XYPRO Technology Corporation

XYGATE® Identity Connector (XIC) Reference Manual

Version 1.10

Email: support@xypro.com

Telephone: +1 805-583-2874

FAX: +1 805-583-0124

XYGATE® Identity Connector 1.10 Reference Manual

Trademarks

XYPRO Technology Corporation
4100 Guardian Street, Suite 100
Simi Valley, CA 93063
Telephone: +1 805-583-2874
Fax: +1 805-583-0124

Publication History

Software version	Description	Date
1.10	Initial publication.	February 2018

Contents

Chapter 1: Introduction

XYGATE® Identity Connector (XIC) provides HPE NonStop user provisioning through SailPoint IdentityIQ. XIC is a Representational State Transfer (REST) service developed in Java 1.8 and runs on any platform that supports Java VM.

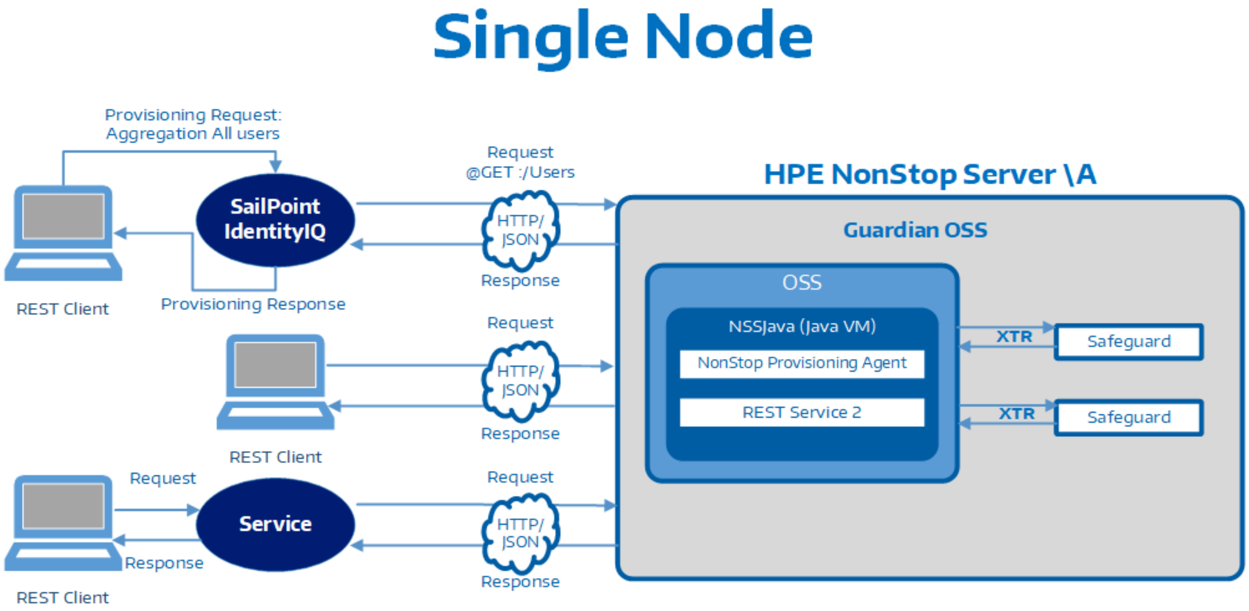
Features

XIC provides for account provisioning through a central channel. Among its key features are:

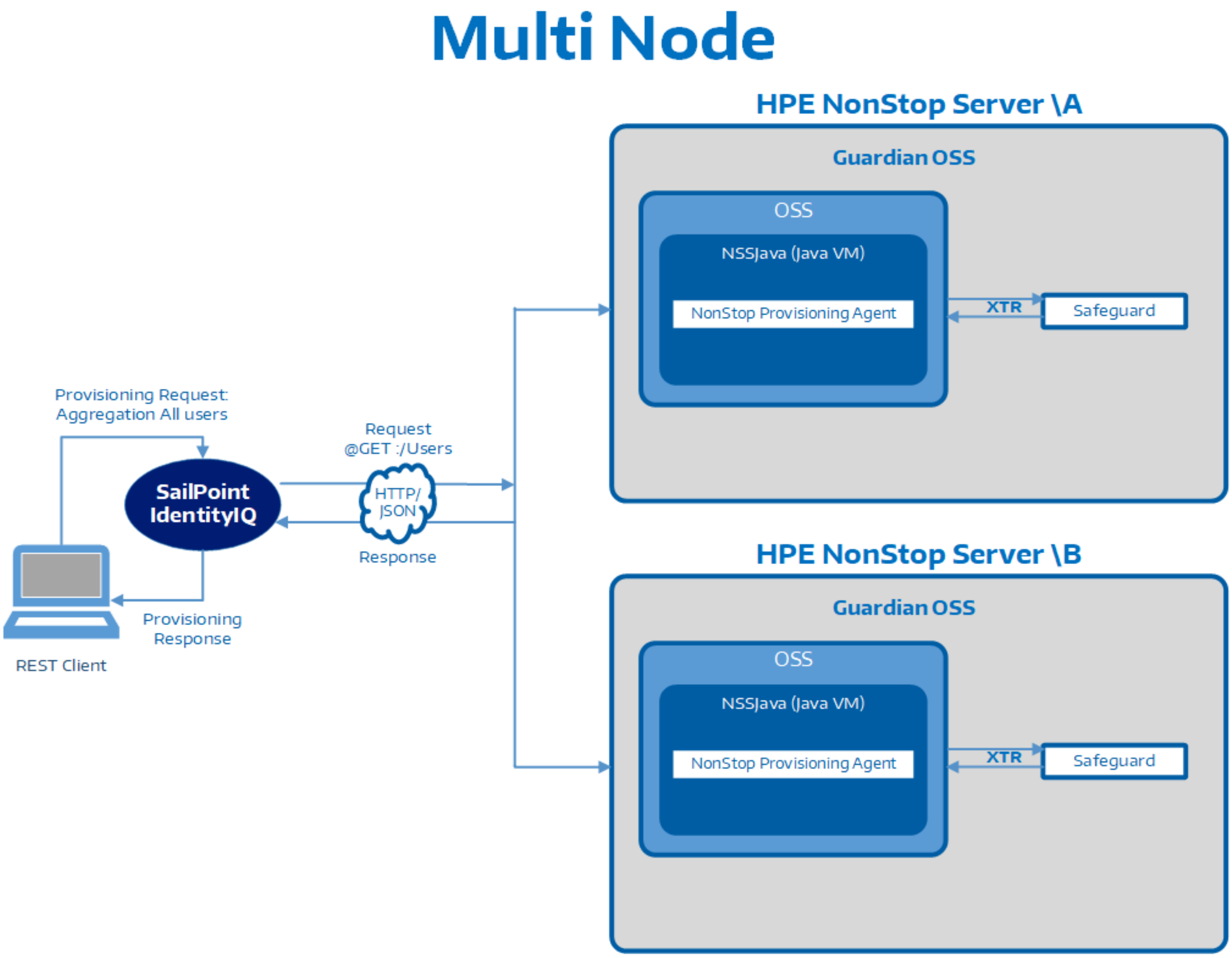
- Integration with SailPoint IdentityIQ
- The ability to support NonStop user attributes
- The ability to create, delete, enable, disable, and update NonStop user accounts

XIC Architecture

The following figure shows XIC in a single-node environment.



And the following shows XIC in a multi-node environment.



XIC Components

The following set of components is required to configure and manage the XIC service.

- Java 1.8 or higher
- XYPRO components:
    - XYGATE Identity Connector (XIC)
    - XIC license
    - XYGATE Transaction Router (XTR)
    - XTR Java Keystore (JKS) file
    - Service Configuration XML file
    - Service Deployer application
- SailPoint IdentityIQ 7.1

General Syntax Notation

The following list summarizes the notation conventions for syntax presentation in this manual.

