

vCloud Demonstration

Infoblox & ForeScout CounterACT Integration



Table of Contents

Overview	3
Description	3
Requirements	3
Demo Script	3
Infoblox Configuration Overview	3
ForeScout Configuration Overview	8
Use Case: Asset Management.....	10
Use Case: Security Remediation	17

Overview


This document describes how to demonstrate integration with ForeScout CounterACT via Infoblox's Outbound API.

The Outbound API templates are published "as is" on the Infoblox community website and are only supported via the Infoblox community website. The Infoblox community website is located at <https://community.infoblox.com/>.

Description

The lab consists of:

1. Infoblox Grid with NIOS 8.4.4
 - a. Grid Master (IB-VM-810)
2. Windows 10 workstation with ForeScout CounterACT console installed
3. ForeScout:
 - a. VCEM-5B
 - i. VTC-2000

System [Name]	Access	Login / Password
pfSense virtual router [pfSense]	172.0.0.1	admin / pfsense
Infoblox Grid Master [DDI]	https://172.0.0.3	admin / infoblox
ForeScout Enterprise Manager Console  [ForeScout]	172.0.0.14	admin / infoblox@123
Windows workstation [Win10]	172.0.0.100	rdp / rdp

Requirements

Before starting the demo ensure that the following requirements have been met:

You have internet connectivity via Google Chrome, or Firefox

You have access to the devices [DDI] and [Win10]

You have access to the device [ForeScout] via the CounterACT Console. The CounterACT Console  is located on the Task Bar of [Win10]

Demo Script

Infoblox Configuration Overview

This is an optional step to briefly overview the interface and configuration of Infoblox device [DDI] for this integration.

1. **[DDI]** Navigate to **Grid → Ecosystem → Templates**. Here you can see the templates used for this integration.

Infoblox Dashboards Data Management Smart Folders **Grid** Administration

Grid Manager Upgrade Licenses HSM Group **Ecosystem**

Outbound Endpoint Notification **Templates**

Templates

Quick Filter: None Filter On Show Filter

+ | | | | |

	NAME	VENDOR TYPE	EVENT TYPE	TEMPLATE TYPE	OUTBOUND TYPE	ADDED ON
	ForeScout Assets Mgmt	ForeScout	DHCP Lease, DB ...	Event	REST API	2018-05-18 14:58:25 PDT
	ForeScout SecEvent Mgmt	ForeScout	DNS RPZ, Analytic...	Event	REST API	2018-05-18 14:58:38 PDT

2. **[DDI]** Click the hamburger icon next to the template **ForeScout Assets Mgmt**. Select **Edit**.

Outbound Endpoint Notification **Templates**

Templates

Quick Filter: None Filter On Show Filter

+ | | | | |

	NAME	VENDOR TYPE	EVENT TYPE	TEMPLATE TYPE
	ForeScout Assets Mgmt	ForeScout	DHCP Lease, DB ...	Event
	ForeScout SecEvent Mgmt	ForeScout	DNS RPZ, Analytic...	Event

3. **[DDI]** Navigate to the **Contents** tab in the left panel. Here you can view and edit the contents of the template. Click **Cancel** when you are finished.


ForeScout Assets Mgmt (Template)

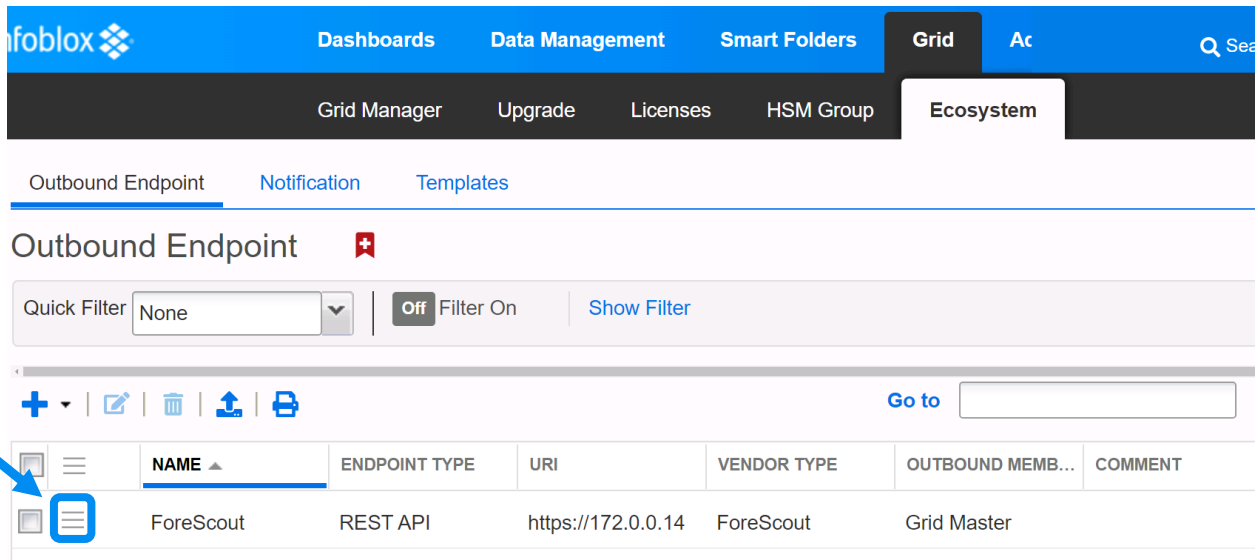
Basic

General **Contents**

```
{
  "version": "2.0",
  "name": "ForeScout Assets Mgmt",
  "comment": "Assets Management",
  "type": "REST_EVENT",
  "event_type": [
    "LEASE",
    "FIXED_ADDRESS_IPV4",
    "HOST_ADDRESS_IPV4"
  ],
  "transport": {
    "path": "/fsapi/niCore/Hosts",
    "action_type": "Assets Management",
    "content_type": "application/xml",
    "vendor_identifier": "ForeScout",
    "quoting": "XML",
    "steps": [
      {
        "name": "DebugOnStart",
        "operation": "NOP",
        "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:{UT:}}",
        "body_list": [
          {
            "name": "assignSyncTime",
            "operation": "NOP",
            "body_list": [
              "${XC:COPY:{L:SyncDate}:{UT:TIME}}${XC:FORMAT:TRUNCATE:{L:SyncDate}:{16t}}",
              {}
            ]
          }
        ]
      }
    ]
  }
}
```

Cancel Save & Close

4. **[DDI]** Navigate to **Grid → Ecosystem → Outbound Endpoint**. Select the  hamburger icon next to **ForeScout**. Select **Edit**. Here you can see the endpoint configuration with **ForeScout**. Click **Cancel** when you are finished.




