

# Bifrost Installation and Configuration

## Content

Introduction

Installation

Bifrost Configuration

SXO Configuration

API calls

# Introduction

The Bifrost Middleware translates secure authenticated REST API calls from external components such as the SecureX Orchestrator to calls against on-prem devices, currently ISE over pxGrid and ERS API, Stealthwatch Enterprise over its API, or the Active Directory over LDAP

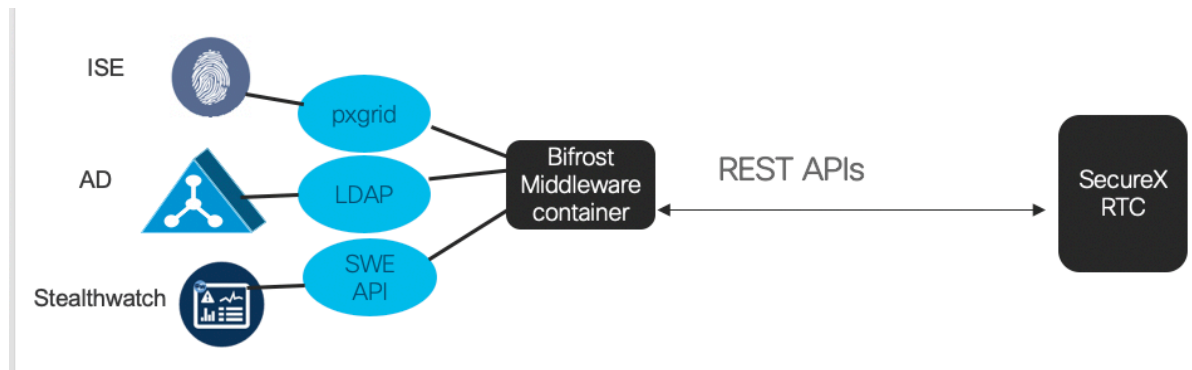


Figure 1 Bifrost Middleware - Overview

Currently the following calls are available

## **getUserByIP**

Retrieves ISE user info given IP address

## **getUserInfoByIP**

Retrieves information from ISE and Active Directory given an IP address

## **getUserInfoByUser**

Retrieves information from Active Directory given a username

## **getFlowsByIP**

Retrieves flows from Stealthwatch Enterprise given an IP address

## **getANCpolicies**

Retrieves the ANC policies defined on ISE

## **setANCpolicy**

Sets (or clears) and ANC policy given IP or MAC address.

The APIs are documented below.

# Installation

On a machine with docker and docker-compose installed, download the docker-compose.yml file from the github repository and run **docker-compose**.

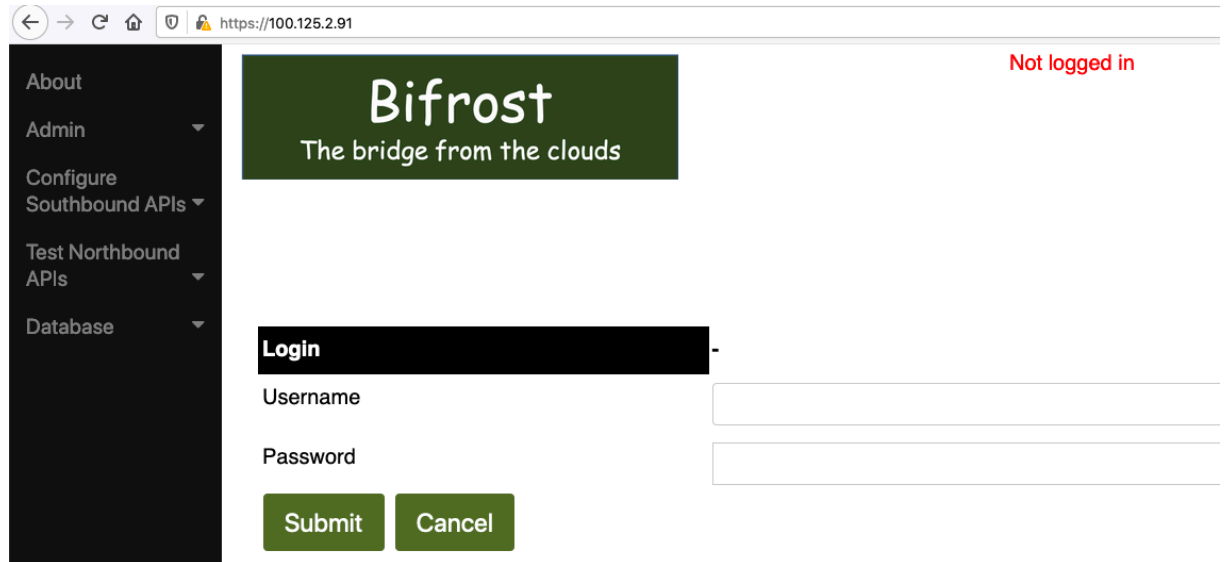
```
[ubuntu@ip-100-125-2-91:~/bifrost$ ls
README.md  docker-compose.yml
[ubuntu@ip-100-125-2-91:~/bifrost$ docker-compose up
Creating network "bifrost_my-net" with driver "bridge"
Pulling web (drnop/bifrost:latest)...
latest: Pulling from drnop/bifrost
```

*Figure 2 Installation with docker-compose*

# Configuration

## 1. Login to Bifrost Middleware Web GUI

Login to the middleware by browsing to <https://<your ip address>>. You will have to accept certificate warning.



The screenshot shows a web browser window with the address bar displaying `https://100.125.2.91`. The page layout includes a dark sidebar on the left with the following menu items: About, Admin, Configure Southbound APIs, Test Northbound APIs, and Database. The main content area has a green header with the Bifrost logo and the tagline "The bridge from the clouds". In the top right corner, it says "Not logged in". Below the header, there is a "Login" section with two input fields labeled "Username" and "Password", and two buttons labeled "Submit" and "Cancel".