UPPERCASE LETTERS. Uppercase letters indicate keywords and reserved words; enter these items exactly as shown. Items not enclosed in brackets are required. For example:

```
MAXATTACH
```

< > Angle Brackets. A pair of matching angle brackets indicate variable items that you supply but without the brackets. For example, where the syntax of a function is stated as:

```
kill -INT <PID>
```

If the <PID> (Process ID) of the process you want to kill is 123456, then the actual command will be as follows:

```
kill -INT 123456
```

[ ] Brackets. Brackets enclose optional syntax items. For example:

```
TERM [\<system-name>.]$<terminal-name>
INT[ERRUPTS]
```

A group of items enclosed in brackets is a list from which you can choose one item or none. The items in the list may be arranged either vertically, with aligned brackets on each side of the list, or horizontally, enclosed in a pair of brackets and separated by vertical lines. For example:

```
FC [ <num>  ]
   [ <-num> ]
   [ <text> ]
 K [ X | D ] <address-1
```

{ } Braces. A group of items enclosed in braces is a list from which you are required to choose one item. The items in the list may be arranged either vertically, with aligned braces on each side of the list, or horizontally, enclosed in a pair of braces and separated by vertical lines. For example:

```
LISTOPENS PROCESS      { $<appl-mgr-name> }
                       { $<process-name> }
          ALLOWSU      { ON | OFF }
```

| Vertical Line. A vertical line separates alternatives in a horizontal list that is enclosed in brackets or braces. For example:

```
INSPECT { OFF | ON | SAVEABEND }
```

… Ellipsis. An ellipsis immediately following a pair of brackets or braces indicates that you can repeat the enclosed sequence of syntax items any number of times. For example:

```
M <address-1> [ , <new-value> ]...
[   ] {0|1|2|3|4|5|6|7|8|9}...
```

An ellipsis immediately following a single syntax item indicates that you can repeat that syntax item any number of times. For example:

```
"s-char..."
```

Punctuation. Parentheses, commas, semicolons, and other symbols not previously described must be entered as shown. For example:

```
<error> := NEXTFILENAME ( <file-name> ) ;
LISTOPENS SU $<process-name>.#<su-name>
```

Quotation marks around a symbol such as a bracket or brace indicate the symbol is a required character that you must enter as shown. For example:

```
"[" <repetition-constant-list> "]"
```

Item Spacing. Spaces shown between items are required unless one of the items is a punctuation symbol such as a parenthesis or a comma. For example:

```
CALL STEPMOM ( <process-id> ) ;
```

If there is no space between two items, spaces are not permitted. In the following example, there are no spaces permitted between the period and any other items:

```
$<process-name>.#<su-name>
```

Bolded. Text indicates user input for a given prompt(s) on the command line, keyboard letters and symbols, and GUI radio and navigation buttons.

Plain *italic* **typeface**. Italic typeface indicates the full name of a document or title, a verbatim screen name, or display and script text in command line actions.

Chapter 2: NonStop XYGATE Identity Connector (XIC) Service Setup

This chapter describes the set up and running of the XIC service on an HPE NonStop server through OSS.

Before You Begin

Ensure that you have the following information and files ready before you begin the installation procedures:

- XTR is installed and enabled on the HPE NonStop systems you want to configure for user provisioning.
- XTR is configured to run the SAFECOM_255_GBL task (see "Configure the XTR TASKDEF File for XIC" on the next page for more information).
- The XIC Installer Package, which consists of the following:
    - Extract.sh script file
    - NonStop Installer Package (TAR), which includes the following
        - iXIC.jar
        - iXYServiceDeployer.jar (Service Deployer)
        - Openssl
        - Openssl.cnf
        - install.sh (NonStop Version)
        - Cert-Generator.sh (NonStop Version)
        - jks_generator.sh
        - istartup.sh
        - prng program file
        - prng.conf configuration file
        - prng-seed program file
        - xylicchk.sh
        - xylicchk.jar

Configure the XTR TASKDEF File for XIC

The XTR TASKDEF file contains references to internal macros and scripts that XTR runs on behalf of the various XYGATE GUIs. Follow the steps below to modify the XTR TASKDEFS file to configure XTR to allow user provisioning on a NonStop server.

1. Define the task "taskdef safecom-255" with the `TASKDEF` command in the TASKDEFS file as shown below.

```
safecom-255 config:
TASKDEF SAFECOM_255_GBL
SCOPE EXTERNAL
OBJECTTYPE BINFILE
OBJECTNAME $system.sysnn.safecom
RUNAS 255,255
```

2. Use the following syntax to add a new TASKDEFGROUP to the TASKDEFS file.

```
TASKDEFGROUP $XT_TEST SAFECOM_255_GBL
```

where `<task-group>` is the user-defined task group name. For example, if your task group name is "$XT_TEST" then you would enter the following.

```
TASKDEFGROUP $XT_TEST SAFECOM_255_GBL
```

3. In the TRACL file, add the following.

```
ACLGROUP $SCIM-TESTER <GROUP>,<USER> UNDERLYING:
<GROUP>,<USER>
TASK $XT_TEST                    ACL $SCIM-TESTER
```

Installing the Service on the NonStop

XIC comes packaged with all files necessary for installation of the service. The installation scripts cover these three areas:

- Install the service and all associated files in a designated location
- Dynamically generate the Service Config XML file based on user input
- Generate the keystore and self-signed certificate needed for HTTPS

Refer to the following subsections to install the service on a NonStop server.

Prerequisites

Before you extract and install the service please make sure the following prerequisites have been met.

- Java 1.8 or higher is installed
- Logging is enabled on the application you use to communicate with the NonStop (e.g., Windows Terminal)
- The administrator performing the install has access to the /usr/local directory

Extraction Steps

Follow the steps below to extract the service on a NonStop server.

1. Open the OSS directory where the NonStop Installer Package TAR and extract.sh script files are located.
2. Run the extract script with the following command.

```
./extract.sh
```

> **Note:** This will extract the files within the TAR file and place them in a /dst folder underneath the same directory.

3. Open the /dst/ns folder. (All the install files are in this folder.)

Installation Overview

When you run the install script you will be prompted to enter configuration parameters for XIC. The prompts are organized into functional groups called *sections*.

> **Note:** "Configuring the Service XML File" on page 18 includes a sample Service Configuration XML file that shows configuration settings.

Many prompts end with the text "<{default}>?", which indicates if you press the **Enter** key without supplying input, the default value or text that is between the brackets will be entered.

For example, if you press the **Enter** key after the following prompt **Y** will be entered.

```
Is this keytool okay to use <Y>
```

> **Note:** The XIC Installer Package includes two versions of Openssl: one for the J-Series NonStop and one for the L-Series NonStop. The TAR file will automatically install the correct version on your NonStop without user intervention.

Installation Steps

Follow the steps below to the install the service.

1. Enter the following command to run the installation script.

```
./install.sh | tee -a installLog.log
```

The next prompts are generic prompts that verify you are trying to do the installation and have met the prerequisites before attempting the install. Once those questions are answered, the following will be displayed.

```
What directory would you like to install the services in
</usr/local/XYPRO/webservices>?
```

2. Enter the base directory for the Service Configuration XML file (ServiceConfig.xml) and Service Deployer (iXYServiceDeployer.jar) file. XIC files will be in a subdirectory within the webservices directory (e.g., /usr/local/XYPRO/webservices/XYGATEIC).

XYGATE Pre-configuration Questions

In this section of the install script, you will be prompted to configure parameters used to generate and find default values needed to properly install XIC.

After you configure the base directory the following will be displayed.

```
The host name found for this system is: '{hostname}',
is this correct <Y>?
```

1. Enter the host name, which is typically the name of your NonStop without the backslash. If the correct name is found, press the **Enter** key. If not, enter **N** and you will be prompted to enter a different host name.

   The following will be displayed.

```
Where is the location of your XTR installation?
```

2. Enter the path to the XTR directory. The following will be displayed.

```
Is this keytool okay to use <Y>
```

3. The keytool utility generates required keystores for XTR and SSL. A search for the keytool on the system is performed and if one is found it is displayed. Press the **Enter** key to accept it. If the keytool is not found you will be prompted to enter the path and name of the keytool.

XYGATE Transaction Router (XTR) JKS Generator

For XIC to communicate and execute the requests, communication between XIC and XTR must be set up. To do so, a keystore is generated to bridge the gap between the two XYGATE products.

After you install the keytool utility the following will be displayed.

```
What is the passphrase for the keystore?
```

After you enter the passphrase the following files will be generated.

