

XYPRO Technology Corporation

XYGATE® Identity Connector (XIC) Design Document

Version 1.10



Email: support@xypro.com

Telephone: +1 805-583-2874

FAX: +1 805-583-0124

XYGATE® Identity Connector 1.10 Design Document

Copyright 2018 XYPRO Technology Corporation. All rights reserved.

This document, as well as the software described in it, is furnished under a License Agreement or Non-Disclosure Agreement. The software may be used or copied only in accordance with the terms of the Agreement. Use of this manual constitutes acceptance of the terms of the Agreement. No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, and translation to another programming language, for any purpose without the written permission of XYPRO Technology Corporation.

Trademarks

XYGATE®, SecurityOne®, and XYPRO® are registered trademarks of XYPRO Technology Corporation. XYGATE® Configuration Manager™ (XCM), XYGATE® Encryption Library™ (XEL), XYGATE® Event Monitor™ (XEM), XYGATE® Key Management™ (XKM), XYGATE® Merged Audit® (XMA), XYGATE® Object Security™ (XOS), XYGATE® Audit Report Manager™ (XRM), XYGATE® Compliance Pro™ (XSW), XYGATE® Transaction Router™ (XTR), and XYGATE® User Authentication™ (XUA) are trademarks of XYPRO Technology Corporation.

All other brand or product names, trademarks or registered trademarks are acknowledged as the property of their respective owners

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 and Overview	5
Purpose	5
Overview of the Design	5
About the Service	5
Unsupported Features	6
Chapter 2: Framework	7
Framework Overview	7
Service Communication	7
Transport (HTTP/S)	7
SCIM Protocol	8
Authentication and Authorization	8
XYGATE Transaction Router (XTR)	8
Auditing and Logging	9
Chapter 3: Functionality	10
Aggregation	11
Create/Delete	12
Freeze/Thaw Instantly	12
Appendix A: Create/Get Request Example	13
Glossary	14

Chapter 1: Introduction and Overview

Purpose

This document provides a high-level overview of the design and functionality of XYGATE Identity Connector (XIC).

Overview of the Design

XIC provides an easy way to integrate your HPE NonStop servers with your enterprise identity connector software. This allows for complete user governance, provisioning, and reconciliation of NonStop user accounts directly from your Identity and Access Management (IAM) system, such as SailPoint. Controlling access to a company's servers and applications are critical to security. Without centralized identity management, onboarding and offboarding employees becomes a manual process that is not only time consuming but introduces a security risk. XIC provides you with complete control over who has access to your NonStop servers from a single enterprise location.

About the Service

Service Communication

XIC uses the standards for web services: HTTPS, JSON, and SSL. It adheres to the standards-based SCIM 2.0 protocol for identity management. SailPoint IdentityIQ sends and receives requests over HTTPS. XYGATE Transaction Router (XTR), which provides a secure and efficient communications channel for task executions on HPE NonStop servers, filters validation, and execution of requests. With the service standards, the SCIM protocol, and XTR guarantee the entire request from start to finish is secure.

Authentication and Authorization

Each request that comes in to XIC requires authentication through XTR before XIC executes a request. If XTR does not present valid credentials, the service will completely reject the request. Each request logs the user's username and the requested operation to the audit log to provide an audit of all requested XIC-supported endpoints.

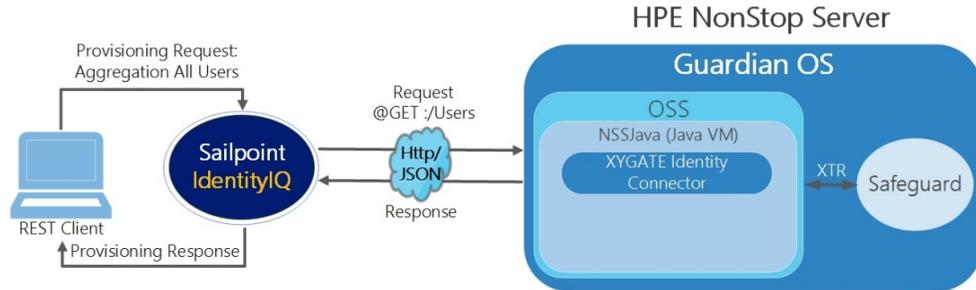
Auditing and Logging

XIC audits and logs all requests to the service. The auditing contains all information necessary to determine what actions were executed, by whom (username), when (date and time), and source (requester IP address). You can then incorporate this information into your enterprise Security Information and Event Management (SIEM) system.

The diagrams below depict the service and how it runs. SailPoint IdentityIQ and XIC package all data communicated between each other as JSON objects.