Infoblox Dashboards Data Management Smart Folders Grid Ac

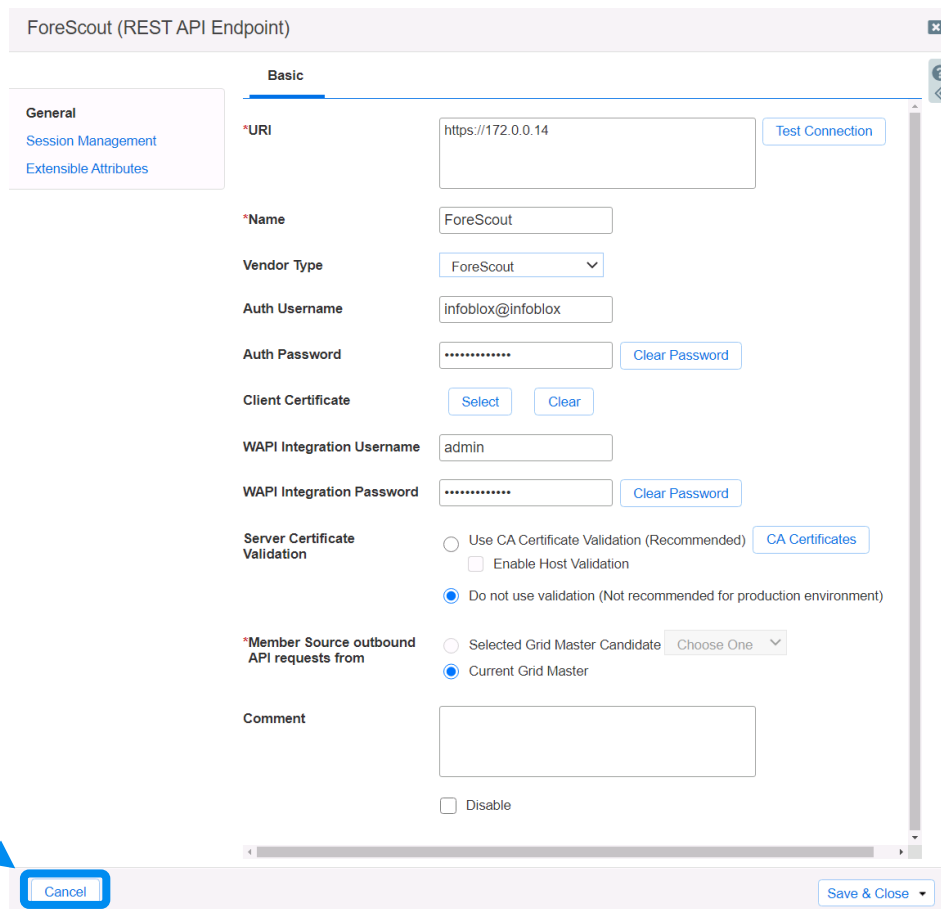
Grid Manager Upgrade Licenses HSM Group Ecosystem

Outbound Endpoint Notification Templates

Outbound Endpoint

Quick Filter: None Filter On Show Filter

	NAME	ENDPOINT TYPE	URI	VENDOR TYPE	OUTBOUND MEMB...	COMMENT
	ForeScout	REST API	https://172.0.0.14	ForeScout	Grid Master	



ForeScout (REST API Endpoint)

Basic

General
Session Management
Extensible Attributes

*URI: https://172.0.0.14 Test Connection

*Name: ForeScout

Vendor Type: ForeScout

Auth Username: infoblox@infoblox

Auth Password: Clear Password

Client Certificate: Select Clear

WAPI Integration Username: admin

WAPI Integration Password: Clear Password

Server Certificate Validation:
☐ Use CA Certificate Validation (Recommended) CA Certificates
☐ Enable Host Validation
☒ Do not use validation (Not recommended for production environment)

*Member Source outbound API requests from:
☐ Selected Grid Master Candidate Choose One
☒ Current Grid Master

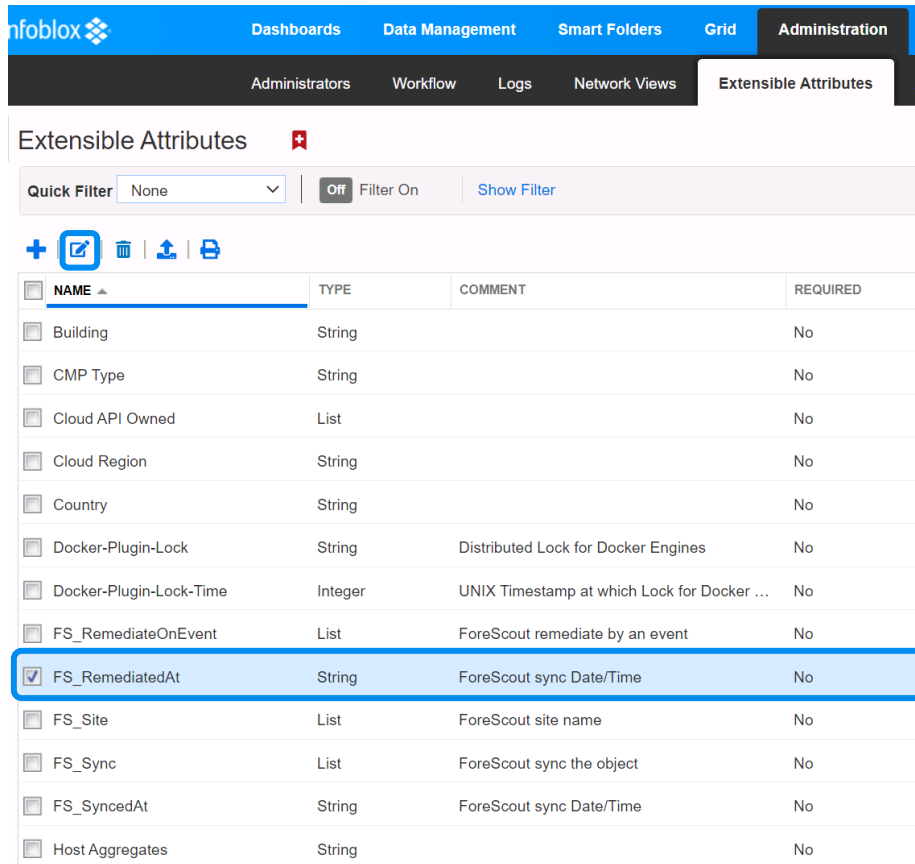
Comment:

☐ Disable

Cancel Save & Close

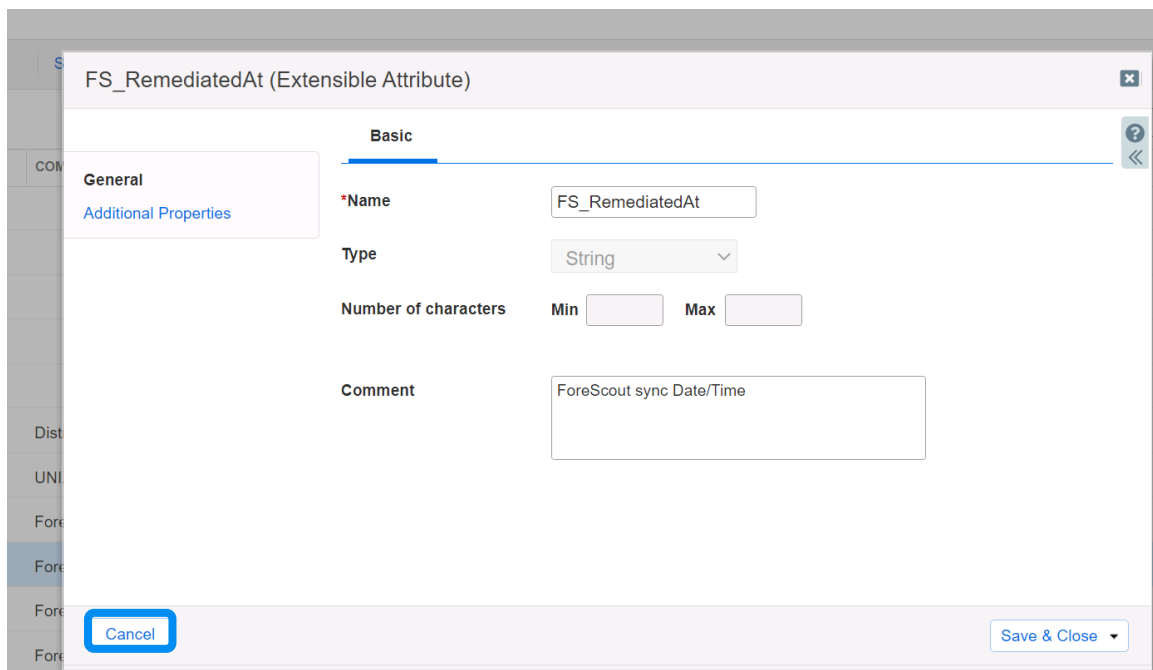
5. **[DDI]** Navigate to **Grid → Ecosystem → Notification**. **Notifications** are configurable rules that define which templates to execute when NIOS events occur under certain circumstances.

