable SP link test	Used in Water Device Manager. It enables access to the Device Maintenance > Get SP-Meter Link Test action on the device list page and the device details page. It also provides access to the Action filter on the device Event History tab. (Electric devices do not have SmartPoints or "SP." There are two actions for this permission: Get SP-Meter Link Test and Cancel Initiate SP-Meter Link Test.	Not assigned to any user roles by default. The Get SP-Meter Link Test and Initiate SP-Meter Link Test actions are specific to NA2W SmartPoints integrated with iPERL ASIC meters in RNI version 4.2 and 4.3. For RNI releases 4.4 and later, general support for these actions is supported for additional meters, including ally, EReg+, and discrete iPERL. Get SP-Meter Link Test solicits the NA2W SmartPoint for the latest link test results. Initiate SP-Meter Link Test solicits the NA2W SmartPoint to perform a new link test. The link test assesses the reliability of the communication across the wire between the SmartPoint module controller and the meter controller.
Remote deactivation	Allows the user to deactivate the capability of a SmartPoint module remotely. Only one SmartPoint module can be deactivated at a time (multiple modules cannot be selected for deactivation).	METER_SHOP_TECHNICIAN
Enable, disable, and configure shutoff alarms		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Shut off valve		DM_ADMIN DM_SYSTEM_OPERATOR GATEWAY METER_SHOP_TECHNICIAN TENANT_ADMIN
Manage the maximum number of devices that can be included in an action		SYSTEM_ADMIN TENANT_ADMIN
Control the display of sub 1hr MSR	Permission first included with RNI 4.9. Required to view and select Meter Sample Rate (MSR) options less than 1 hour in the MSR drop-down menu. This permission is required to view these options even if the device is unlocked.	DM_ADMIN DM_SYSTEM_OPERATOR TENANT_ADMIN
Synchronize meter and related data from the Customer Billing system to the RNI		DM_ADMIN GATEWAY SYSTEM_ADMIN TENANT_ADMIN
Manage broadcast groups		GATEWAY

Permission name	Detailed definition (if needed)	Associated roles
View broadcast group information		GATEWAY
Perform group system calls used by messaging		This permission is not assigned to any roles by default. It must be granted to a custom role added by the utility or to an existing user to use this new functionality included in RNI 4.13.1.
Perform group system calls used by group command senders		This permission is not assigned to any roles by default. It must be granted to a custom role added by the utility or to an existing user to use this new functionality included in RNI 4.13.1.
Manage meter disconnect reconnect scheduled jobs		This permission is not assigned to any roles by default. It must be granted to a custom role added by the utility or to an existing user to use this new functionality included in RNI 4.13.1.
Clear existing disconnect reconnect schedule on meter		This permission is not assigned to any roles by default. It must be granted to a custom role added by the utility or to an existing user to use this new functionality included in RNI 4.13.1.
Change alert severity	Enables the user to change the severity level for each individual alert so that it best reflects the actual severity of the alert for their utility.	DM_ADMIN

Password Management tab

Use the **Password Management** tab to set expirations, warnings, history, lockout, length and complexity of passwords.

The screenshot shows the 'Password Management' tab in a system administration interface. At the top, there are three tabs: 'Users', 'Roles', and 'Password Management', with 'Password Management' being the active tab. Below the tabs, a message states: 'Use the inputs below to edit User. Enter all *Required information.' The main section is titled 'Password Policy Management'. It contains several input fields: 'Policy Name' (a dropdown menu showing 'ACME'), 'Password Expiration*' (a text box with '90' and a tooltip 'in days'), 'Password Minimum Change*' (a text box with '0' and a tooltip 'in days'), 'Password Expiration Warning*' (a text box with '7' and a tooltip 'in days'), 'Password History*' (a text box with '10'), 'Password Lockout*' (a text box with '3'), 'Password Lockout Duration*' (a text box with '900' and a tooltip 'in seconds'), and 'Password Minimum Length*' (a text box with '12'). There is a checkbox labeled 'Password Complexity' which is checked. At the bottom, a note states: 'Changes to the password policy are not immediately reflected in any specific account until the password for that account has been changed'. Below this note are 'Save' and 'Cancel' buttons.

Users Roles Password Management

Use the inputs below to edit User. Enter all *Required information.

Password Policy Management

Policy Name

Password Expiration* in days

Password Minimum Change* in days

Password Expiration Warning* in days

Password History*

Password Lockout*

Password Lockout Duration* in seconds

Password Minimum Length*

☒ Password Complexity

Changes to the password policy are not immediately reflected in any specific account until the password for that account has been changed

or [Cancel](#)

Policy Name

The name of the password policy to establish or modify. Select the name of the password policy from the drop-down list before updating the policy's parameters. Options typically include *CUSTOMER* (the customer's name as set up in the RNI), *CUSTOMER_SERVICE* (for remote LDAP service accounts), default, and/or special.

Password Expiration (in days)

Specifies the number of days before a user password expires.

Password Minimum Change (in days)

Sets the period of time (in days) that a password must be used before the user can change it.

Password Expiration Warning (in days)

Specifies the number of days before the expiration date to display a password warning message and send a password expiration notification email.

Password History

Specifies how many passwords the password history stores. This setting determines the number of unique new passwords that must be associated with a user ID before an old password can be reused. The RNI uses this value to prevent the user from using the same password too often.

Password Lockout

Specifies how many times a user can enter an incorrect password before the system locks them out.