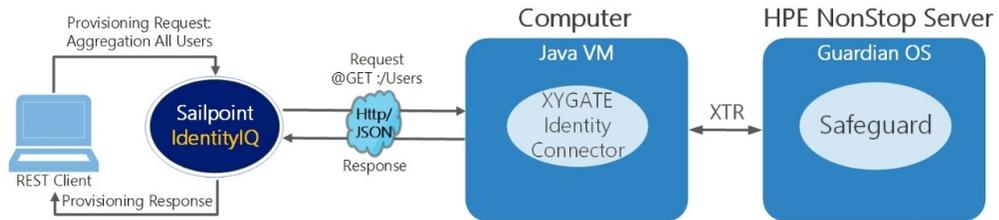
Configuration #1: XIC running directly on the NonStop

XIC



Configuration #2 XIC running directly on Windows

XIC



Unsupported Features

XIC does not support the following:

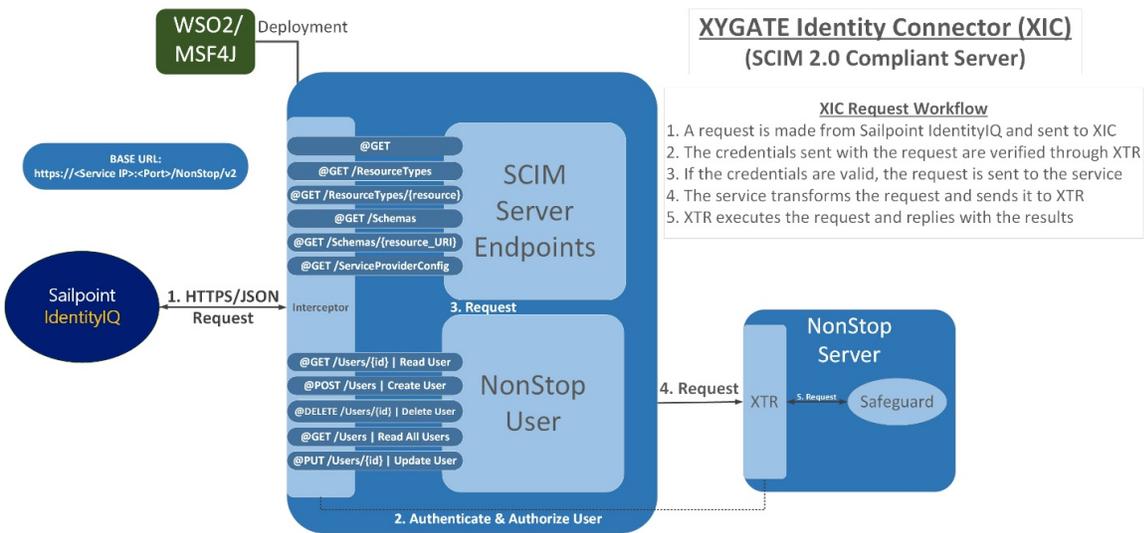
- @PATCH (updates to users) operations
- Group Resource
- Bulk operations

Chapter 2: Framework

Framework Overview

XIC is built upon a flexible, highly scalable, and lightweight Java-based micro services framework (MSF4J) with container-based deployment. It provides high performance HTTP/HTTPS transports based on Netty 4.0. The user provisioning agent module is deployed as a SCIM 2.0 compliant server with extensions to support HPE NonStop server user attributes.

See the following diagram for a more in-depth look at the structure of XIC.



Service Communication

Transport (HTTP/S)

All communication from the web client application to the XIC web service occurs over HTTP or HTTPS transport protocol. HTTPS is configured in a YAML configuration file that is loaded by Netty at startup. As with any trusted secure communications, a valid keystore and a valid certificate are required.

SCIM Protocol

The System for Cross-domain Identity Management (SCIM) standard simplifies user management in the cloud by defining a schema for representing users and groups and a REST API for all the necessary CRUD operations. SCIM is a protocol that is based on HTTP ([RFC7230](#)). Along with HTTP headers and URLs, SCIM uses JSON ([RFC7159](#)) payloads to convey SCIM resources, as well as protocol-specific payload messages that convey request parameters and response information such as errors. Both resources and messages pass between XIC and SailPoint IdentityIQ in the form of JSON-based structures in the message body of an HTTP request or response. To identify this content, SCIM uses a media type of "application/scim+json".

The SCIM protocol specifies well-known endpoints and HTTP methods for managing resources defined in the SCIM Core Schema document ([RFC7643](#)). XIC supports the following endpoints.

HTTP Method	SCIM Usage
GET	Retrieves one or more complete or partial resources.
POST	Depending on the endpoint, creates new resources or creates a search request
PUT	Modifies a resource by replacing existing attributes with a specified set of replacement attributes (replace). Do NOT use PUT to create new resources.
DELETE	Deletes a resource.