7. [DDI] Navigate to **Administration** → **Extensible Attributes**. Extensible Attributes attach additional data to objects, such as hosts. Scroll down and select **FS_RemediatedAt**. Click the **Edit** icon.



NAME	TYPE	COMMENT	REQUIRED
Building	String		No
CMP Type	String		No
Cloud API Owned	List		No
Cloud Region	String		No
Country	String		No
Docker-Plugin-Lock	String	Distributed Lock for Docker Engines	No
Docker-Plugin-Lock-Time	Integer	UNIX Timestamp at which Lock for Docker ...	No
FS_RemediateOnEvent	List	ForeScout remediate by an event	No
FS_RemediatedAt	String	ForeScout sync Date/Time	No
FS_Site	List	ForeScout site name	No
FS_Sync	List	ForeScout sync the object	No
FS_SyncedAt	String	ForeScout sync Date/Time	No
Host Aggregates	String		No

8. [DDI] Here you can view the configuration for the Extensible Attribute **FS_RemediatedAt**. Click **Cancel** when you are finished.



FS_RemediatedAt (Extensible Attribute)

Basic

General

Additional Properties

*Name

FS_RemediatedAt

Type

String

Number of characters

Min

Max

Comment


ForeScout sync Date/Time

Cancel

Save & Close

ForeScout Configuration Overview

This is an optional step to briefly overview the interface and configuration of the ForeScout device **[ForeScout]** for this integration.

1. **[Win10]** Double-click the ForeScout CounterACT console icon  pinned to the taskbar of **[Win10]**. The login credentials are found in the [Description](#) section of this script.

The image shows the ForeScout login interface. At the top, there is a logo consisting of a stylized '<)' and the text 'FORESCOUT' below it. Underneath the logo is 'Version 8.2'. The login form includes fields for 'IP/Name:' (containing '172.0.0.14'), 'Login Method:' (a dropdown menu showing 'Password'), 'User Name:' (containing 'admin'), and 'Password:'. Below these fields is a checkbox labeled 'Remember this address and user name' which is checked. At the bottom of the form is a blue button labeled 'LOG IN'.

IP/Name:
172.0.0.14

Login Method:
Password

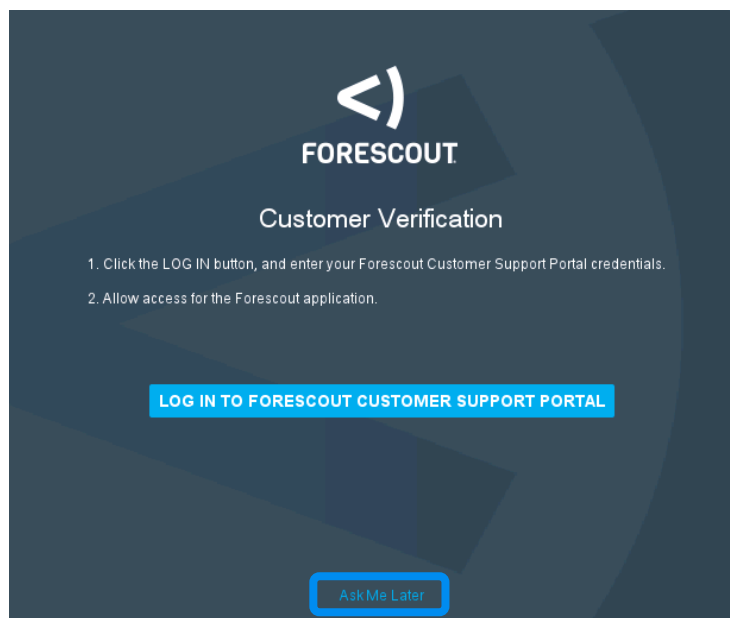
User Name:
admin

Password:

☒ Remember this address and user name

LOG IN

2. If a menu appears asking for customer verification, click **Ask Me Later**.

The image shows the 'Customer Verification' screen. It features the ForeScout logo at the top. Below the logo, the title 'Customer Verification' is centered. There are two numbered instructions: '1. Click the LOG IN button, and enter your ForeScout Customer Support Portal credentials.' and '2. Allow access for the ForeScout application.' At the bottom, there is a blue button labeled 'LOG IN TO FORESCOUT CUSTOMER SUPPORT PORTAL' and a smaller, rounded button labeled 'Ask Me Later' which is highlighted with a blue border.

Customer Verification

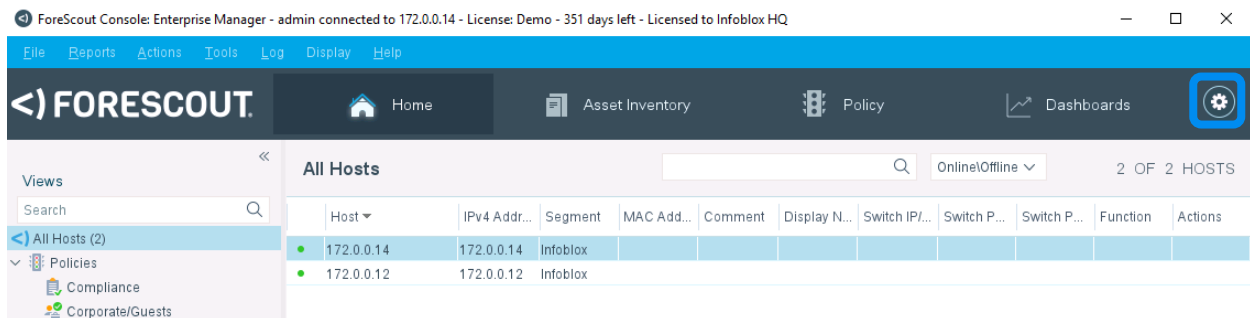
1. Click the LOG IN button, and enter your ForeScout Customer Support Portal credentials.