- XIC_XTR_PubKey.pem
- XIC_XTR_PrivatePair.pem
- XIC_XTR_EP.ssl
- XIC_XTR.jks

These files will be placed in your {$HOME}/.ssh directory.

Global Properties

Global properties are values that will be sent to all services/instances when the Service Deployer is run. Every service/instance requires these properties.

After you enter the passphrase the following will be displayed.

```
What is the ip address or hostname the service will be
running on <{IP}>?
```

Enter the IP address or host name of the NonStop system where you are installing XIC.

Log Properties

Log properties are properties that are used to configure logging for XIC. Every service/instance will receive these properties.

After entering the IP or host name of the NonStop as described above the following will be displayed.

```
What is the max size of each log file <10mb>?
```

1. Each log has a certain size it can reach before it starts a new one. Enter a number followed by one of the following suffixes: "kb", "mb", or "gb". (The default is 10 megabytes.) For example, enter **2gb** to set the maximum log size to 2 gigabytes.

   The following will be displayed.

```
How many backups do you want to keep of each log <10>?
```

2. When the maximum size of a log is reached, a new log file and a backup of the previous log will be created. By default, up to 10 backups will be stored. Once this limit is reached the oldest backup will be deleted when a new log file is created. Enter the number of log files you would like backed up.

XYGATE Services

The current service is XIC. When additional services are available, you will select the service you want here. For now, after you configure the global properties the following will be displayed.

```
What service are you trying to install <XIC>?
```

Press the **Enter** key.

XYGATE-IC Version 1.10

This section prompts you to configure specific properties needed by XIC. After you set XIC as the service to install the following will be displayed.

```
Do you want to have this service initially flagged to run
<Yes>?
```

1. Press the **Enter** key or enter **Y** (the default) to set the run property (runInstance) to true or enter **N** to set it to false. When the Service Deployer runs it will search each service to see if it is flagged to run. If it is set to run, the Service Deployer will go through the instances of that service and determine which to deploy based on if runInstance is set to true.

   The following will be displayed.

```
What directory do you want to place the logs
</usr/local/XYPRO/webservices/XYGATEIC/logs>?
```

2. Enter the directory (the logPath property) where XIC will store all XIC logs. (By default, logs are stored inside the XYGATEIC folder.)

   The following will be displayed.

```
What is the name of this instance <{hostname}>?
```

3. Enter the instance ID of this XIC deployment. (The default is the host name.) You can configure multiple deployments of XIC on a single system by specifying a unique instance ID for each one. However, on NonStop servers, XYPRO recommends only one instance.

   The following will be displayed.

```
For {instance name}, do you want to flag it to run <Yes>?
```

4. Press the **Enter** key or enter **Y** to run the current XIC instance or **N** to skip the current instance. (This sets the run property runInstance.) If the run property is flagged, all instances within XIC that have runInstance set to true (Yes) will be deployed.

   The following will be displayed.

```
For {instance name}, what is the port number that this
instance will be listening on?
```

5. Enter the port number (servicePort property) that will be used by SailPoint IdentityIQ to communicate with XIC.

The following will be displayed.

```
For {instance name}, what is the IP address or hostname that
XTR will be connecting to <{XTR IP}>?
```

6. Enter the IP address or host name of the NonStop where XTR is located. (This sets the xtrIP property.) Normally, the default value will be populated with the value that can be found in your XTR directory.

   The following will be displayed.

```
For {instance name}, what is the port number that XTR will be
listening on <{port}>?
```

7. Enter the port that the XTR Listner process uses. (This sets the xtrPort property.) Normally, the default value will be populated with the value that can be found in your XTR directory

   The following will be displayed.

```
Do you want to add another instance <N>?
```

Press the **Enter** key or enter **N** (recommended) to proceed to the "Generating the HTTPS Certificate" below or enter **Y** to go back to Step 3 on the previous page and configure another instance on this system. XYPRO recommends only a single instance for NonStop systems.

All files generated during this section are placed under your {$HOME}/.ssh directory. Each file name begins with an "XIC_Sailpoint" prefix.

Generating the HTTPS Certificate

This section generates the keystore and certificate that is needed to provide HTTPS communication between XIC and SailPoint IdentityIQ.

> **Note:** The default values for the subject information are copied from XTR's SSL certificate (if it was found).

```
What is the Common Name (CN) <{XTR-SSL CN}>?
What is the Organizational Unit (OU) <XTR-SSL OU>?
What is the Organization (O) <XTR-SSL O>?
What is the Locality (L) <XTR-SSL L>?
What is the State (S) <XTR-SSL S>?
What is the Country Name (C) < XTR-SSL C>?
Enter in a passphrase (minimum of 6 characters):
```

XIC uses this passphrase to validate a requestor's SSL certificate. Once it is entered, the keystore and certificate are generated. The passphrase is then encrypted using RSA.

Completing the Install

After you have configured the HTTPS certificate you will be asked if you want to configure another service. Enter **N** since there are currently no other services. The installation will be complete.

Next, a “How to Run” prompt will be displayed that provides instructions on where and how to deploy the service.

Uninstalling XIC

Follow the steps below to uninstall XIC using the uninstall.sh script file.

> **Note:** Please verify that all services have been stopped before uninstalling XIC. See "Stopping the Service" on page 23 for more information.

1. Navigate to the /dst folder, which contains all XIC's install files.
2. Enter the following command to run the uninstall script file.

```
./uninstall.sh | tee -a uninstallLog.log
```

As the uninstall script runs it will attempt to read the attributeLog.log file, which was generated during installation and contains the target directories. The uninstall scrip uses this file to determine the following.

- The XIC base directory
- XIC-related files from the user's /.ssh directory

If this file exists and has not been tampered with the script will set this data as the default input. Simply press **Enter** to delete these items when prompted. Otherwise, you will be prompted to provide the items listed above.

Next, the uninstall script will prompt you to delete other items. Delete these items as necessary.

HTTPS Access

To add HTTPS access, the certificate for XIC must be added to the Java environment that SailPoint IdentityIQ is installed on. This certificate, XIC_SailPoint_Cert.cer, was generated during installation and is in your {$HOME}/.ssh directory as shown below.

```
XIC_SailPoint_Cert.cer
```

Follow these steps to add HTTPS access for SailPoint IdentityIQ.

1. FTP the certificate in binary mode from the NonStop onto the system that will be used to access SailPoint IdentityIQ.
2. Open a Command prompt with administrator privileges and navigate to the /<java path>/lib/security folder and verify that a cacerts file, which is a collection of Certificate Authority (CA) certificates, exists.
3. You must add the certificate as a trusted certificate by entering the following command:

```
keytool -import -alias <alias> -file <filePath>/
XIC_SailPoint_Cert.cer -keystore cacerts -storepass
<password>
```