Authentication and Authorization

To ensure security for the service, every request made to the system must be valid and authenticated. XIC uses basic authentication but the credentials supplied by the SailPoint application must be a valid HPE NonStop user with security administration access rights.

XYGATE Transaction Router (XTR)

XTR is a framework that provides client applications with efficient communication and task executions on HPE NonStop servers. XTR implements a proprietary protocol for client/server communications. This protocol is based on messages over TCP sockets. Services provided are encryption, connection pooling, task management, authentication, and authorization for the HPE NonStop server.

Auditing and Logging

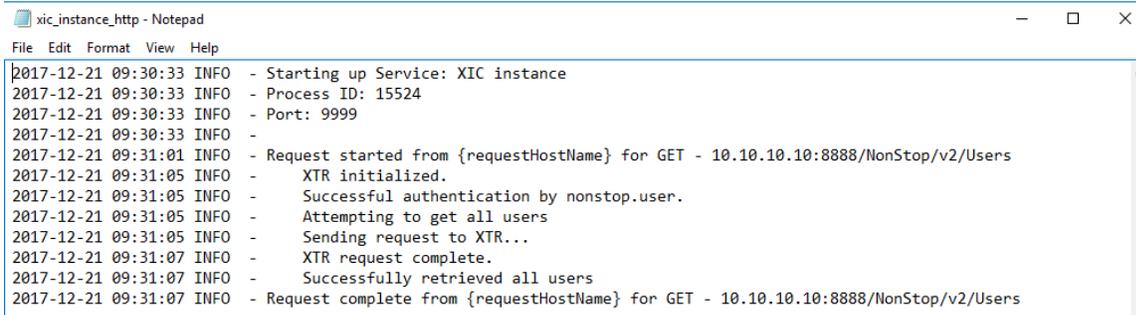
XIC audits and logs all requests for configured endpoints and records the following information:

- Date and time
- Username and IP address of the requester
- Type of request the requester is trying to make
- If they have valid credentials to access the system
- If the request was successfully executed

XIC uses three different logs to record information for the service: **Audit**, **Error**, and **HTTP**.

- **Audit Log**: Contains information about the requester, the type of request, the data they are attempting to send, and if the request was successful.
- **Error Log**: Contains logs of any error that occurs while the service is running.
- **HTTP Log**: Contains some audit and all error log information, step by step info of the request coming in, along with service specific information (e.g., what port its running on, the Process ID).

The following shows an example of an HTTP log.



```
xic_instance_http - Notepad
File Edit Format View Help
2017-12-21 09:30:33 INFO - Starting up Service: XIC instance
2017-12-21 09:30:33 INFO - Process ID: 15524
2017-12-21 09:30:33 INFO - Port: 9999
2017-12-21 09:30:33 INFO -
2017-12-21 09:31:01 INFO - Request started from {requestHostName} for GET - 10.10.10.10:8888/NonStop/v2/Users
2017-12-21 09:31:05 INFO - XTR initialized.
2017-12-21 09:31:05 INFO - Successful authentication by nonstop.user.
2017-12-21 09:31:05 INFO - Attempting to get all users
2017-12-21 09:31:05 INFO - Sending request to XTR...
2017-12-21 09:31:07 INFO - XTR request complete.
2017-12-21 09:31:07 INFO - Successfully retrieved all users
2017-12-21 09:31:07 INFO - Request complete from {requestHostName} for GET - 10.10.10.10:8888/NonStop/v2/Users
```

Chapter 3: Functionality

All functionality of XIC is accessed through the service's endpoints. The base URL for the service is as follows:

https://<Service IP>:<Port>/NonStop/v2

Important: The URL is case sensitive.

The table below lists the base SCIM endpoints XIC offers that are geared towards information about the service and provide for communication between XIC and SailPoint.

Functionality	HTTP Method Type	Endpoint
Schemas	@GET	/NonStop/v2/Schemas
Specific Schema	@GET	/NonStop/v2/Schemas/{URL}
Resources	@GET	/NonStop/v2/ResourceTypes
User Resource	@GET	/NonStop/v2/ResourceTypes/User
Service Config	@GET	/NonStop/v2/ServiceProviderConfig

NonStop User URL: com:xypro:nonstop:User

XIC extends the current SCIM user attribute list to cover most of the HPE NonStop user attributes. This provides complete control over a user and his or her assets on a NonStop system.

XIC supports the following attributes that are HPE NonStop user specific.