2. Allow access for the ForeScout application.

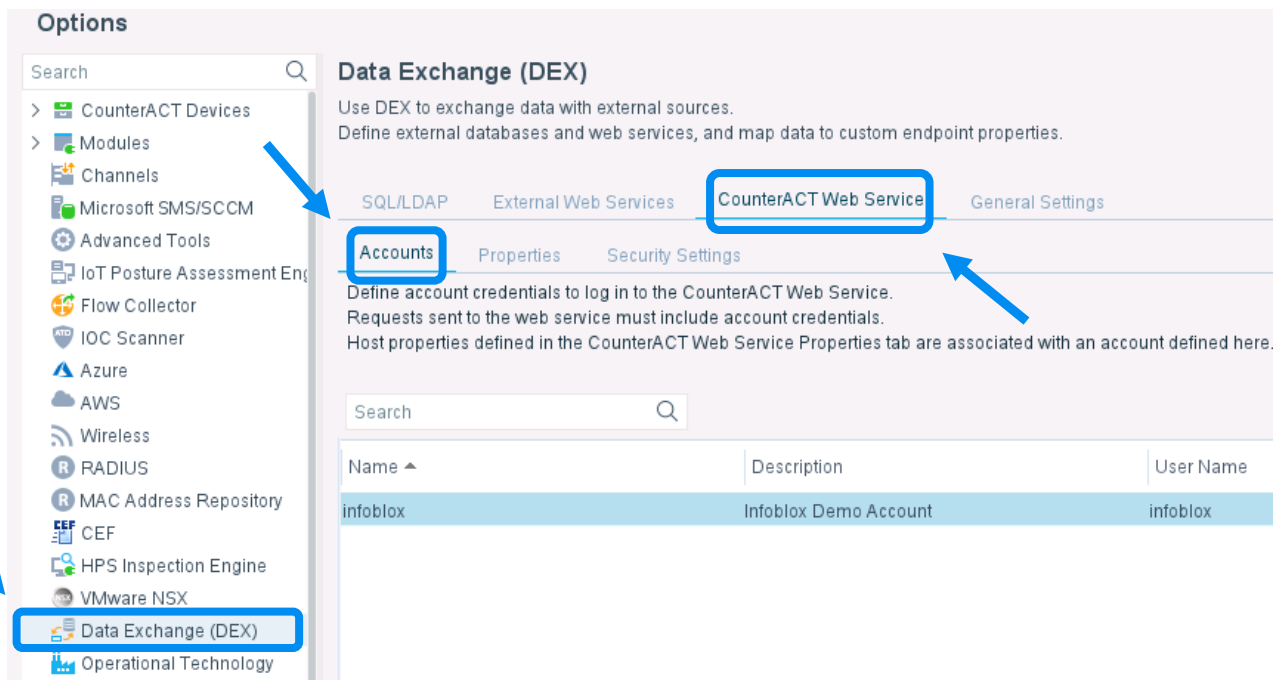
LOG IN TO FORESCOUT CUSTOMER SUPPORT PORTAL

Ask Me Later

3. **[ForeScout]** Open the **Options** menu by clicking on the **Gears** icon located on the topbar. You can also select **Tools → Options**.



4. **[ForeScout]** In the left side panel, click **Data Exchange**. Navigate to **CounterACT Web Service → Accounts**. This is the account used by the NIOS Outbound API to access the CounterACT Web Service for the integration.



5. **[ForeScout]** Click the **Properties** tab. These are the custom attributes associated with NIOS objects added to ForeScout via the Outbound API. Close the **Options** menu when you are finished viewing it.

Data Exchange (DEX)

Use DEX to exchange data with external sources.

Define external databases and web services, and map data to custom endpoint properties.

SQL/LDAP External Web Services CounterACT Web Service General Settings

Accounts **Properties** Security Settings

Define host properties that are set by the CounterACT Web Service.
Each host property defined in this tab is associated with one of the accounts in the CounterACT Web Service Accounts tab.
To set a property, a client must send a request that uses the account credentials of the associated account for authentication.

Search

Name	Description	Type ^	Account
IB_Location	Location device in the network	Composite	infoblox
IB_User	MS AD and Cisco ISE username a...	Composite	infoblox
IB_MAC	MAC Address	MAC Address	infoblox
IB_Scan	Internal field used to initiate policy ...	String	infoblox
IB_Comment	Synchronize date and time	String	infoblox
IB_Delete	Internal field used to requests asse...	String	infoblox

6. **[ForeScout]** Navigate to the **Policy** tab in the topbar. Policies govern how your assets are organized and define how ForeScout will respond to threats. View the **IB_OutboundAPI** policy here.

<) FORESCOUT

Home Asset Inventory **Policy** Dashboards

Policy Folders

Policy Manager

Search Show subfolder policies

Name	Status	User Scope	Segme...	Category	Groups	Exceptions	Conditions	Actions
> Corporate/Guest Control	Complete	172.0.0.2...	Corporat...	Linux/...			No Conditions	
✓ IB_OutboundAPI	Complete	infoblox	None				No Conditions	
Remediate							IB_Scan: Matches Remediate, Event previously detected	
Delete Assets							IB_Delete: Matches Delete, Event previously detected	
Add to Infoblox Group							IB_Location: Event previously detected	
> Primary Classification	Complete	172.0.0.2...	Classifica...				No Conditions	

Use Case: Asset Management

This use case shows how to manage assets using the ForeScout integration. This integration supports Hosts, Fixed IPs, Reservations, and IPv4 and IPv6 Leases. Additionally, ForeScout policies can be applied to delete assets when its properties change.

1. (Optional) **[DDI]** Navigate to **Grid → Ecosystem → Outbound Endpoint**. Select the icon next to **ForeScout** and click **Clear Debug Log**.
2. **[DDI]** Navigate to **Data management → IPAM → 172.0.0.0/24**.
3. **[DDI]** Let's create an **IPv4 Reservation** on the address **172.0.0.10**.

- a. Select the empty bubble for address **172.0.0.10**.

The screenshot shows the Infoblox IPAM interface. The top navigation bar includes 'Dashboards', 'Data Management', 'Smart Folders', 'Grid', and 'Adminis'. Below this, there's a 'default' dropdown and tabs for 'IPAM', 'VLANs', 'Super Host', 'DHCP', 'DNS', and 'File Distribution'. The main content area is titled 'IPAM Home' and shows the network '172.0.0.0/24' as an 'IPv4 Network'. There are tabs for 'IP Map' and 'List'. The 'IP Map' tab is active, displaying a grid of IP address bubbles. A blue arrow points to the bubble for 172.0.0.10, which is highlighted with a green border. A tooltip for this bubble shows: 'IP Address: 172.0.0.10', 'Status: Unused', and 'Usage: None'. The bottom of the grid shows the range '172.0.0.0 - 172.0.0.255'.

- b. **[DDI]** In the **Toolbar** towards the right, click the downward facing arrow to the right of **Add**. Select **IPv4 Reservation**.

The screenshot shows the 'Toolbar' dropdown menu. The 'Add' button has a downward arrow next to it, which is highlighted by a blue arrow labeled '1.'. The dropdown menu is open, showing options: 'Network', 'Range', 'Host', 'Fixed Address', 'IPv4 Reservation', 'A Record', 'Add To Existing Host', 'PTR Record', and 'AAAA Record'. The 'IPv4 Reservation' option is highlighted with a blue box and a blue arrow labeled '2.'. At the bottom of the menu, there is a 'vDiscovery' option.

- c. [DDI] Click **Save & Close**.

Add IPv4 Reservation Wizard > Step 1 of 5

☒ Add Reservation

☐ Add Reservation using Template Select Template





Cancel Previous Next Schedule for Later Save & Close

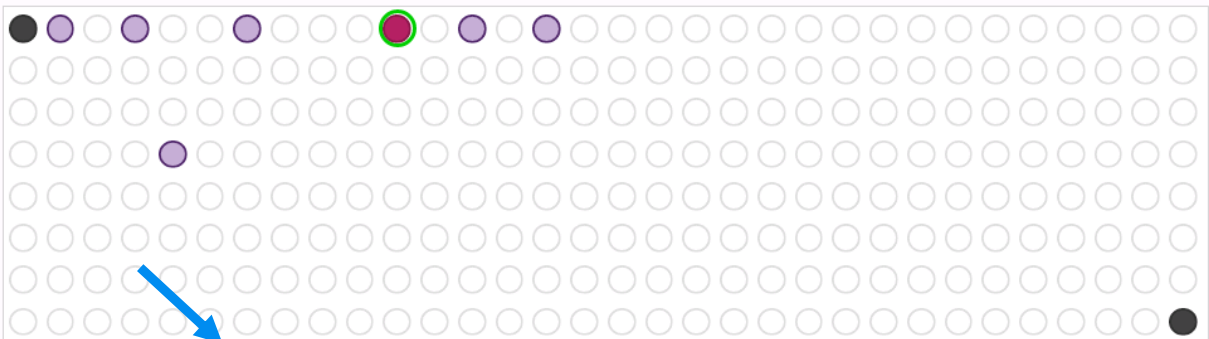
- d. [DDI] Wait at least 10 seconds. Click the **Refresh** button.


IPAM Home

172.0.0.0/24 IPv4 Network

IP Map [List](#)



 172.0.0.0 - 172.0.0.255

- e. [DDI] Scroll down to view the Extensible Attribute **FS_SyncedAt** for the newly made reservation. This value shows when the asset was added to [ForeScout].