Figure 3 Logging in to the Web UI

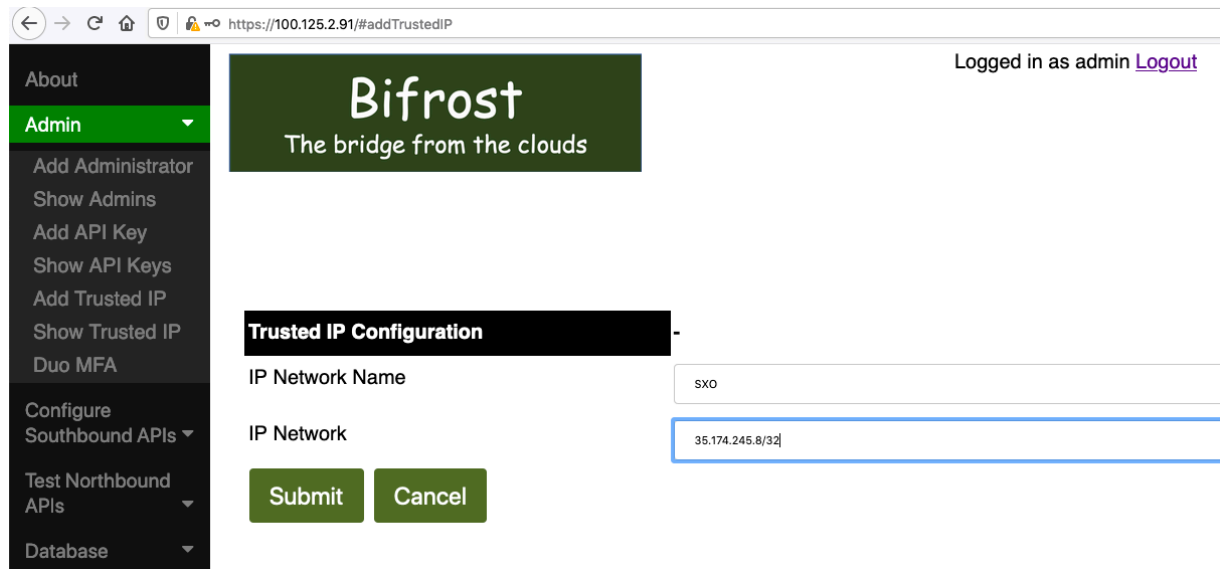
Username admin.  
Password C!sco123.

## 2. Hardening: Configure Trusted Networks.

By default, all IP addresses can connect to the middleware. Change this by

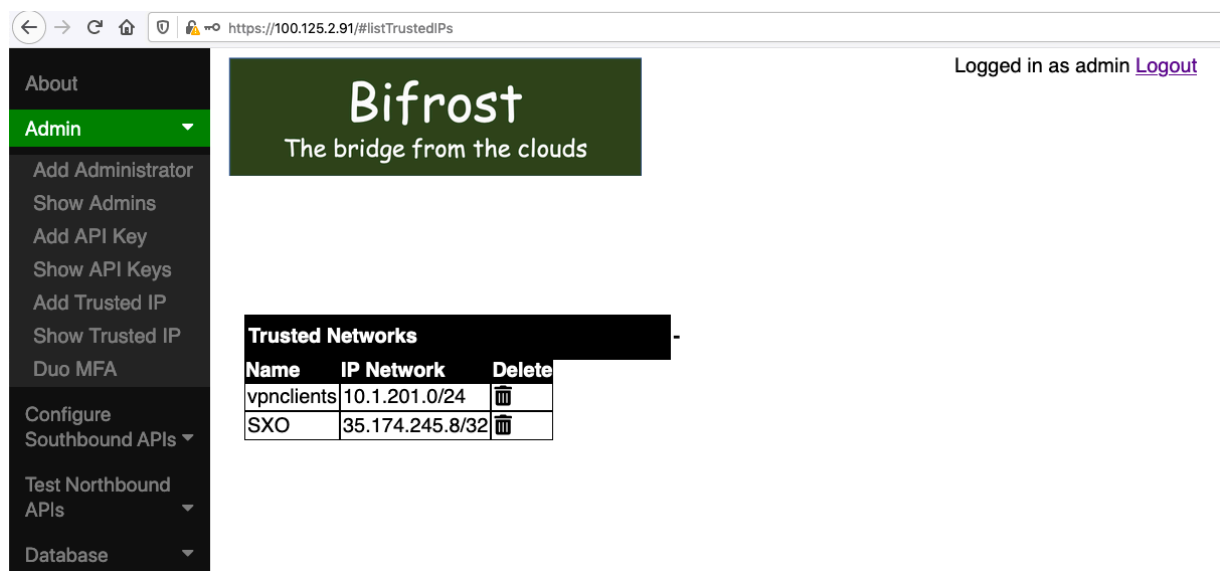
- Add a trusted network for your admins (e.g. bastion hosts)
- Add a trusted network for your SXO
- Delete the default network

You can find out the public IP of the SXO by creating a trivial workflow that connects to a REST API such as ipify.com



The screenshot shows the Bifrost Admin interface. The left sidebar has a menu with 'Admin' selected, showing options like 'Add Administrator', 'Show Admins', 'Add API Key', 'Show API Keys', 'Add Trusted IP', 'Show Trusted IP', 'Duo MFA', 'Configure Southbound APIs', 'Test Northbound APIs', and 'Database'. The main content area has a header 'Bifrost The bridge from the clouds' and a 'Trusted IP Configuration' form. The form has two input fields: 'IP Network Name' with the value 'SXO' and 'IP Network' with the value '35.174.245.8/32'. There are 'Submit' and 'Cancel' buttons. The top right shows 'Logged in as admin Logout'.