- Remote Password
- Username
- Text Description
- User-ID
- Guardian [Default] Security
- Owner
- Guardian [Default] [Sub]Volume
- Password
- Initial Directory
- User-Expires
- Initial Program
- Password Must Change
- Initial Progtype
- Password Expiry Grace

- CI Prog
- Password Expires
- CI Lib
- Audit Authenticate Pass
- CI CPU
- Audit Authenticate Fail
- CI Name
- Audit Manage Pass
- CI Swap
- Audit Manage Fail
- CI PRI
- Audit User Action Pass
- CI Param Text
- Audit User Action Fail

The following HPE NonStop user-specific attributes are unsupported on XIC.

- Owner List
- Default Protection

Aggregation

XIC can aggregate user accounts from across your HPE NonStop servers into IdentityIQ. This provides a central and convenient repository that associates NonStop accounts with their enterprise identity.

Functionality	HTTP Method Type	Endpoint
All Users	@GET	/NonStop/v2/Users
Specific User	@GET	/NonStop/v2/Users/{id}

Create/Delete

You can provision and de-provision users through SailPoint IdentityIQ. Nearly all attributes on the NonStop are completely configurable and available when provisioning a user.

Note: The only required attributes during a creation of a NonStop user are **USERNAME**, **USER-ID**, and **PASSWORD**.

Functionality	HTTP Method Type	Endpoint
Create	@POST	/NonStop/v2/Users
Delete	@DELETE	/NonStop/v2/Users/{id}

An example of a typical JSON object when creating a user is shown below:

```
{"schemas": ["com:xypro:nonstop:User"], "USER-ID": "85,15",  
"USERNAME": "nonstop.user", "PASSWORD": "Pa$55W0rD"}
```

Freeze/Thaw Instantly

You can thaw (enable) or freeze (disable) accounts on the HPE NonStop through SailPoint IdentityIQ. This provides the ability to safely restrict or provide access to a given system with a single click.

Functionality	HTTP Method Type	Endpoint
Freeze/Thaw	@PUT	/NonStop/v2/Users/{id}

Appendix A: Create/Get Request Example

The following is an example of a response object sent back from a Create/Get request from XIC to SailPoint IdentityIQ:

```
{ "BINARY-DESCRIPTION LENGTH": "0",  
  "CI-PARAM-TEXT": "",  
  "GUARDIAN DEFAULT VOLUME": "$SYSTEM.NOSUBVOL",  
  "TEXT-DESCRIPTION": "",  
  "FROZEN/THAWED": "THAWED",  
  "CREATOR-USER-TYPE": "USER (255,255)",  
  "AUDIT-USER-ACTION-PASS": "NONE",  
  "PASSWORD-EXPIRES": "* NONE *",  
  "PASSWORD-MAY-CHANGE": "* NONE *",  
  "AUDIT-MANAGE-FAIL": "NONE", "CI-CPU": "* NONE *",  
  "CI-PRI": "* NONE *",  
  "CI-LIB": "* NONE *",  
  "GROUP": " NONSTOP ",  
  "OWNER": "255,255",  
  "STATUS": "THAWED",  
  "CI-PROG": "* NONE *",  
  "INITIAL-PROGRAM": "",  
  "GUARDIAN DEFAULT SECURITY": "OOOO",  
  "INITIAL-DIRECTORY": "",  
  "LAST-LOGON": "* NONE *",  
  "USERNAME": " NONSTOP.USER",  
  "AUDIT-AUTHENTICATE-PASS": "NONE",  
  "CREATOR-NODENUMBER": "200",  
  "id": "21804",  
  "USER-ID": "85,44",  
  "AUDIT-MANAGE-PASS": "NONE",  
  "PASSWORD-MUST-CHANGE EVERY": "* NONE *",  
  "CI-NAME": "* NONE *",  
  "INITIAL-PROGTYPE": "PROGRAM",  
  "STATIC-FAILED-LOGON-RESET": "* NONE *",  
  "active": true,  
  "LAST-UNSUCCESSFUL-ATTEMPT": "* NONE *",  
  "AUDIT-AUTHENTICATE-FAIL": "NONE",  
  "AUDIT-USER-ACTION-FAIL": "NONE",  
  "CI-SWAP": "* NONE *",  
  "PASSWORD-EXPIRY-GRACE": "* NONE *",  
  "STATIC FAILED LOGON COUNT": "0",  
  "meta": {  
    "CREATION-TIME": "2018-01-19T5:29:00",  
    "location": "https://10.10.10.10:9099/NonStop/v2/Users/21804",  
    "LAST-MODIFIED": "2018-01-19T5:29:00",  
    "resourceType": "User"},  
  "schemas": ["com:xypro:nonstop:User"],  
  "CREATOR-USER-NAME": "SUPER.SUPER",  
  "USER-EXPIRES": "* NONE *",  
  "PRIMARY-GROUP": " NONSTOP "}
```

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.