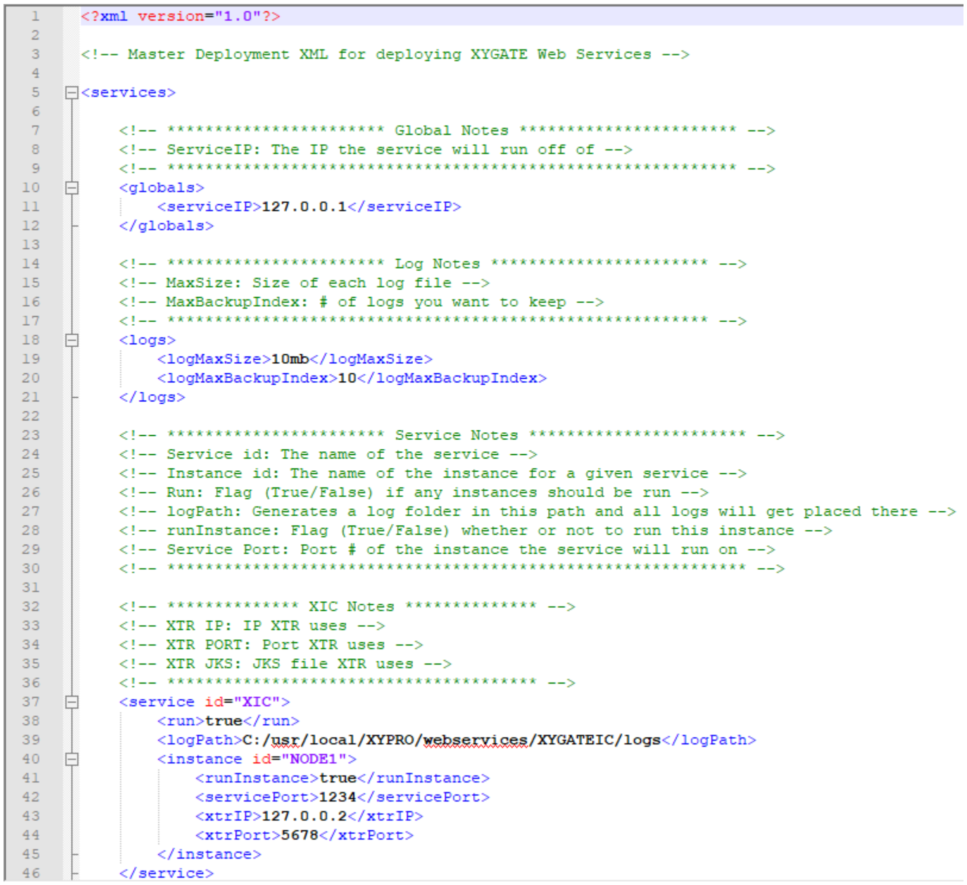
Note: The Storepass password is typically "`changeit`".

4. When prompted to trust the certificated, enter **Yes**.
5. Reopen SailPoint IdentityIQ. HTTPS should now be enabled.

Configuring the Service XML File

The Service Configuration XML file (ServiceConfig.XML) is used during deployment and is critical to ensuring that the services are configured properly. The file contains three main sections: Globals, Logs, and Services. The following shows an example Service Configuration XML file.

Note: Each NonStop system that deploys a service will need its own copy of the Service Configuration XML file.



```xml
<?xml version="1.0"?>

<!-- Master Deployment XML for deploying XYGATE Web Services -->

<services>

    <!-- *********************** Global Notes *********************** -->
    <!-- ServiceIP: The IP the service will run off of -->
    <!-- ************************************************************ -->
    <globals>
        <serviceIP>127.0.0.1</serviceIP>
    </globals>

    <!-- *********************** Log Notes *********************** -->
    <!-- MaxSize: Size of each log file -->
    <!-- MaxBackupIndex: # of logs you want to keep -->
    <!-- ********************************************************* -->
    <logs>
        <logMaxSize>10mb</logMaxSize>
        <logMaxBackupIndex>10</logMaxBackupIndex>
    </logs>

    <!-- *********************** Service Notes *********************** -->
    <!-- Service id: The name of the service -->
    <!-- Instance id: The name of the instance for a given service -->
    <!-- Run: Flag (True/False) if any instances should be run -->
    <!-- logPath: Generates a log folder in this path and all logs will get placed there -->
    <!-- runInstance: Flag (True/False) whether or not to run this instance -->
    <!-- Service Port: Port # of the instance the service will run on -->
    <!-- ************************************************************* -->

    <!-- ************** XIC Notes ************** -->
    <!-- XTR IP: IP XTR uses -->
    <!-- XTR PORT: Port XTR uses -->
    <!-- XTR JKS: JKS file XTR uses -->
    <!-- *************************************** -->
    <service id="XIC">
        <run>true</run>
        <logPath>C:/usr/local/XYPRO/webservices/XYGATEIC/logs</logPath>
        <instance id="NODE1">
            <runInstance>true</runInstance>
            <servicePort>1234</servicePort>
            <xtrIP>127.0.0.2</xtrIP>
            <xtrPort>5678</xtrPort>
        </instance>
    </service>
```

Globals Section

The following configuration property will be sent to all flagged services. It is required for every service.

- **serviceIP**: The service IPv4 address on which the service will be running.

Logs Section

These following configuration properties will be used to configure your auditing and logging.

- **logMaxSize**: The maximum size of each log before it rolls over to a new log file.
- **logMaxBackupIndex**: The number of logs that will be rolled over before being overwritten.

Services Section

The Services section contains properties that allow you to dynamically add, remove, and configure services. The Services section contains three main subsections: Service, Instance, and Properties.

Service Subsection

The service is the unique XYGATE service. (Currently, there is only XIC.)

Instance Subsection

The instance is a unique configuration for that service. XIC allows for multiple instances of a service to be deployed at any given instance if it is configured properly.

Properties Subsection

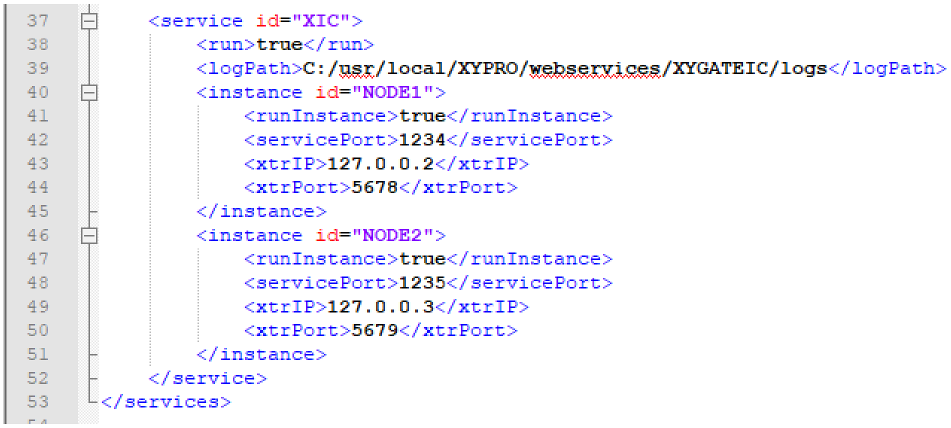
The properties, described below, are the values for the current service and instance.

- **logPath**: The folder path on which you would like the services to place their logs.

  Note: If the folder path does not exist, it will be generated.
- **Service id**: The acronym for the service you are trying to deploy. (In this case, XIC.)
- **Run**: A flag that determines whether any instance(s) of the service will run.
  - If flagged as true, the Service Deployer will go through every instance configuration and deploy each instance that has runInstance flagged as true.
  - If flagged as false, the deployment will skip over all instances even if the instance itself is flagged as true or false.
- **Instance id**: A unique identifier for that instance of the service
- **runInstance**: A flag as to whether this instance should be deployed.
- **servicePort**: The port you would like this instance of the service to be listening on.
- **xtrIP**: The IP or host name of the HPE NonStop that XTR will be using to communicate.
- **xtrPort**: The port on the HPE NonStop that XTR will be using to communicate.

Adding Multiple Instances

XIC allows for multi-node provisioning. To enable multi-node provisioning, there must be multiple instances of the service running (one for each node). The following shows an example section of the Service Configuration XML file that configures multiple instances.



```
    <service id="XIC">
        <run>true</run>
        <logPath>C:/usr/local/XYPRO/webservices/XYGATEIC/logs</logPath>
        <instance id="NODE1">
            <runInstance>true</runInstance>
            <servicePort>1234</servicePort>
            <xtrIP>127.0.0.2</xtrIP>
            <xtrPort>5678</xtrPort>
        </instance>
        <instance id="NODE2">
            <runInstance>true</runInstance>
            <servicePort>1235</servicePort>
            <xtrIP>127.0.0.3</xtrIP>
            <xtrPort>5679</xtrPort>
        </instance>
    </service>
</services>
```