Figure 4 Adding a Trusted IP



The screenshot shows the Bifrost Admin interface with the 'Trusted Networks' table. The left sidebar is the same as in Figure 4. The main content area has a header 'Bifrost The bridge from the clouds' and a table titled 'Trusted Networks'. The table has three columns: 'Name', 'IP Network', and 'Delete'. It contains two rows: 'vpnclients' with IP '10.1.201.0/24' and 'SXO' with IP '35.174.245.8/32'. Each row has a delete icon in the 'Delete' column. The top right shows 'Logged in as admin Logout'.



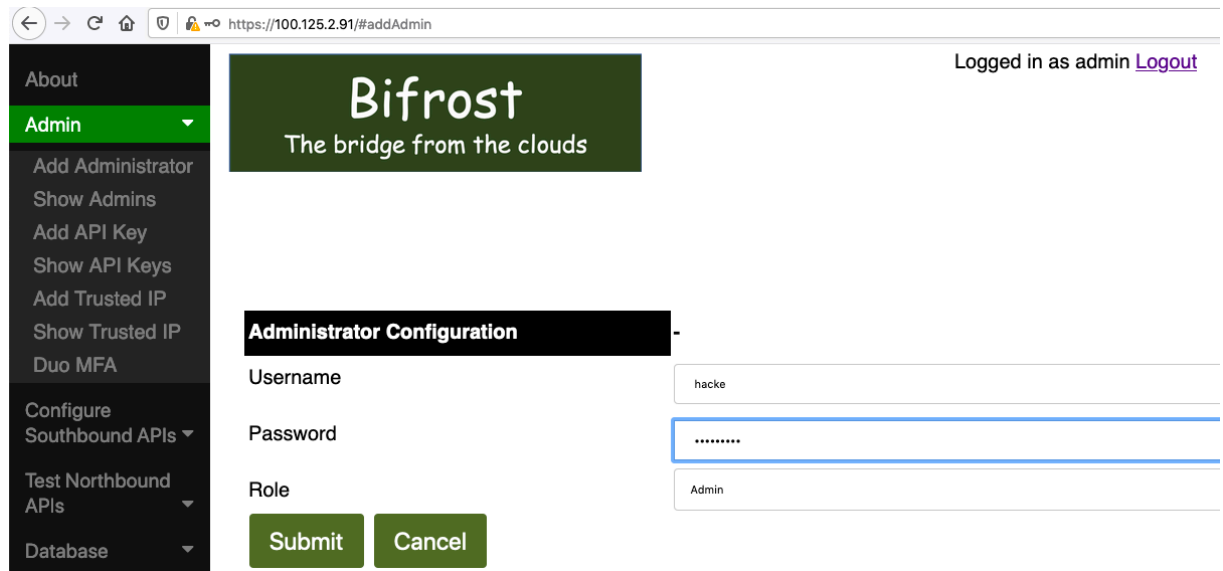
Name	IP Network	Delete
vpnclients	10.1.201.0/24	
SXO	35.174.245.8/32	

Figure 5 After adding trusted IPs and deleting default

### 3. Hardening: Add New Admin User and default admin

Add a new admin user with a password.



The screenshot shows a web browser at the URL `https://100.125.2.91/#addAdmin`. The page features a dark sidebar menu on the left with options like 'About', 'Admin', 'Add Administrator', 'Show Admins', 'Add API Key', 'Show API Keys', 'Add Trusted IP', 'Show Trusted IP', 'Duo MFA', 'Configure Southbound APIs', 'Test Northbound APIs', and 'Database'. The 'Admin' menu item is selected. The main content area has a header with the 'Bifrost' logo and the tagline 'The bridge from the clouds'. In the top right corner, it says 'Logged in as admin' with a 'Logout' link. Below the header, there is a section titled 'Administrator Configuration' with a minus sign. This section contains three input fields: 'Username' with the value 'hacke', 'Password' with masked characters '\*\*\*\*\*', and 'Role' with the value 'Admin'. At the bottom of this section are two green buttons: 'Submit' and 'Cancel'.

Figure 6 Adding a new admin user

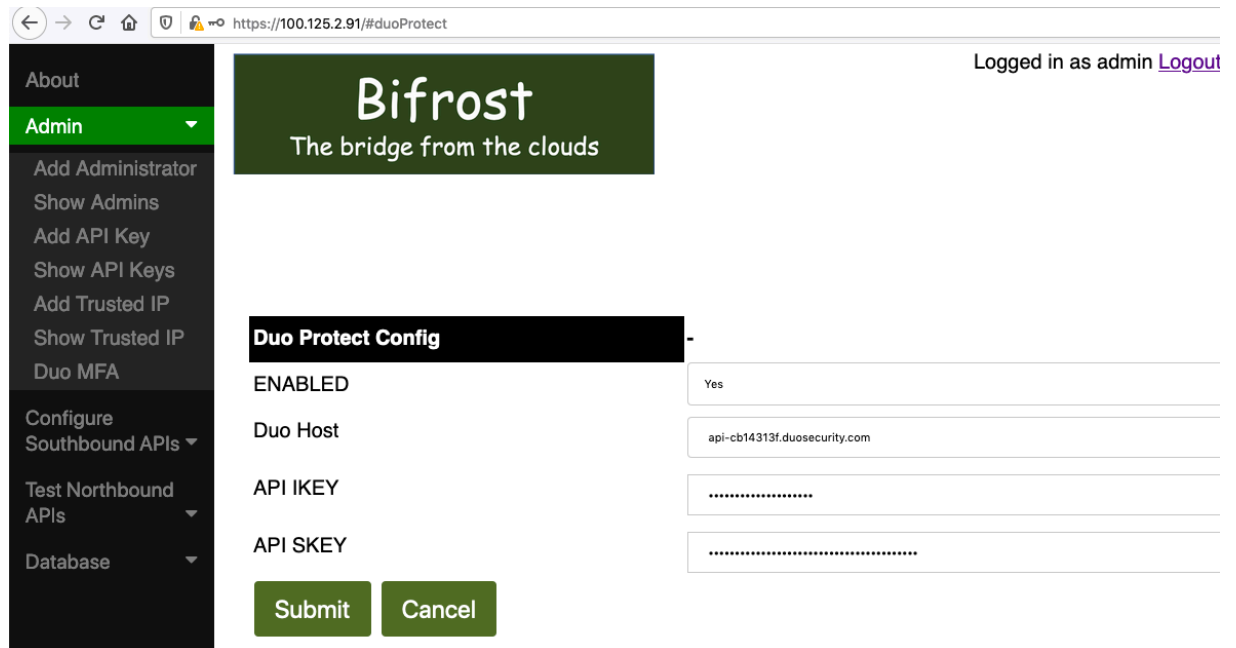
Delete the old admin user (admin).