Related Objects [Audit History](#)

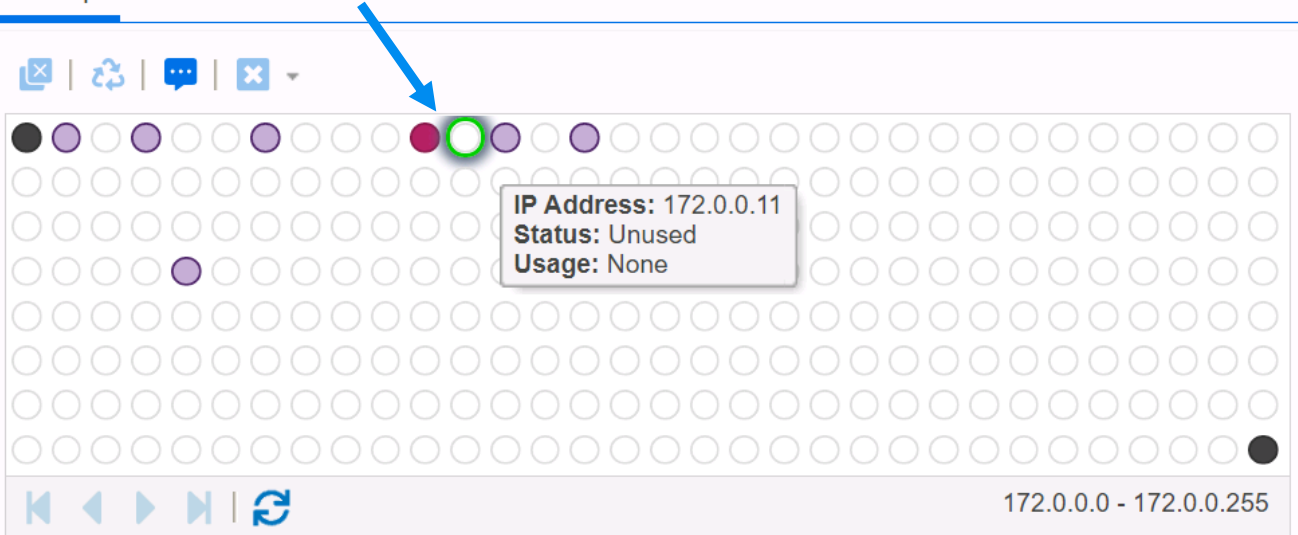
	NAME	TYPE	FS_SYNC	FS_SITE	FS_SYNCEDAT	FS_REMEDIATEDAT
		IPv4 Reservation	true	Lab	2020-10-09T00:17	

4. **[DDI]** Let's create a **Host** on the address **172.0.0.11**.
 - a. Select the empty bubble for address **172.0.0.11**.

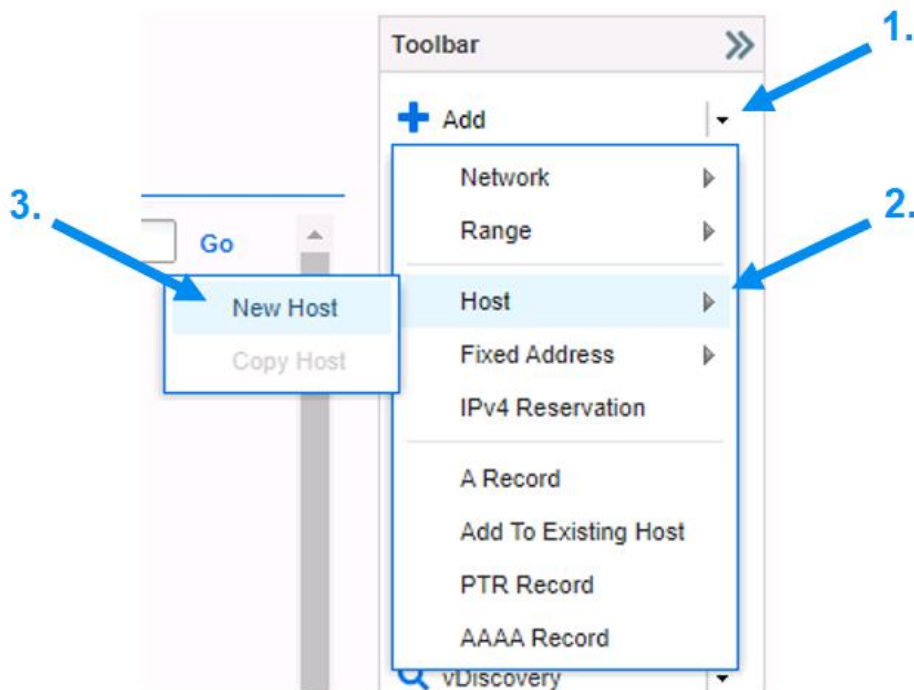
IPAM Home

172.0.0.0/24 IPv4 Network

IP Map List



- b. **[DDI]** In the **Toolbar** towards the right, click the downward facing arrow to the right of **Add**. Select **Host** → **New Host**.



c. [DDI] Give the Host a **Name**. Select the Zone **.poc.infoblox.local**. Click **Save & Close**.

Add Host Wizard > Step 1 of 3

Name: test .poc.infoblox.local Select Zone Clear

Enable in DNS: ☒

Protected: ☒ Restrict DDNS updates to this Host

Host Name Policy: Allow Underscore

To update the host settings, first complete and save the Host configuration, and then update the settings in the Host editor.

IPv4 Addresses

IPv4 ADDRESS	MAC ADDRESS	DHCP
<input checked="" type="checkbox"/> 172.0.0.11		<input type="checkbox"/>

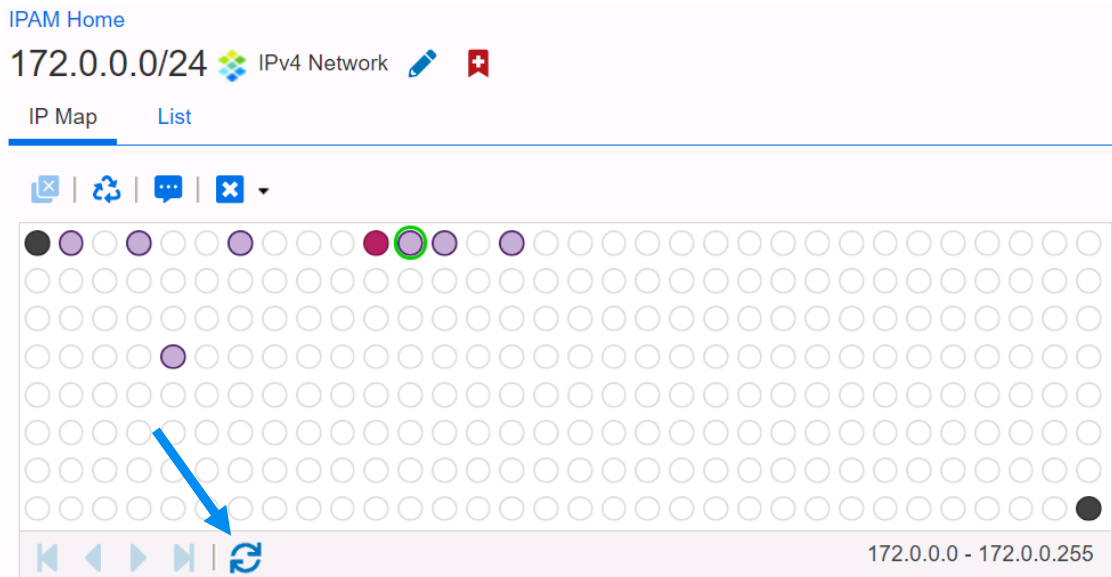
IPv6 Addresses

IPv6 ADDRESS	DUID	DHCP
No data		

IP Address for Extensible Attribute: 172.0.0.11

Cancel Previous Next Schedule for Later Save & Close

d. [DDI] Wait at least 10 seconds. Click the **Refresh** button.