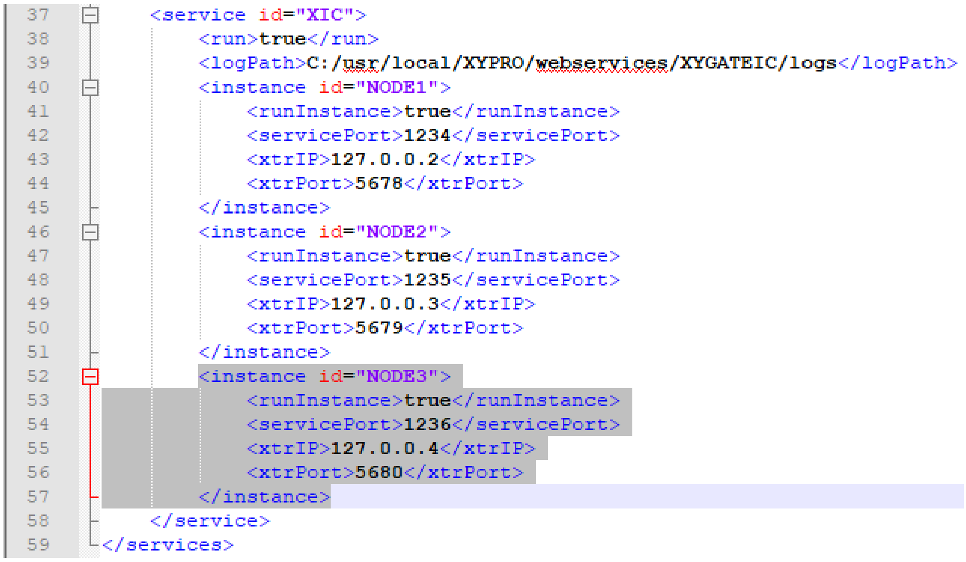
You can add multiple instances during installation with the Service Deployer or after installation. See the subsections below for more information.

Adding Multiple Instances with the Service Deployer

The Service Deployer lets you dynamically add and remove instances. To add another instance, simply create a second Instance section and configure the properties accordingly with the other node. When the Service Deployer is rerun, it will now deploy (if flagged) any new instances.

Adding Multiple Instances After Installation

You can add multiples instances without the need to run the installer again by editing the Service Configuration XML file with a text editor. To add a new instance, create a new section for it in the Services section and configure the runInstance, servicePort, xtrIP, xtrPort, and xtrJKS properties for it. The following shows an example of a new "NODE3" that has been added to the Service Configuration XML file shown on the previous page.



```
    <service id="XIC">
        <run>true</run>
        <logPath>C:/usr/local/XYPRO/webservices/XYGATEIC/logs</logPath>
        <instance id="NODE1">
            <runInstance>true</runInstance>
            <servicePort>1234</servicePort>
            <xtrIP>127.0.0.2</xtrIP>
            <xtrPort>5678</xtrPort>
        </instance>
        <instance id="NODE2">
            <runInstance>true</runInstance>
            <servicePort>1235</servicePort>
            <xtrIP>127.0.0.3</xtrIP>
            <xtrPort>5679</xtrPort>
        </instance>
        <instance id="NODE3">
            <runInstance>true</runInstance>
            <servicePort>1236</servicePort>
            <xtrIP>127.0.0.4</xtrIP>
            <xtrPort>5680</xtrPort>
        </instance>
    </service>
</services>
```

Removing Instances

To delete an instance, open the Service Configuration XML file and simply remove it from the file.

NonStop Deployment

Refer to the sections below to deploy XIC on a NonStop server.

Startup Script Overview

The startup.sh startup script file runs the Service Deployer. In addition to performing deployment functions, the Service Deployer also checks to validate that the port configured for the instance is not in use before it deploys it. All information about the deployment is logged in files named in the following format.

```
deployment_{yyyymmdd}-{hhmm}.log
```

License Checking

XIC performs a license check once it is deployed (not before deployment). When XIC validates/checks a license, that information is stored in the XIC logs. Licensing information (e.g., whether the license was valid, how many days remain, etc.) can be found in the logs.

If you want to check if a license is valid without running XIC, perform the steps below.

1. Navigate to the /XYGATEIC directory.
2. Enter the following command.

```
./xylicchk.sh
```

3. The xylicchk.sh script will run and then prompt you for the name of the license file. Please note this file needs to be in the same directory as the script file.
4. When prompted for the product number, enter **83**.

XIC also performs a license check every 24 hours to verify the license is still valid. If the license expiration is 30 days or less XIC will send an EMS message.

Running the Service

All services are required to be run through the Service Deployer (iXYServiceDeployer.jar). Make sure the Service Configuration XML file (ServiceConfig.XML) is configured properly with the correct instance(s) flagged to run.

> **Important:** The service cannot be run unless a valid license file (p83f001) is in the /XYGATEIC directory.

Once complete, within OSS navigate to the directory containing all the files and enter the following command:

```
./startup.sh
```

The Service Deployer will read your Service Configuration XML file and deploy each instance that is flagged to run. The service and its instance(s) will now be up and running. Each service instance that was successfully deployed will be added to the file XYProcess, which contains a list of all XYGATE services that are currently running.

Displaying Service Information

As the service deploys, all instances will show up as "java" if you enter **ps** at the prompt. To avoid confusion, XYPRO recommends opening the logs to find the service information once the service has been deployed. Another way of checking the service process ID is to enter the following command:

```
ps -f
```

This command will provide you with all processes running under its name, along with the parameters sent for that process.

In addition, you can check the Service Log by following the steps below.

1. Navigate to the log directory within OSS (</usr/local/XYPRO/webservices/XYGATEIC/logs>).
2. Enter the following command.

```
cat XIC_<instance>_http.log
```

Each service has an XIC_<instance>_http.log file that on startup logs the Process ID. To display the log information for an instance named "NODE1" you would enter the following.

```
cat XIC_NODE1_http.log
```

This will populate the screen with the log information. Scroll down until you find the startup as shown in the example below.

```
2018-01-19 05:13:07 INFO  - XYGATE-IC license is valid.
2018-01-19 05:13:07 INFO  - /users/user1/XYGATEIC/p83f001
expires in 29931 Days.
2018-01-19 05:13:07 INFO  - Starting up Service: XIC NODE1
2018-01-19 05:13:07 INFO  - Process ID: 1577058455
2018-01-19 05:13:07 INFO  - Port: 1234
```

Stopping the Service

XIC includes a script file, /shutdown.sh, that stops services on the host. Follow the steps below to run this script file.

1. Navigate to the /dst folder, which contains all XIC's install files.
2. Enter the following command to run the /shutdown.sh script file.

```
/shutdown.sh
```

A list of currently-running XYGATE services and a prompt for what service to stop will be displayed.

3. Perform one of the following.

- To stop a single service, enter its number.
- To stop multiple services, enter their numbers separated by spaces.
- To stop all services, enter an asterisk (*****).

If you stop all services then the XYProcess file will be deleted. Otherwise, shutdown.sh will update the XYProcess so that it has the most up-to-date information on running services.

Chapter 3: SailPoint IdentityIQ Environment Setup

This chapter describes the methods of setting up the SailPoint IdentityIQ environment for the XYGATE Identity Connector (XIC) service.

> **Important:** This chapter is not intended as a guide to SailPoint IdentityIQ. Please refer to SailPoint's latest documentation for features unrelated to creating an environment for the XIC service.

SailPoint IdentityIQ Documentation

SailPoint documents should be located underneath the deployed web application container under **Docs**. In addition, you can access SailPoint documents on SailPoint's Compass Portal (https://community.sailpoint.com/welcome) in the documents section for the relevant release version of IdentityIQ.

> **Note:** Please ensure that the SailPoint IdentityIQ documentation version matches your IdentityIQ version.

SailPoint IdentityIQ Administration Guide

Use the *SailPoint IdentityIQ Administration Guide* as your principal guide for IdentityIQ setup. This guide covers the following topics.

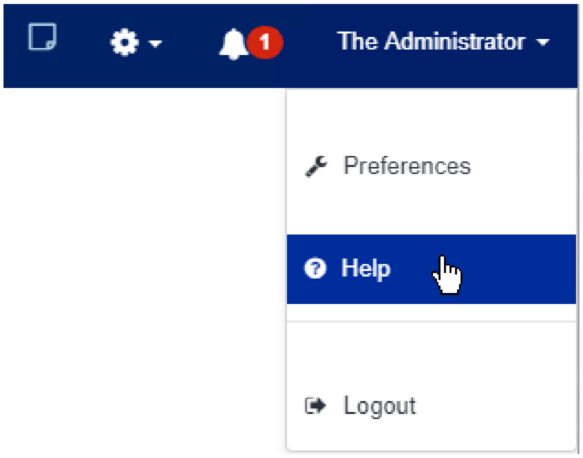
- Setting up IdentityIQ applications
- Setting up IdentityIQ tasks
- Provisioning users with IdentityIQ
- Enabling access to the user-configured NonStop application
- How to correlate HPE NonStop account attributes to IdentityIQ application attributes on the Correlation tab
- Managing accounts

SailPoint Direct Connectors Admin and Config Guide

For specifics about the SCIM 2.0 connector, please refer to the *SailPoint Direct Connectors Admin and Config Guide*.