*It is advisable to first logout and test login as the newly created user, before deleting admin account. If you want to apply Duo MFA as in step 5, it is best to wait until after Duo MFA has been implemented and tested before deleting the admin user.*

#### 4. Hardening: Configure Duo Protect to enable MFA for users.

The middleware supports MFA with Duo.

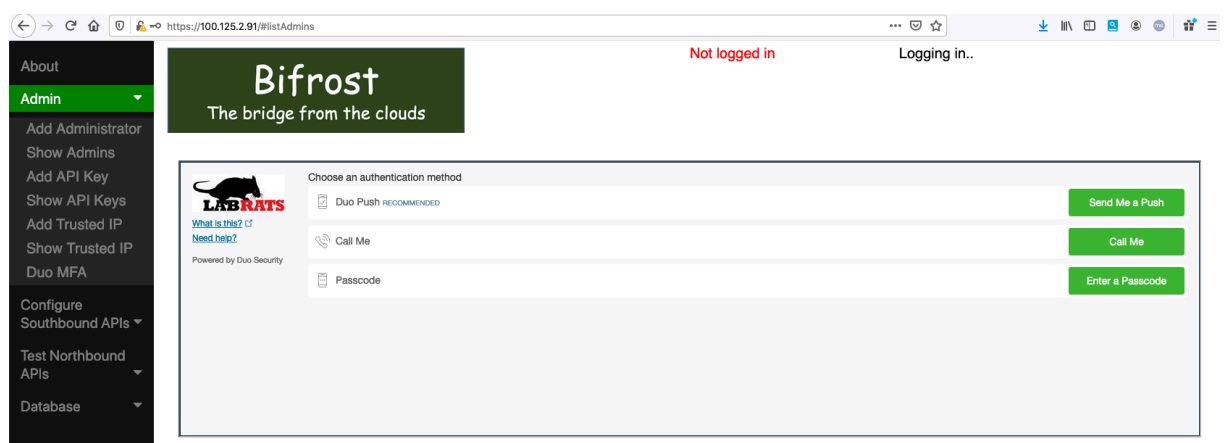
Enter the duo host, I-KEY and S-KEY (from the Duo Portal configuration).



The screenshot shows the Bifrost web interface for Duo Protect configuration. The top navigation bar includes 'About', 'Admin' (selected), and 'Logout'. The 'Admin' dropdown menu lists options: 'Add Administrator', 'Show Admins', 'Add API Key', 'Show API Keys', 'Add Trusted IP', 'Show Trusted IP', and 'Duo MFA'. The main content area is titled 'Duo Protect Config' and shows the status as 'ENABLED'. Below this, there are fields for 'Duo Host' (api-cb14313f.duosecurity.com), 'API IKEY' (masked with dots), and 'API SKEY' (masked with dots). There are 'Submit' and 'Cancel' buttons at the bottom.

Figure 7 Duo Protect Configuration

After configuring Duo Protect, all users will require to use MFA except any user called “admin”. You can test by logging out and in again with any username except “admin”.



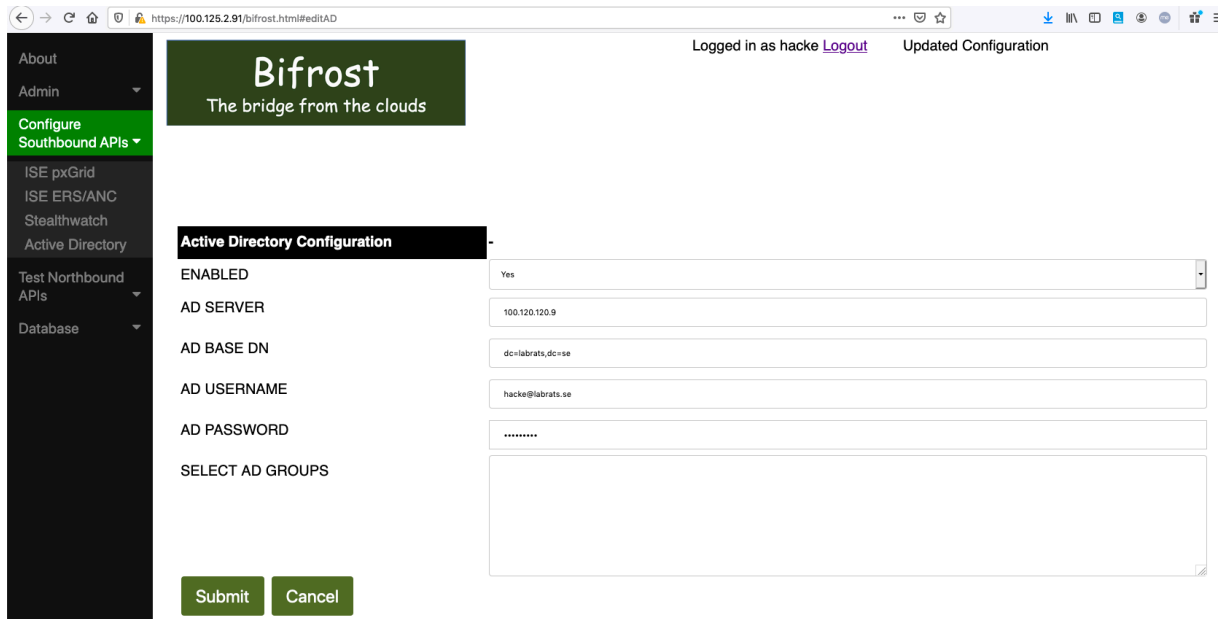
The screenshot shows the Bifrost login page. The top navigation bar includes 'About', 'Admin' (selected), and 'Logout'. The main content area is titled 'Choose an authentication method'. It lists three options: 'Duo Push RECOMMENDED' with a 'Send Me a Push' button, 'Call Me' with a 'Call Me' button, and 'Passcode' with an 'Enter a Passcode' button. The page also displays 'Not logged in' and 'Logging in..'.