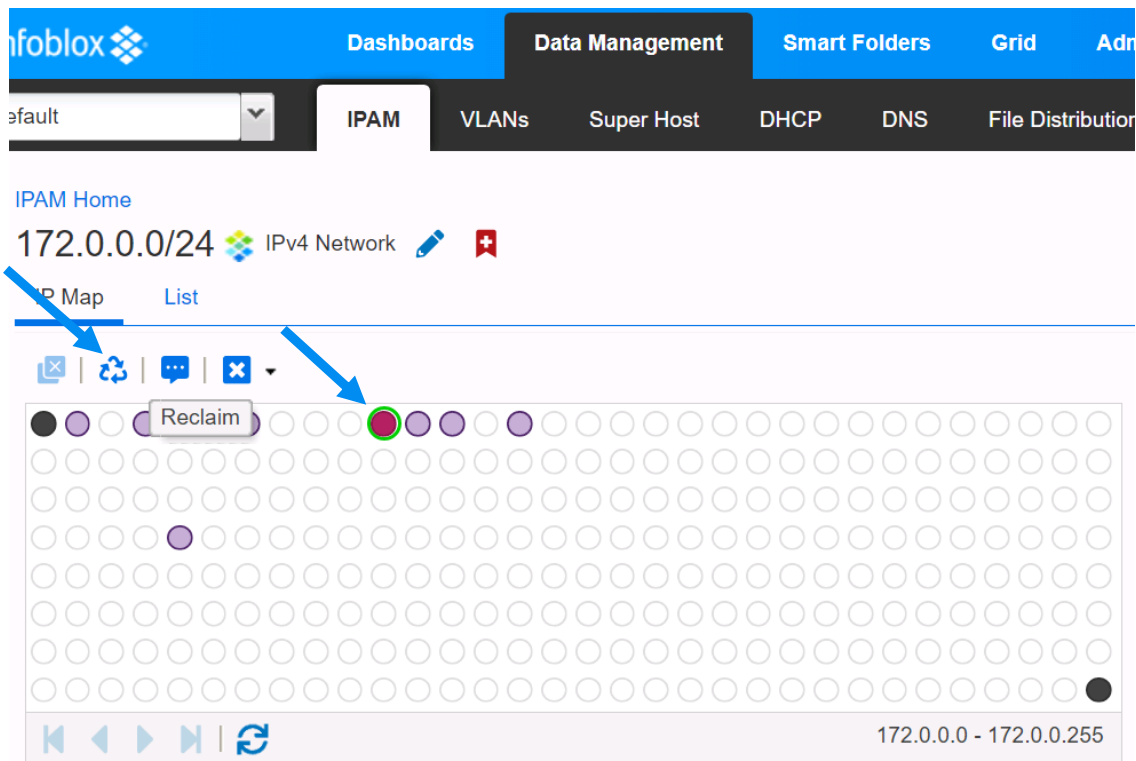
- e. **[DDI]** Scroll down to view the contents of the Extensible Attribute **FS_SyncedAt** for the newly made reservation. This value shows when the asset was added to **[ForeScout]**.

Related Objects Audit History

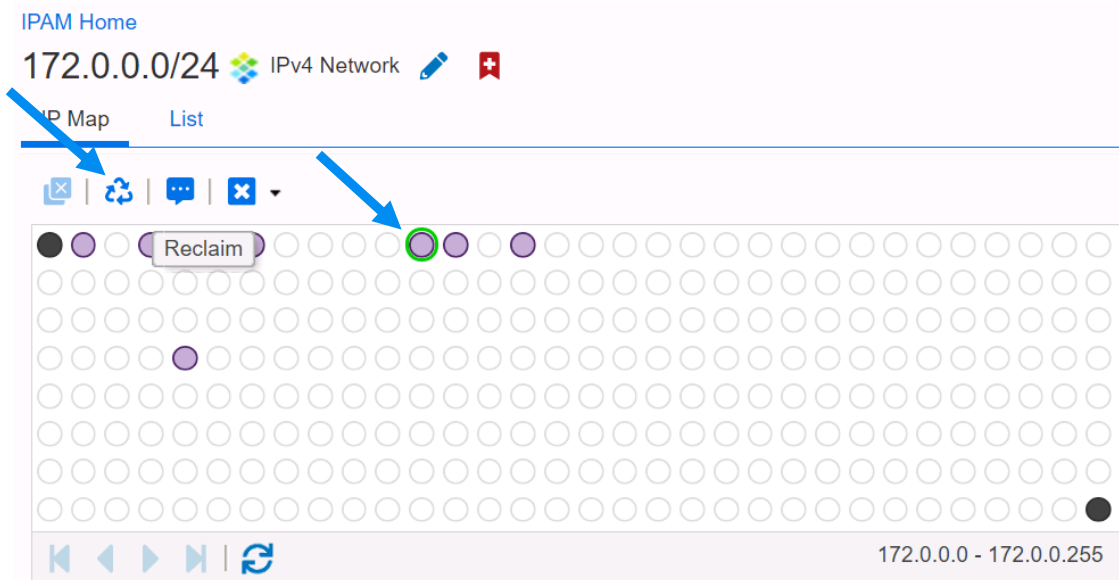
	NAME	TYPE	FS_SYNC	FS_SITE	FS_SYNCEDAT ▲	FS_REMEDIATEDAT
	test.poc.infoblox.local	Host	true	Lab	2020-10-09T01:04	

5. **[ForeScout]** In the ForeScout CounterACT console, click the **Home** tab in the topbar. In the left side menu inside the **Filters** panel, click the **Infoblox** Group. The **IPv4 Reservation** and the **Host** you just created in NIOS appear here.

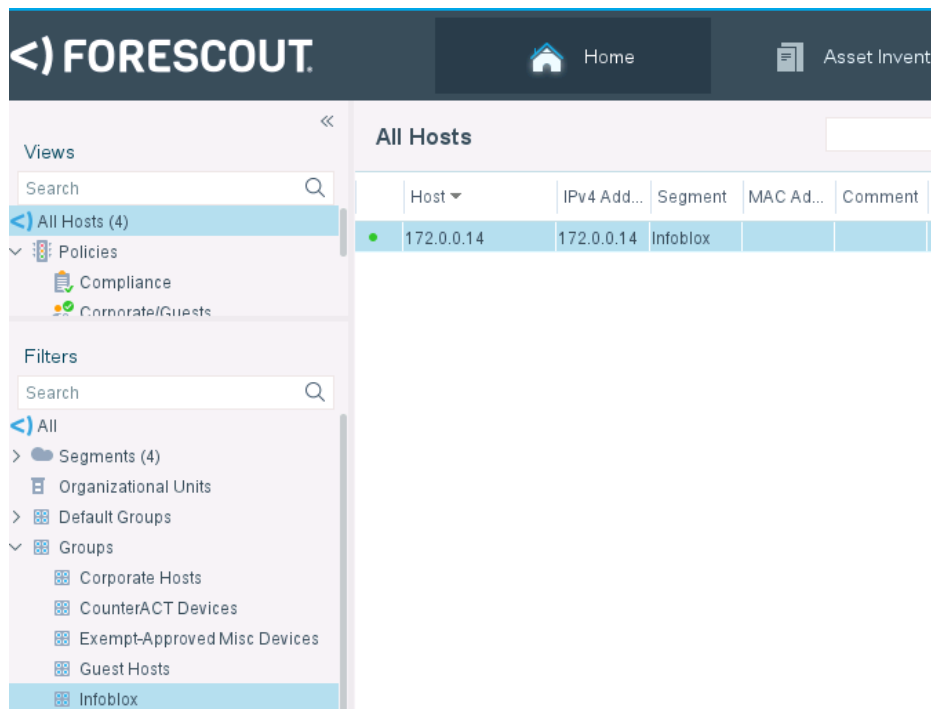
6. **[DDI]** Now we will delete both the **Host** and **IPv4 Reservation**.
 - a. **[DDI]** In NIOS, navigate to **Data management → IPAM → 172.0.0.0/24**.
 - b. **[DDI]** Select the address bubble for address **172.0.0.10**. Click the **Reclaim** button.