SailPoint IdentityIQ User's Guide

To access the *SailPoint IdentityIQ User's Guide*, click the dropdown next to your login name and select **Help** as shown below.



Before You Begin

Ensure that you have the following ready before you begin the installation procedures:

- An administrator account for an IdentityIQ instance, version 7.1 or higher
- You have successfully setup the XIC service (see "NonStop XYGATE Identity Connector (XIC) Service Setup" on page 10 for more information)
- You have an active NonStop server user ID that has XTR privileges

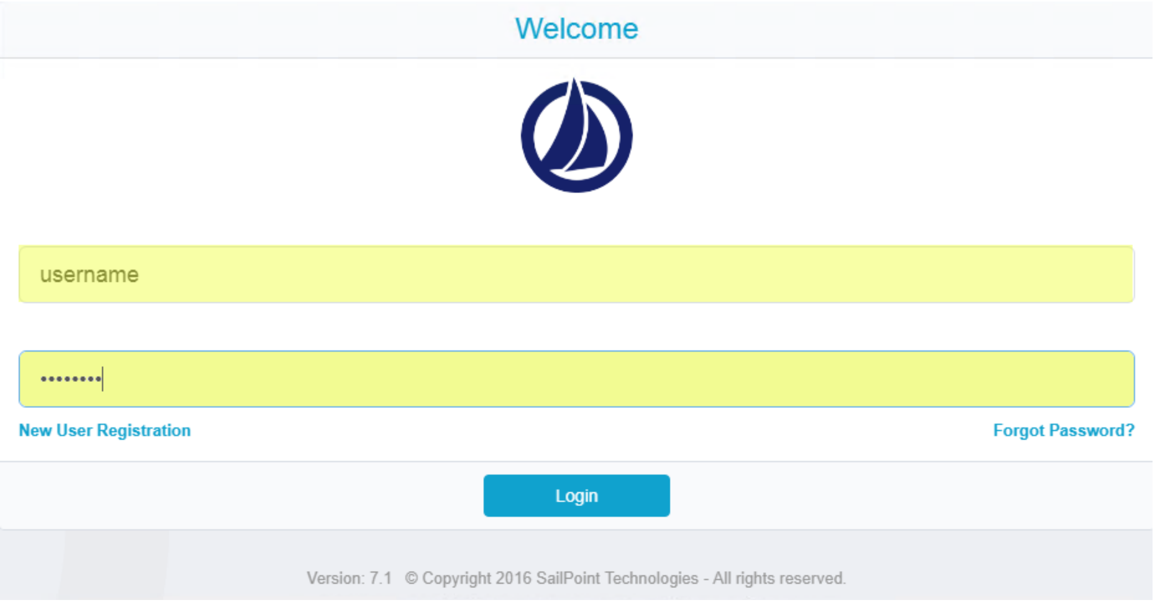
SailPoint IdentityIQ Login

Follow the steps below to log into SailPoint IdentityIQ.

1. Open SailPoint IdentityIQ. The login path will look like the following example:

```
Localhost:8080/identitiq71/login.sfj
```

2. Once on the login screen, enter your SailPoint credentials.

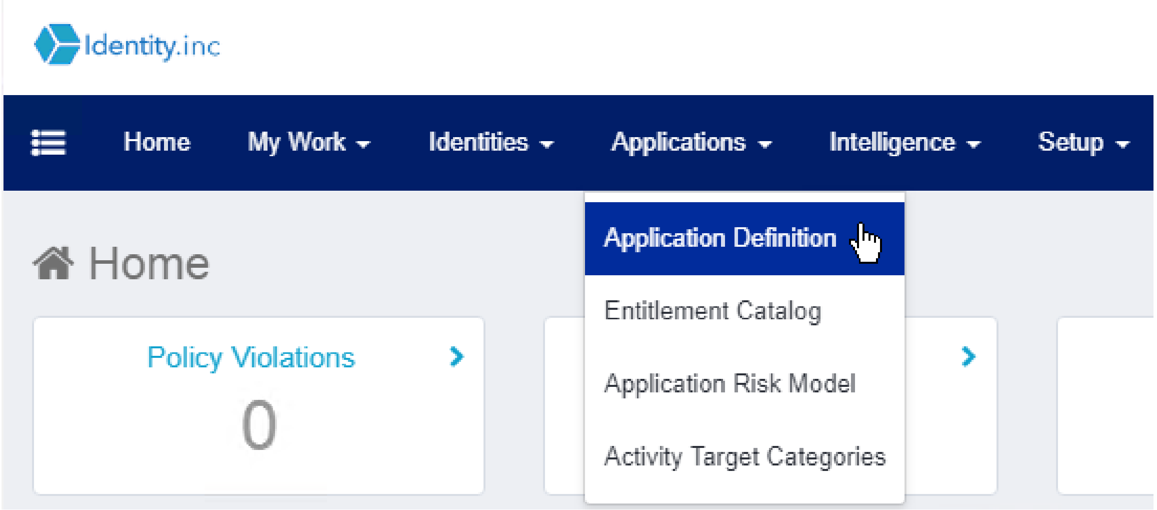

Welcome
username
••••••••
New User Registration
Forgot Password?
Login
Version: 7.1 © Copyright 2016 SailPoint Technologies - All rights reserved.

Creating a NonStop Application

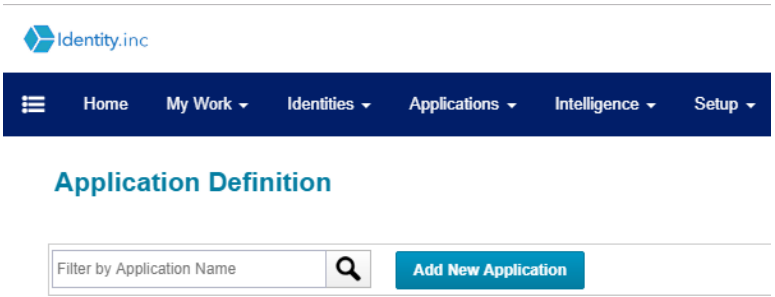
SailPoint IdentityIQ needs an application to connect to the XIC service. Therefore, before you can start provisioning users, an application must first be created.

> **Note:** Make sure the service has already been deployed and is running in the background during application setup.

Once logged in, select **Application Definition** from the **Applications** dropdown as shown below.



The *Application Definition* page, which provides a list of all applications associated with the current account, will be displayed as shown below.