Figure 8 Logging in with Duo MFA

## 5. Configure and Test the Active Directory Interface

Configure the Active Directory interface with

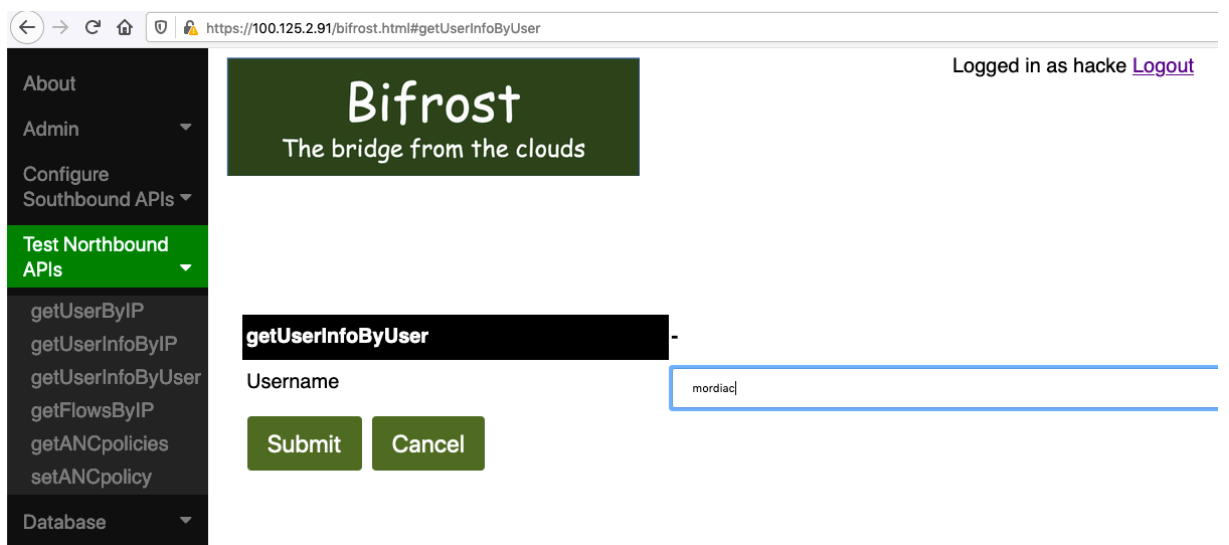
- Enabled Yes
- Server IP
- Base DN
- The username and password of a user that can browse the Active Directory



The screenshot shows the Bifrost web interface at the URL `https://100.125.2.91/bifrost.html#editAD`. The user is logged in as 'hacke' and the configuration was updated. The left sidebar has a menu with 'About', 'Admin', 'Configure', 'Test Northbound APIs', and 'Database'. The 'Configure' menu is expanded, showing 'Southbound APIs' and 'Active Directory'. The 'Active Directory Configuration' form is displayed with the following fields: 'ENABLED' (set to 'Yes'), 'AD SERVER' (set to '100.120.120.9'), 'AD BASE DN' (set to 'dc=labrats,dc=se'), 'AD USERNAME' (set to 'hacke@labrats.se'), 'AD PASSWORD' (masked with dots), and 'SELECT AD GROUPS' (empty). 'Submit' and 'Cancel' buttons are at the bottom.

Figure 9 Configuring Active Directory

You can test the Active Directory Interface by searching for a user that exists in the active directory. Test Northbound APIs/`getUserInfoByUser` and specify a valid username in the AD. You will get an alert showing the API request, and the response returned from the middleware.



The screenshot shows the Bifrost web interface at the URL `https://100.125.2.91/bifrost.html#getUserInfoByUser`. The user is logged in as 'hacke'. The left sidebar has a menu with 'About', 'Admin', 'Configure', 'Test Northbound APIs', and 'Database'. The 'Test Northbound APIs' menu is expanded, showing a list of APIs: 'getUserByIP', 'getUserInfoByIP', 'getUserInfoByUser', 'getFlowsByIP', 'getANCPolicies', 'setANCPolicy', and 'Database'. The 'getUserInfoByUser' API is selected. The form has a 'Username' field with the value 'mordiac' and 'Submit' and 'Cancel' buttons.



Figure 10 Test AD configuration



/cgi-bin/getUserInfoByUser.py/?username=mordiac

mordiac

OK

**getUserInfoByUser**

**getUserInfoByUser**

```
{
  "rtcResult": "OK",
  "ad_info": {
    "memberOf": [
      "CN=Cats,CN=Users,DC=labrats,DC=se",
      "CN=PostureCheck,OU=Lab,DC=labrats,DC=se",
      "CN=Network Configuration Operators,CN=Builtin,DC=labrats,DC=se",
      "CN=Domain Admins,CN=Users,DC=labrats,DC=se",
      "CN=Enterprise Admins,CN=Users,DC=labrats,DC=se"
    ],
    "mail": "mordiac@labrats.se",
    "badPasswordTime": "2021-03-15 08:21:31.494835+00:00",
    "lastLogon": "2021-03-16 15:14:08.155075+00:00",
    "badPwdCount": "0",
    "userPrincipalName": "mordiac@labrats.se",
    "distinguishedName": "CN=mordiac,OU=WiredDot1X,OU=Lab,DC=labrats,DC=se",
    "sAMAccountName": "mordiac"
  }
}
```

Figure 11 Test AD result (displaying groups and other info)

## 6. Configure and Test the ISE pxGrid Interface

The middleware currently only supports authentication with (dynamically generated) pre-shared key to the pxGrid bus. Manual Approval in the ISE GUI is therefore required.