- c. **[DDI]** Select the address bubble for address **172.0.0.11**. Click the **Reclaim** button.




7. **[ForeScout]** In the **ForeScout CounterACT Console**, click the **Home** tab. In the left side menu inside the **Filters** panel, click the **Infoblox** Group. Verify the **IPv4 Reservation** and **Host** have been deleted from the Group. *Note their data still exists under **All Hosts**.*

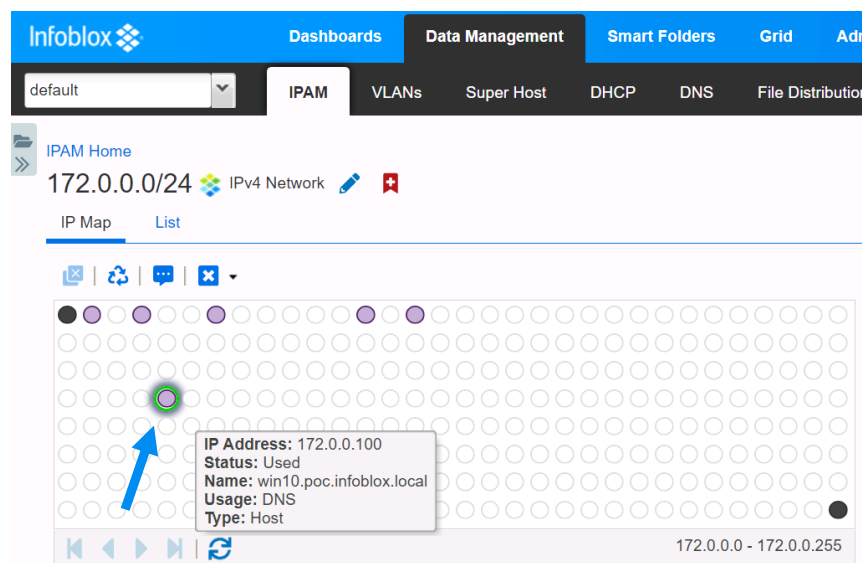


8. (Optional) **[DDI]** If you would like to view the steps performed by the **Outbound Endpoint**, navigate to **Grid → Ecosystem → Outbound Endpoint**. Select the  next to **ForeScout** and click **View Debug Log**.

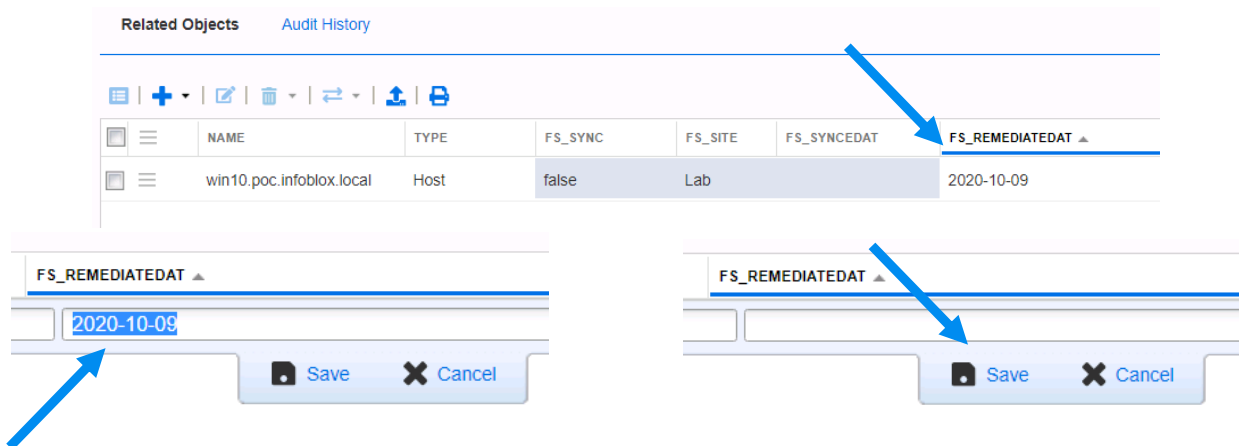
Use Case: Security Remediation


This use case shows Infoblox's ability to respond to DNS security events and apply ForeScout policies to offending assets.

1. (Optional) **[DDI]** Navigate to **Grid → Ecosystem → Outbound Endpoint**. Select the  next to **ForeScout** and click **Clear Debug Log**.
2. **[DDI]** Navigate to **Data management → IPAM → 172.0.0.0/24**.
3. Select the bubble for address **172.0.0.100**. This is the IP for device **[Win10]**.



4. **[DDI]** Verify that the Extensible Attribute **FS_RemediatedAt** is cleared. If the Extensible Attribute is not empty, clear it by performing the following steps:
 - a. Double-click on the **FS_RemediatedAt** content.
 - b. Delete the text.
 - c. Click **Save**.

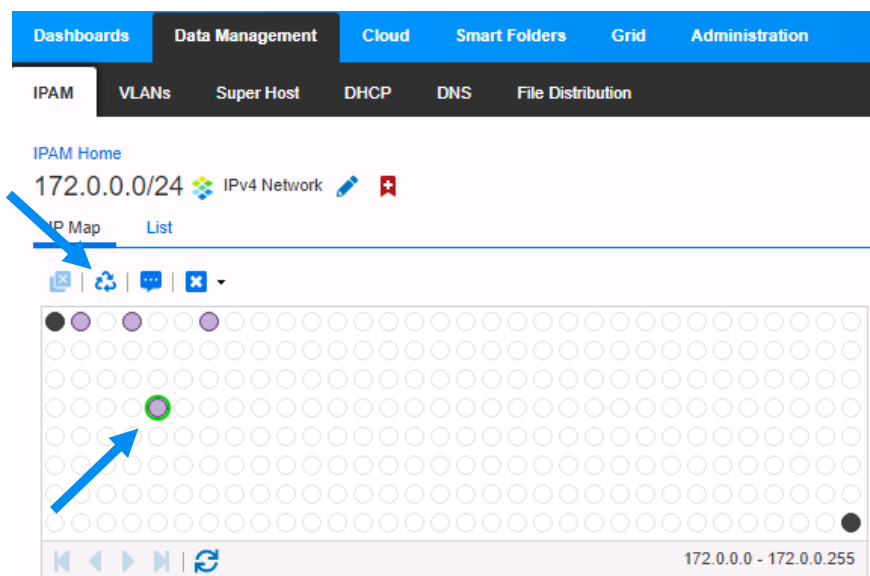


5. **[Win10]** Open a command line. A shortcut  is pinned to the taskbar. Input the command **nslookup example.com 172.0.0.3**. The response will be a NXDOMAIN showing that an RPZ event has occurred.

```
cmd
C:\Windows\system32>nslookup example.com 172.0.0.3
Server: 172-0-0-3.lightspeed.brhmal.sbcglobal.net
Address: 172.0.0.3

*** 172-0-0-3.lightspeed.brhmal.sbcglobal.net can't find example.com: Non-existent domain
C:\Windows\system32>
```

6. **[DDI]** Wait at least 10 seconds. Click the **Refresh** button. Select the bubble for address **172.0.0.100**.



7. **[DDI]** Verify that the Extensible Attribute **FS_RemediatedAt** has been updated.