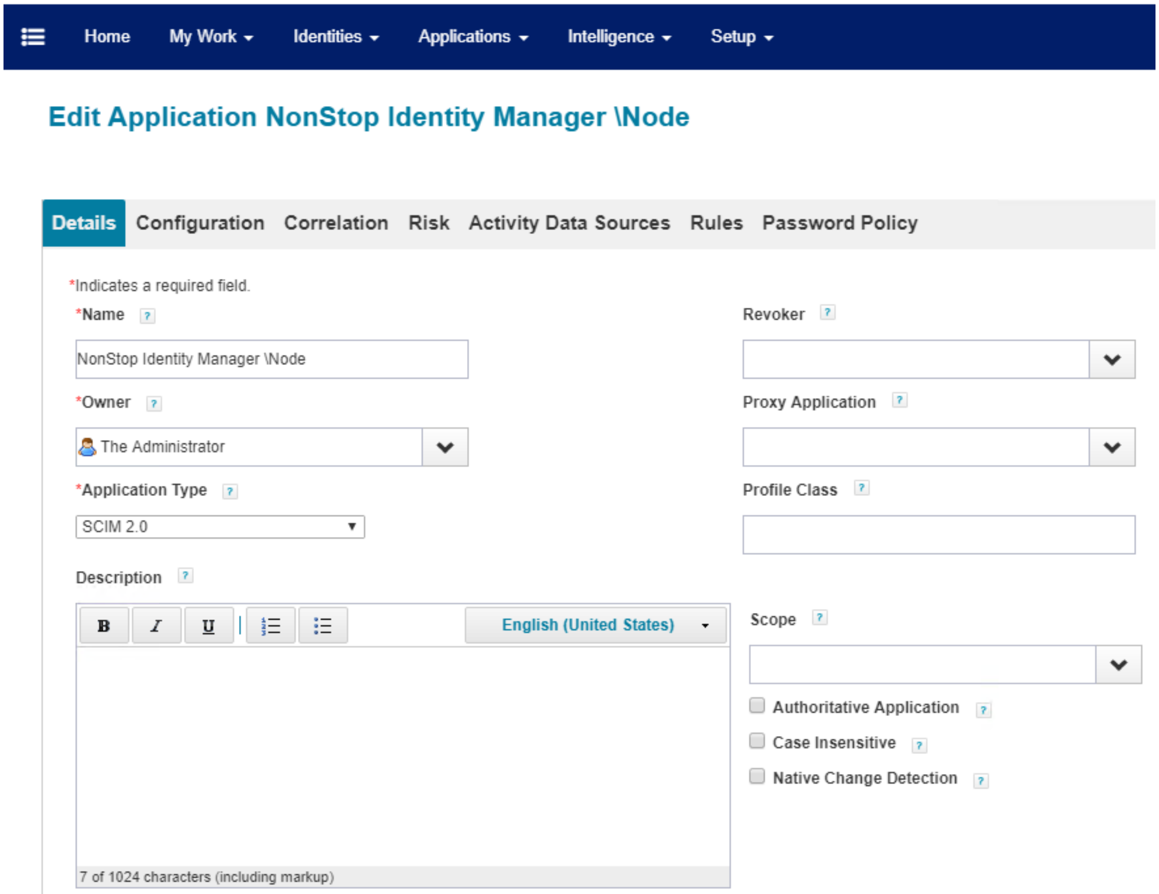


Application Definition

Since this is the initial setup, you need to add a new application by clicking the **Add New Application** button. This will display the *Details* tab, which is described below.

Details Tab

Click **Details** in the top menu bar to display the *Details* tab, which contains the high-level information about the application (e.g., the account name, what kind of application, etc.) and is shown below.



Edit Application NonStop Identity Manager \Node

*Indicates a required field.

*Name: NonStop Identity Manager \Node

*Owner: The Administrator

*Application Type: SCIM 2.0

Description

7 of 1024 characters (including markup)

Revoker

Proxy Application

Profile Class

Scope

□ Authoritative Application

□ Case Insensitive

□ Native Change Detection

For this tab, the only initial setup that is required is to configure the following.

- **Name**: What the application will be referenced as throughout SailPoint IdentityIQ. XYPRO recommends that the name is related to NonStop and which node (e.g., NODE1).
- **Owner**: This is the designated owner of the application.
- **Application Type**: This drives SailPoint IdentityIQ's configuration for the application.
- **Required**: From this dropdown select **SCIM 2.0**.

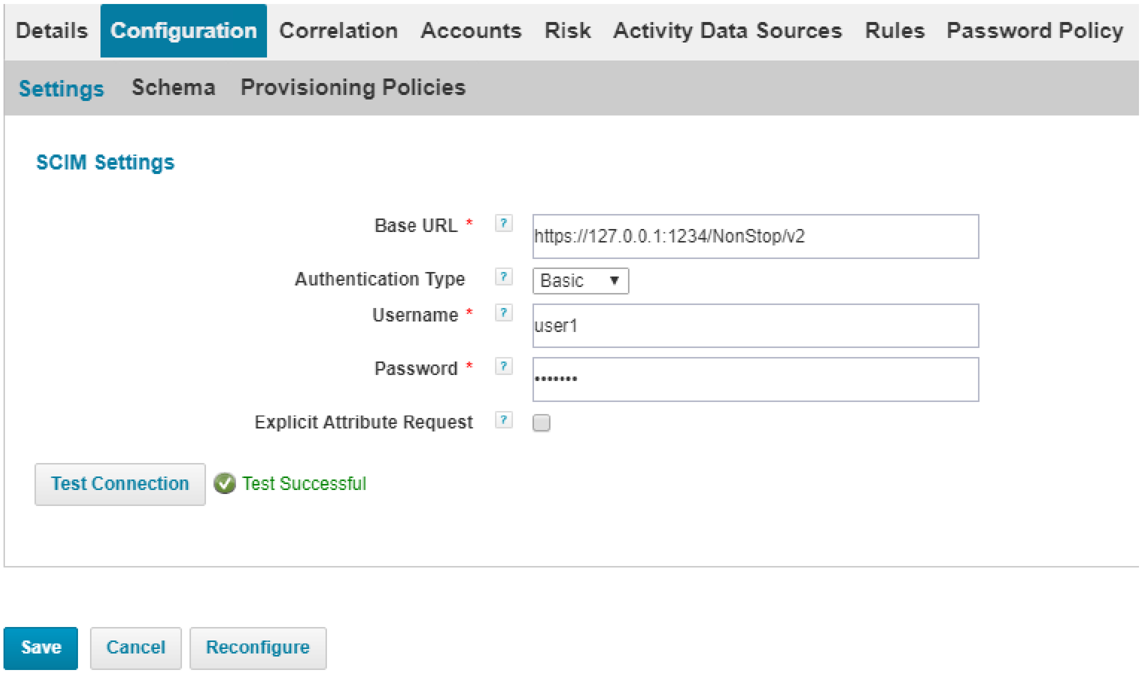
Note: For a complete description of these attributes, and where they are utilized within the SailPoint IdentityIQ platform, please see the official SailPoint documentation.

Configuration Tab

Click **Configuration** in the top menu bar to display the *Configuration* tab, where you will configure SailPoint IdentityIQ to provide information unique to the XIC service and its functionality. This tab also contains three sub-tabs: Settings, Schema, and Provisioning Policies. The Settings and Schema sub-tabs are described below. Please refer to the SailPoint IdentityIQ documentation for more information about the Provisioning Policies sub-tab.

Settings Sub-tab

The *Settings* sub-tab, as shown below, is where you provide the base URL along with the authentication you will be using when accessing the service.



Base URL * https://127.0.0.1:1234/NonStop/v2

Authentication Type Basic

Username * user1

Password * •••••••

Explicit Attribute Request □

✓ Test Successful

The fields on this sub-tab are described below.

- **Base URL**: The base URL for the System for the Cross-domain Identity Management (SCIM) service. Enter the base URL using the format `https://<IP Address of Service>:<Service Port>/NonStop/v2`.

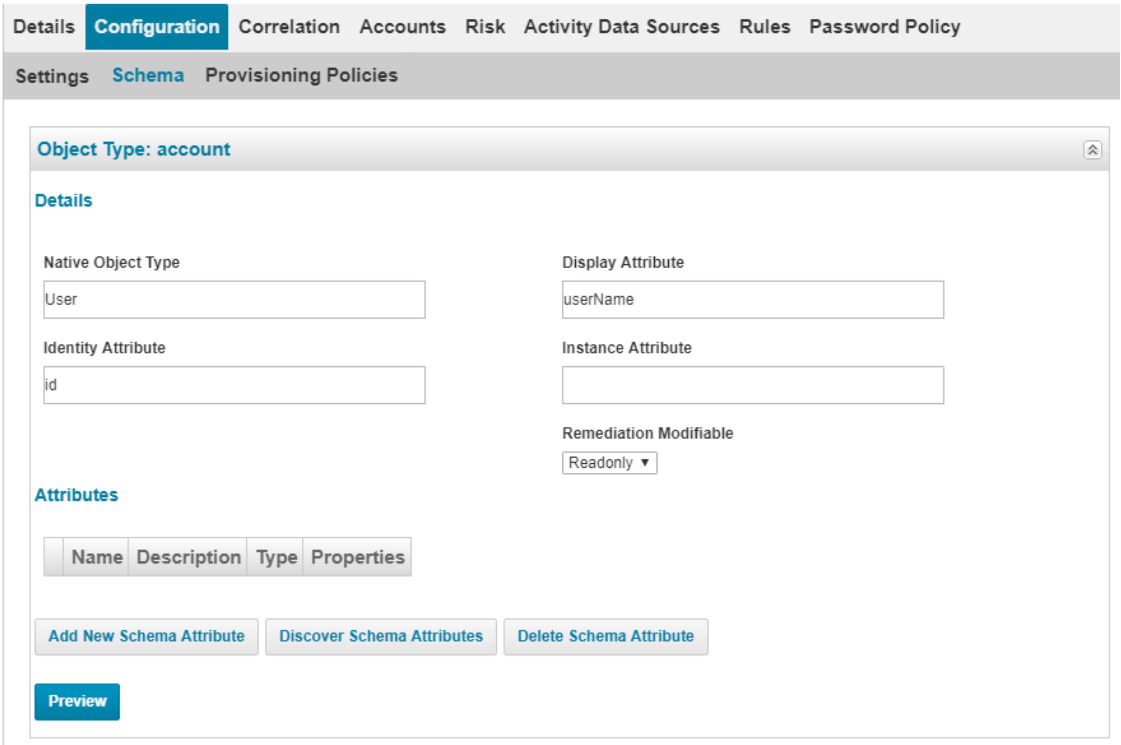
  > **Important:** The URL is case sensitive. For example, if the IP address is "127.0.0.1" and the port number is "1234" you must enter **https://127.0.0.1:1234/NonStop/v2**.