Prepare by opening a separate tab in your browser and login to ISE, browsing to the page with pxGrid clients (ISE : Administration/pxGrid Services)

In the middleware, configure the ISE API by specifying

- Enabled Yes
- IP address of ISE server
- Nodename of pxGrid client, e.g. the middleware (must be unique)

The screenshot shows the Bifrost web interface. The top header includes the Bifrost logo and the tagline 'The bridge from the clouds'. The top right corner shows the user is logged in as 'hacke' with a 'Logout' link. The left sidebar contains navigation links: 'About', 'Admin', 'Configure Southbound APIs', 'Test Northbound APIs', and a list of API endpoints. The main content area is titled 'pxGrid Configuration' and contains the following fields:

Configuration Item	Value
ENABLED	Yes
Activated (SET DYNAMICALLY)	
ISE SERVER	100.120.120.38
PXGRID NODE NAME	bifrost003
PXGRID AUTHENTICATION	Manual approval from ISE GUI
PXGRID PASSWORD (SET DYNAMICALLY)	

Figure 12 Configure ISE

After submitting the ISE configuration, you must approve the client in the ISE GUI. This has to be done within 4 minutes from configuring ISE in the middleware.

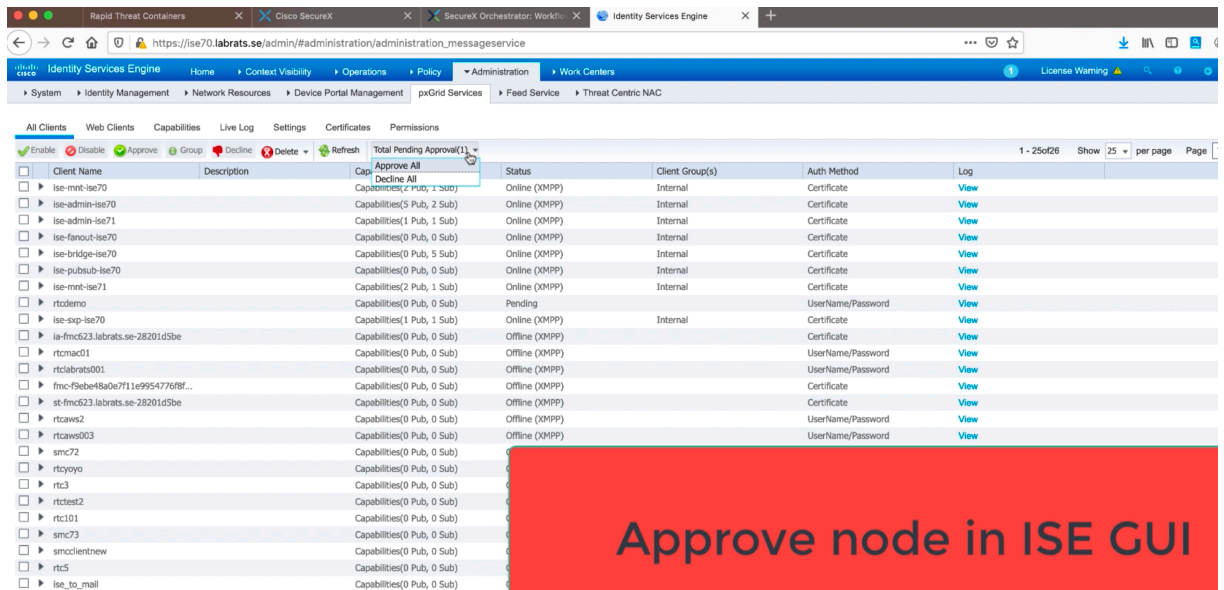


Figure 13 Approve pxGrid node in ISE GUI

You can test the ISE pxGrid connection by searching ISE API for an IP address, which should return the session data for that IP. Test Northbound APIs/getUserByIP.

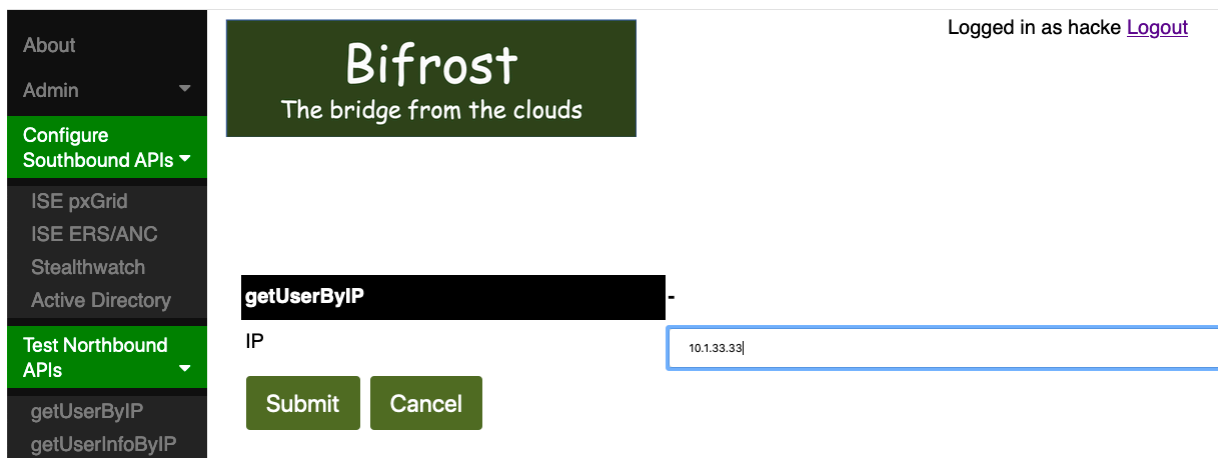
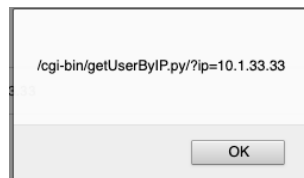