Related Objects [Audit History](#)

	NAME	TYPE	FS_SYNC	FS_SITE	FS_SYNCEDAT	FS_REMEDIATEDAT ▲
	win10.poc.infoblox.local	Host	true	Lab		2020-10-09

8. **[ForeScout]** In the **ForeScout CounterACT Console**, click the **Home** tab in the topbar. In the left side menu inside the **Filters** panel, click the **Infoblox** Group. The Windows machine host appears here.

The screenshot shows the ForeScout CounterACT Console interface. The top navigation bar includes 'Home' and 'Asset Inventory'. The left sidebar has a 'Filters' panel with a tree view showing 'Groups' expanded, and 'Infoblox' selected. The main area displays a table titled 'All Hosts' with columns: Host, IPv4 Addr..., Segment, MAC Address, Comment, and Dis. The table contains two rows: 172.0.0.14 and 172.0.0.100. The row for 172.0.0.100 is highlighted with a blue box.

9. **[ForeScout]** Double-click on the host. Here you can see more information about the host, including the custom Infoblox properties shown in step 5 of the [ForeScout Configuration Overview](#) section of this document. In the popup, navigate to **All Policies**. Observe the host matched the **IB_OutboundAPI** policy. Click **Show host log**.

The screenshot shows the 'Host Details' popup for host 172.0.0.100. The 'All Policies' tab is selected. The 'IPv4 Address' is 172.0.0.100. Below the address, there are search and filter options. A list of policies is shown, with the 'IB_OutboundAPI' policy highlighted as 'Matched'. At the bottom, there are two buttons: 'Show host in Assets Portal' and 'Show host log', with the latter being highlighted by a blue box. A 'Close' button is in the bottom right corner.

10. **[ForeScout]** In the **Host Log** window that is revealed, retrieve all records generated in the last hour. If necessary, alter the **Relative Time** value by using the associated buttons. Click **Ok**.

Host Log

×

Time Scope

☒ Relative Time

Last

1

Hours

☐ Time Range

From

Oct 8, 2020

...

at

9:16 AM

...

To

Oct 8, 2020

...

at

10:16 PM

...

Record Limitation

Limit the number of records to:

10000

OK

Cancel

11. **[ForeScout]** Filter the results by **Policy** “**IB_OutboundAPI**” using the dropdown menu.

Host Log 172.0.0.100

File Edit

Host Log

Filter: Not ☐ All ☒ Match Text

Time Appliance ... ▲ | ... ▼

- All
- Changes
- Evaluation
- ID change
- Log
- Policy "Corporate/Guest Control"
- Policy "IB_OutboundAPI"
- Policy "Primary Classification"

10/8/20 10:00:00	172.0.0.100	Applications Installed - Failed to learn Win...	Enterprise Manager
10/8/20 10:00:00	172.0.0.100	Software Updates Missing - Failed to lear...	Enterprise Manager
10/8/20 10:00:00	172.0.0.100	Status - Failed to learn VMware Tools...	Enterprise Manager
10/8/20 10:00:00	172.0.0.100	Is Orphan - Failed to learn Virtual M...	Enterprise Manager
10/8/20 10:00:46 PM	172.0.0.100	Windows Services Running - Failed to learn Windo...	Enterprise Manager
10/8/20 10:00:46 PM	172.0.0.100	Windows SecureConnector Version - Failed to learn...	Enterprise Manager
10/8/20 10:00:46 PM	172.0.0.100	Virtual Machine Port Group - Failed to learn Virtual ...	Enterprise Manager
10/8/20 10:00:46 PM	172.0.0.100	VPC Load Balancer Information - Failed to learn VP...	Enterprise Manager
10/8/20 10:00:46 PM	172.0.0.100	EC2's Virtual Private Cloud - Failed to learn EC2's Vi...	Enterprise Manager
10/8/20 10:00:46 PM	172.0.0.100	VPC Name - Failed to learn VPC Name : IP is not as...	Enterprise Manager
10/8/20 10:00:46 PM	172.0.0.100	Windows Active Users - Failed to learn Windows Act...	Enterprise Manager
10/8/20 10:00:46 PM	172.0.0.100	Virtual Machine Guest State - Failed to learn Virtual ...	Enterprise Manager
10/8/20 10:00:46 PM	172.0.0.100	VMware Server Host Profile Compliance Status - Fai...	Enterprise Manager
10/8/20 10:00:46 PM	172.0.0.100	Virtual Machine Memory Usage (%) - Failed to learn...	Enterprise Manager
10/8/20 10:00:46 PM	172.0.0.100	Macintosh User - Failed to learn Macintosh User : IP ...	Enterprise Manager
10/8/20 10:00:46 PM	172.0.0.100	IOG Core State - Failed to learn IOG Core State : IP ...	Enterprise Manager

190 items (0 selected)

Done.


Close

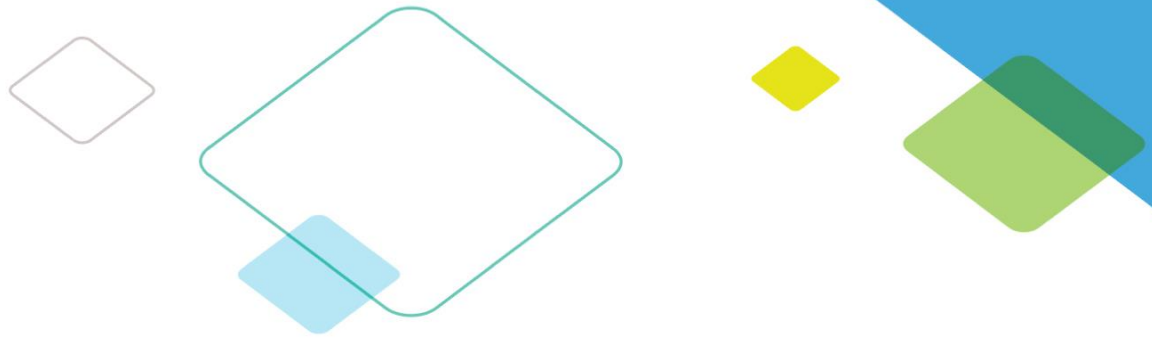
12. **[ForeScout]** Here you can see the actions ForeScout has taken on this host. Confirm remediation has occurred. Close the ForeScout CounterACT Console and all associated windows.

The screenshot shows the 'Host Log' window for host 172.0.0.100. The window has a blue header with 'File' and 'Edit' menus. Below the header, there's a title 'Host Log' and a filter section with 'Filter: Not' and a dropdown menu showing 'Policy "IB_OutboundAPI"'. To the right of the filter is a 'Match Text' input field and three icons: a pause icon, a play icon, and an up arrow icon. Below the filter section is a table with columns: Time, Host, Details, and Appliance. The table contains five rows of log entries. The second row is highlighted in blue. Below the table, there's a status bar that says '5 items (1 selected)' and 'Done.'. A modal window titled 'Details for - 172.0.0.100' is open in the foreground, showing details for the selected event. The modal has a close button in the top right corner. The details are as follows:

Property	Value
Host	172.0.0.100
Time	10/8/20 10:00 PM
Status	OK
Type	Action
Name	Policy "IB_OutboundAPI" Rule "Remediate"
Details	Action completed O.K. - Send Delete Properties: Properties : fsapi_IB_Scan; Schedule: Action runs when the endpoint matches a policy condition.

At the bottom right of the modal is a blue 'Close' button. At the bottom right of the main window, there is also a blue 'Close' button.

13. (Optional) **[DDI]** If you would like to view the steps performed by the **Outbound Endpoint**, navigate to **Grid → Ecosystem → Outbound Endpoint**. Select the  hamburger icon next to **ForeScout** and click **View Debug Log**.



Infoblox enables next level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com



© 2019 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).