- **Authentication Type**: The method of authorization into the SCIM service. Select **Basic** from the dropdown. Please note when using Basic authentication is not secure. Security will need to be an active part of the deployment (e.g., use HTTPS, secure networking, etc.).
- **Username** and **Password**: Enter the HPE NonStop credentials that have access to XTR tasks and authorization to perform user provisioning.

Once these are added, start up the service and click **Test Connection**. A notification next to the button should popup displaying either **Test Success** or **Fail**.

Schema Sub-tab

The *Schema* sub-tab provides information unique to the resources and attributes the service provides and how SailPoint IdentityIQ handles those resources. (XIC only supports User accounts.) The information for this will be filled underneath the *Object Type: account* section as shown below.



Object Type: account

Details

Native Object Type: User

Display Attribute: userName

Identity Attribute: id

Instance Attribute:

Remediation Modifiable: Readonly

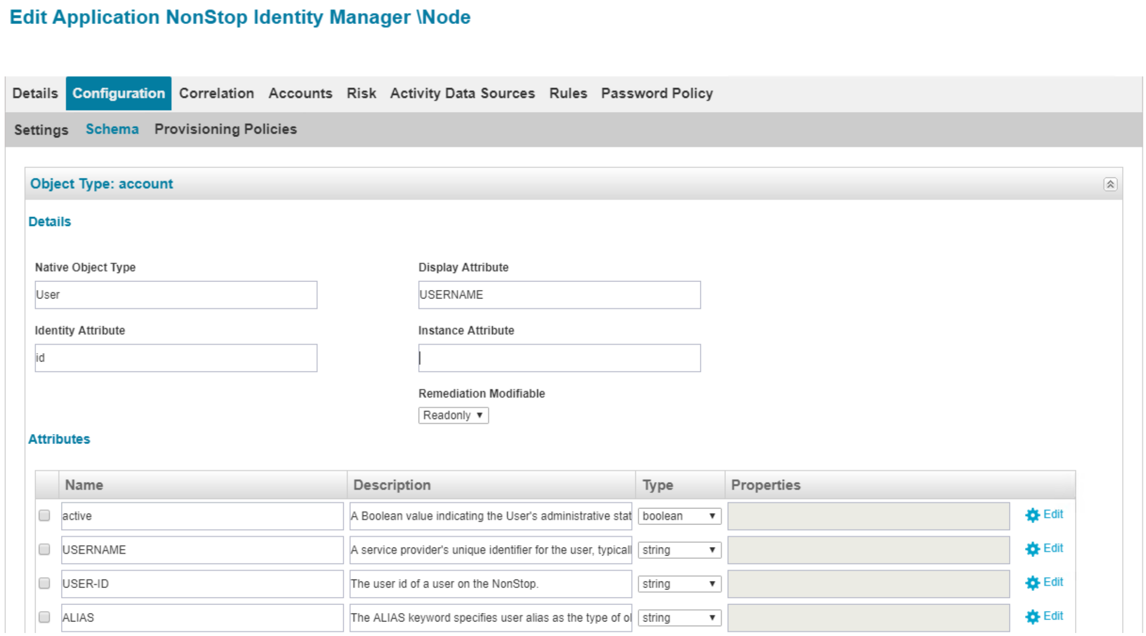
Attributes

	Name	Description	Type	Properties

Within the *Details* section, make sure the information is as follows:

- **Native Object Type**: This field defines what kind of resource/account this is on the NonStop. Enter **User** for this field.

Next, scroll down to the *Attributes* section and click the **Discover Schema Attributes** button. The following will be displayed.



Edit Application NonStop Identity Manager \Node

Object Type: account

Details

Native Object Type: User

Display Attribute: USERNAME

Identity Attribute: id

Instance Attribute:

Remediation Modifiable: Readonly ▾

Attributes

	Name	Description	Type	Properties	
□	active	A Boolean value indicating the User's administrative stat	boolean ▾		Edit
□	USERNAME	A service provider's unique identifier for the user, typicall	string ▾		Edit
□	USER-ID	The user id of a user on the NonStop.	string ▾		Edit
□	ALIAS	The ALIAS keyword specifies user alias as the type of ol	string ▾		Edit

SailPoint IdentityIQ will send a "GET" web request to the service and return a list of all attributes that are supported by XIC. Once returned, the fields in the table will be populated with those attributes and their descriptions. Scroll down to the bottom of the window and then click the **Save** button to save the schema.

Correlating NonStop User Attributes with SailPoint Attributes

On the SailPoint IdentityIQ *Correlation* tab you must correlate application-specific attributes (user attributes on the NonStop) with attributes on Sailpoint IdentityIQ. Please refer to the "Configure Applications" chapter in the *SailPoint IdentityIQ Administration Guide* for more information.

Enabling Access to the NonStop Application

Use the SailPoint IdentityIQ Lifecycle Manager to configure and enable access to the NonStop application you configured above. Please refer to the chapters in the "Lifecycle Manager" section in the *SailPoint IdentityIQ User's Guide* for more information.

Configuring Aggregation

SailPoint IdentityIQ uses aggregation to copy all user records from the NonStop server to SailPoint IdentityIQ. You must configure a task in SailPoint IdentityIQ to enable aggregation. Please refer to the "Tasks" chapter in the *SailPoint IdentityIQ Administration Guide* for more information.

Glossary

A

Account - SailPoint

An identity's association to a specific application/system in SailPoint IdentityIQ.

Aggregation - SailPoint

The pulling of all user accounts on a system through a SailPoint IdentityIQ task.

Application - SailPoint

SailPoint IdentityIQ's way of configuring and connecting to a specific service/system.

Attribute

A specific property for an account related to a given system.

I

Identity - SailPoint

A unique user that is associated with zero or more accounts.

IdentityIQ

An open identity and access management platform developed by SailPoint.

J

JKS

The Java Keystore (JKS) is the repository for security certificates used by XIC.

JSON

JavaScript Object Notation. An object structure used by SCIM to carry user data from one system to the next. It is based on key value pairs.

N

NonStop

A fault tolerant server developed by Hewlett Packard Enterprise (HPE).

R

Resource (SCIM)

An accumulation of attributes and their schemas for a given account on a specific application/system.

REST

Representational State Transfer. An architecture style for web services that provides communication between two or more systems.

S

Schema (SCIM)

A schema is the detail about an attribute. The schema defines the data type, the uniqueness, along with other defining features for the attribute.

SCIM

System for Cross-domain Identity Management. An industry standard protocol used for user identity provisioning and management.

X

XYGATE Products

A set of XYPRO product configuration files collected when the "XYGATE Products" check box is selected. These product files display under the XYGATE Products tree entity and have a range of files; *ACL, *CONF, FILTERS, and GLOBALAG files are collected if the NonStop server contains these installations and are configured in the TRACL file for the connect node.