Figure 14 Testing ISE pxGrid API



**getUserByIP**

**getUserByIP**

```
{
  "timestamp": "2021-03-17T15:42:33.916Z",
  "state": "STARTED",
  "userName": "CN=garfield,OU=WiredDot1X,OU=Lab,DC=labrats,DC=se",
  "callingStationId": "00:50:56:8B:95:4A",
  "calledStationId": "A0:F8:49:0F:9A:83",
  "auditSessionId": "FD28010A0000072E40DA53D4",
  "ipAddresses": [
    "10.1.33.33"
  ],
  "macAddress": "00:50:56:8B:95:4A",
  "nasIpAddress": "10.1.40.253",
  "nasPortId": "GigabitEthernet1/0/3",
  "nasIdentifier": "sec9300",
  "nasPortType": "Ethernet",
  "endpointProfile": "Windows10-Workstation",
  "endpointOperatingSystem": "Windows 10 Enterprise",
  "ctsSecurityGroup": "SGcats",
  "adNormalizedUser": "CN=garfield",
  "adUserDomainName": "labrats.se",
  "adUserNetBiosName": "LABRATS",
  "adUserResolvedIdentities": "garfield@labrats.se",
  "adUserResolvedDns": "CN=garfield,OU=WiredDot1X,OU=Lab,DC=labrats,DC=se",
  "providers": [
    "None"
  ],
  "endpointCheckResult": "none",
  "identitySourcePortStart": 0,
  "identitySourcePortEnd": 0,
}
```

Figure 15 Testing ISE pxGrid API, output

## 7. Configure ISE ERS API

The ISE ERS API is used by the middleware to set and clear ANC policies (which can be done without a pxGrid configuration).

About

Admin

Add Administrator

Show Admins

Add API Key

Show API Keys

Add Trusted IP

Show Trusted IP

Duo MFA

Configure Southbound APIs

ISE pxGrid

ISE ERS/ANC

Stealthwatch

Active Directory

Test Northbound APIs

Bifrost

The bridge from the clouds

ISE ERS Configuration

ENABLED

ISE SERVER

ISE USERNAME

ISE PASSWORD

Submit

Cancel

Logged in as hacke [Logout](#)

Yes

100.120.120.38

ERSadmin

\*\*\*\*\*

The API can be tested with Test NorthBound APIs/getANCpolicies

About

Admin

Add Administrator

Show Admins

Add API Key

Show API Keys

Add Trusted IP

Show Trusted IP

Duo MFA

Configure Southbound APIs

Test Northbound APIs

getUserByIP

getUserInfoByIP

getUserInfoByUser

getFlowsByIP

Bifrost

The bridge from the clouds

getANCpolicies

Submit

Cancel

Logged in as hacke [Logout](#)

## 8. Configure Stealthwatch API

The Stealthwatch API is used to retrieve flows for a specific IP address.

The screenshot shows the Bifrost web interface. The header includes the Bifrost logo and the tagline "The bridge from the clouds". The user is logged in. The left sidebar contains a menu with options: About, Admin (selected), Add Administrator, Show Admins, Add API Key, Show API Keys, Add Trusted IP, Show Trusted IP, Duo MFA, Configure Southbound APIs (selected), ISE pxGrid, ISE ERS/ANC, Stealthwatch, Active Directory, Test Northbound APIs, and Database. The main content area displays the "Stealthwatch Configuration" form. The form has the following fields: ENABLED (Yes), SW SERVER (100.120.120.35), SW USERNAME (admin), SW PASSWORD (password), and SELECT HOST GROUPS (empty). There are Submit and Cancel buttons at the bottom.

The configuration can be tested with Test Northbound APIs/getFlowsByIP.

The screenshot shows the Bifrost web interface. The header includes the Bifrost logo and the tagline "The bridge from the clouds". The user is logged in. The left sidebar contains a menu with options: About, Admin (selected), Add Administrator, Show Admins, Add API Key, Show API Keys, Add Trusted IP, Show Trusted IP, Duo MFA, Configure Southbound APIs, Test Northbound APIs (selected), getUserByIP, getUserInfoByIP, and getUserInfoByUser. The main content area displays the "getFlowsByIP" form. The form has the following fields: IP (10.1.33.33), Days (1), Hours (1), and Minutes (1). There are Submit and Cancel buttons at the bottom.

## 9. Generate API key

The API calls are authenticated with an API key. Generate the API key and copy it to notepad or similar.

The screenshot shows the Bifrost web interface. On the left is a navigation menu with 'About' and 'Admin' (selected). The 'Admin' menu includes 'Add Administrator', 'Show Admins', 'Add API Key', 'Show API Keys', 'Add Trusted IP', 'Show Trusted IP', 'Duo MFA', 'Configure Southbound APIs', 'Test Northbound APIs', and 'APIs'. The main header area displays the 'Bifrost' logo and the tagline 'The bridge from the clouds'. In the top right corner, it says 'Logged in as hacke' with a 'Logout' link. The 'API Key Configuration' form is visible, with 'API Key Name' set to 'SXO' and 'Role' set to 'Read/Write'. There are 'Submit' and 'Cancel' buttons. Below the form, a message box indicates 'API Updated, save RTCAuth Header' and displays a long alphanumeric string. An 'OK' button is at the bottom right of the message box.

About  
Admin ▾  
Add Administrator  
Show Admins  
Add API Key  
Show API Keys  
Add Trusted IP  
Show Trusted IP  
Duo MFA  
Configure Southbound APIs ▾  
Test Northbound APIs ▾

**Bifrost**  
The bridge from the clouds

Logged in as hacke [Logout](#)

**API Key Configuration**

API Key Name: SXO

Role: Read/Write

**Submit** **Cancel**

Configuration

API Updated, save RTCAuth Header  
U1hPMjpiJ3RceDhhXHhiM31UdFx4YmRceGU2XHgwZVx4YmVceGRmXHhiMlx4OWUrflx4YjNKe1x4YjY+e1x4ZmFceDlIXHgwM3tqXHg5M1RceGFkXHg5NFx4ZGJceDlmXHgxM1x4ZWFo

Read/Write

**OK**

Figure 15 Add API key for SecureX Orchestrator.