Password Lockout Duration (in seconds)

Specifies the amount of time a user will be locked out of the system due to the lockout.

Password Minimum Length

The minimum number of characters in a user password.

Password Complexity

Select this in order to inform the user if their password meets the system standards for password complexity.

Save

To save changes to the Password Management policy, select **Save**.



Note: For instructions to change your RNI user password, see **Change your RNI user password** under **Common activities** in the *Device Manager Electric, Gas, or Water User Guide*.

Password management for service accounts

RNI version 4.12.1 introduces a new separate password policy for service accounts. The separate password policy helps to prevent machine-to-machine integrations from failing due to a required password change.

A service account is an RNI-managed non-human service used to log in the RNI. Service accounts are typically used to manage integrations with the RNI and other related systems.



Important: The new password policy for service accounts only applies to **remote LDAP** accounts (in Sensus' Data Center). Local LDAP accounts can use the Special policy (assigned on the [Password Management](#) page). Active Directory customers manage their password policies outside of the RNI.

Configure the password policy for service accounts

You can configure a specific password policy for **remote LDAP** service accounts.

1. Select **Users > Password Management** to open the Password Management page.
2. From the **Policy Name** menu, select **CUSTOMER_SERVICE** to open the settings for the service account password policy.



Note: *CUSTOMER* is the name of the customer (or tenant) as it is configured in the RNI. In the following example, the customer is GOTG.

Password Management

Use the inputs below to edit User. Enter all ***Required** information.

Password Policy Management

Policy Name GOTG GOTG_SERVICE

Password Expiration* in days

After selecting the service account, the service account password policy options display.

Users Roles Password Management

Use the inputs below to edit User. Enter all ***Required** information.

Password Policy Management

Policy Name GOTG_SERVICE

Password Expiration* 365 in days

Password Minimum Change* 0 in days

Password Expiration Warning* 2 in days

Password History* 10

Password Lockout* 3

Password Lockout Duration* 900 in seconds

Password Minimum Length* 12

☒ Password Complexity

Changes to the password policy are not immediately reflected in any specific account until the password for that account has been changed

Save or Cancel

3. For the **Password Expiration** field, enter the number of days for the service account password to remain valid before it expires.
4. For the **Password Minimum Change** field, enter the number of days that a password must be used before the user can change it.
5. For the **Password Expiration Warning** field, enter the number of days before the expiration date to display a password warning message and send a password expiration notification email.
6. For the **Password History** field, enter how many passwords the password history stores.
This setting determines the number of unique new passwords that must be associated with a user ID before an old password can be reused. The RNI uses this value to prevent the user from using the same password too often.
7. For the **Password Lockout** field, enter how many times a user can enter an incorrect password before the system locks them out.
8. For the **Password Lockout Duration** field, enter the amount of time in seconds that a user will be locked out of the system due to the lockout.

9. For the **Password Minimum Length** field, enter the minimum number of characters in a user password.
10. Optionally, select the **Password Complexity** option.
This informs the user if their password meets the system standards for password complexity.
11. Select **Save** to save the changes to the password management policy for service accounts.

Apply the password policy to service accounts

After configuring the service account password policy, apply the new policy to service account users.



Note: As a one-time step after an upgrade from RNI 4.11.1 to 4.12.1, an administrator needs to change all service accounts to use the Service Account password policy.

You can specify which password policy to use on a per-user basis when a user is created or edited. The Service Account policy is only available for selection if the Service Account check box is selected for the user.

1. Use the instructions in [Add or edit a user](#) on page 64 to create or edit the service account user that needs to be designated to use the new Service Account password policy.

Software
Configuration
Users
SentryPoint Users

Edit "serviceaccountT"

Use the inputs below to edit User. Enter all ***Required** information.

[«Back to User List](#)

First Name:*

Last Name:*

User ID:*

Email:*

Service Account:

☒

[Change Password](#)

Customers:

Select Customer(s)

GOTG
MARVE
GUARD

Password Policy:

Select Policy

GOTG
GOTG_SERVICE

Multi-Factor Authentication

Disabled for service accounts

2. If there is more than one customer (tenant) for the RNI, select the correct customer from the **Customers** list.

3. For the **Password policy**, select the service policy which is named *CUSTOMER_SERVICE*. In this example, the Password Policy to select is *GOTG_SERVICE*.
4. Select **Save User** to update the service account user to use the service password policy.

Xylem |'zīləm|

- 1) The tissue in plants that brings water upward from the roots;
- 2) a leading global water technology company.

We're a global team unified in a common purpose: creating advanced technology solutions to the world's water challenges. Developing new technologies that will improve the way water is used, conserved, and re-used in the future is central to our work. Our products and services move, treat, analyze, monitor and return water to the environment, in public utility, industrial, residential and commercial building services settings. Xylem also provides a leading portfolio of smart metering, network technologies and advanced analytics solutions for water, electric and gas utilities. In more than 150 countries, we have strong, long-standing relationships with customers who know us for our powerful combination of leading product brands and applications expertise with a strong focus on developing comprehensive, sustainable solutions.

For more information on how Xylem can help you, go to www.xylem.com



SENSUS

637 Davis Drive

Morrisville, NC 27560

Tel +1.800.638.3748

www.sensus.com

Sensus, the Sensus logo, FlexNet® and associated logos are trademarks of Sensus and its subsidiaries and affiliates.

© 2023, Sensus USA, Inc., a subsidiary of Xylem, Inc.

All Rights Reserved. AUG-10051-21 November 2023