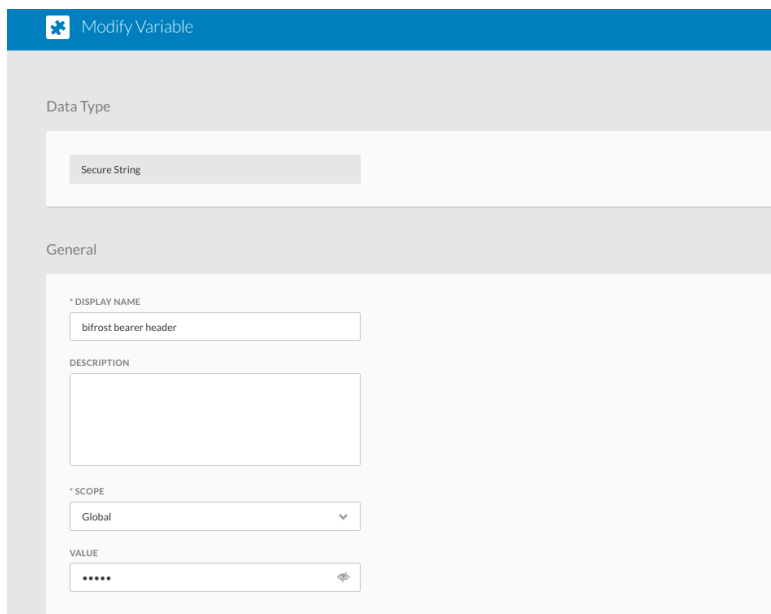
The API key has to be present in all calls in the custom header: Bearer.

**Bearer <key>**

# SecureX Orchestration Configuration

## 10. SXO – Create Secure String Variable with API Key

In SXO, create a Secure String Variable with the API key from previous step.



The screenshot shows the 'Modify Variable' configuration interface. The 'Data Type' is set to 'Secure String'. Under the 'General' tab, the 'DISPLAY NAME' is 'bifrost bearer header', the 'DESCRIPTION' is empty, the 'SCOPE' is 'Global', and the 'VALUE' is masked with five dots.


Figure 16 Create Secure String Variable with API key

## 11. SXO – Create Target

In SecureX Orchestration, create a Target that points to your Bifrost Middleware.

- Protocol HTTPS
- Specify hostname/IP of your Middleware
- Path /cgi-bin
- Check Disable Server Certificate Validation



 Modify Target

DESCRIPTION

Account Keys

NO ACCOUNT KEYS ⓘ

True

DEFAULT ACCOUNT KEYS

Select

HTTP

\* PROTOCOL

HTTPS

\* HOST/IPADDRESS

bifrost.aws.labrats.se

PORT

PATH

/cgi-bin

Figure 17 SXO - specify target

## 12. SXO - Creating web requests to the Bifrost Middleware

In SXO when you create a workflow with a web request to the Bifrost middleware, ensure that

Target is set to the target defined in previous step

The screenshot shows the 'Target' configuration panel. It has a title 'Target' and a section '\* TARGET'. There are three radio button options: 'Use Workflow Target', 'Override Workflow Target' (which is selected), and 'Use Workflow Target Group'. Below the 'Override Workflow Target' option, there is a dropdown menu labeled '\* TARGET' with the value 'bifrostaws' selected. At the bottom, there are two more radio button options: 'Use Workflow Target Group' and 'Override Workflow Target Group Criteria'.

You specify the url (relative to cgi-bin)

The screenshot shows the 'HTTP Request' configuration panel. It has a title 'HTTP Request' and a section 'RELATIVE URL' with a text input field containing the value '/getUserInfoByIP.py?ip=[\${workflow.Respond to Hacked IPorg.input.observable\_value\$}]'. Below this is a section '\* METHOD' with a dropdown menu showing 'GET'. At the bottom is a section 'REQUEST BODY' with a text input field containing the value '1'. There are 'FORMAT' and 'JSON' buttons at the bottom right.

You add a custom header named Bearer with the value of the Secure String from previous step where we set the global variable (which is the API key we created in Bifrost middleware).

The screenshot shows the 'Headers' configuration panel. It has a title 'Headers' and a section 'CONTENT TYPE' with a dropdown menu showing 'Select'. Below this is a section 'ACCEPT' with a text input field containing the value 'application/json'. At the bottom is a section 'USER-AGENT' with a text input field. Below these is a section 'CUSTOM HEADERS' with a table. The table has two columns: 'HEADER' and 'VALUE'. There is one row with the header 'Bearer' and the value '[\${global.bifrost bearer header\$}]'. At the bottom, there is an 'ADD' button.

# API Calls

Base url for all API calls <https://hostname/cgi-bin/>

Authorization is with custom Bearer header followed by the generated API keys.

API call	Relative URL	Method	Body
<b>Get User By IP</b>	/getUserByIP.py/?ip=...	GET	
<b>Get User Info from IP</b>	/getUserInfoByIP/?ip=...	GET	
<b>Get User Info from username</b>	/getUserInfoByUser/?user=...	GET	
<b>Get flows by IP</b>	getFlowsByIP.py/?ip=ip&days=1&hours=1&minutes=1	GET	
<b>Get ANC policies</b>	getANCpolicies.py	GET	
<b>Apply ANC</b>	setANCpolicy.py	POST	{"action":"Apply Policy","policy":"Qu", "ip":"10.1.33.33"}
<b>Clear ANC</b>	setANCpolicy.py	POST	{"action":"Clear Policy","policy":"Qu", "ip":"10.1.33.33"}