

DEPLOYMENT GUIDE

Enabling Infoblox Identity Mapping with Microsoft Active Directory

Table of Contents

Introduction.....	2
How Infoblox Gets User Information.....	2
Prerequisites.....	2
Best Practices.....	2
Deploying Identity Mapping.....	3
Enabling Identity Mapping.....	3
Viewing User Data.....	4
Active Users.....	4
User Login History.....	6
Search Filters.....	6
User Session.....	7
Logged Event Types Read by Infoblox.....	7
Dashboard Widget.....	8
Reporting.....	9

Introduction

Identity Mapping on the NIOS appliance is used to provide Active Directory domain user information if the NIOS appliance is connected to a Microsoft server. By enabling this feature, an IT administrator can monitor Active Directory domain users by viewing their IP address, login status, and the duration of their current status. This guide describes how to enable Identity Mapping on an Infoblox appliance running NIOS to provide Microsoft Active Directory (AD) domain user information when the appliance is connected to a Microsoft domain controller.

How Infoblox Gets User Information

Infoblox Identity Mapping relies on live event logs, which are available on Microsoft servers. Upon enabling the Identity Mapping feature, the appliance communicates with Microsoft servers to pull event logs.

NOTE: The user information displayed is only as accurate as the Microsoft event logs.

Prerequisites

The following are prerequisites for Infoblox Identity Mapping;

- Functional 7.2 or greater Infoblox Grid with a Grid Master
- Microsoft Servers Event logs enabled on the Microsoft servers
- Microsoft Server versions supported [here](#)

NOTE: Identity Mapping doesn't require the Microsoft server to run DNS or DHCP in order to gather authentication information.

Best Practices

To get the most from Infoblox Identity Mapping, we recommend the following best practices:

- Install a Microsoft management license on the Grid to allow you to manage the Microsoft DNS, DHCP, and Active Directory servers.
- Choose and sync Microsoft servers that handle large quantities of authentications, domain controllers, Exchange servers, etc.
- A best practice is NOT to provide any protocol on the members running Microsoft AD user management. Members running Identity Mapping will run processes that share resources with other Microsoft DNS/DHCP/AD site synchronization if configured.
- Any Microsoft server responsible for a large number of domain authentications can be configured. Suggested targets are the Microsoft Exchange server, Microsoft domain controller, SharePoint servers, and IIS servers to sync the user information.

- A Microsoft user that belongs to a Domain User group and Event Log Reader group should at a minimum be used to start a session between the Infoblox Grid and Microsoft servers to obtain network user information
- TE-14XX and above can be used as an Infoblox appliance for this feature, although the number of users per Grid member varies with the appliance model.
- Avoid using a Grid Master to perform the Identity Mapping sync.
- Take into consideration that a Grid member will perform additional work to process synchronized data from other members; so upsize appropriately.

Deploying Identity Mapping

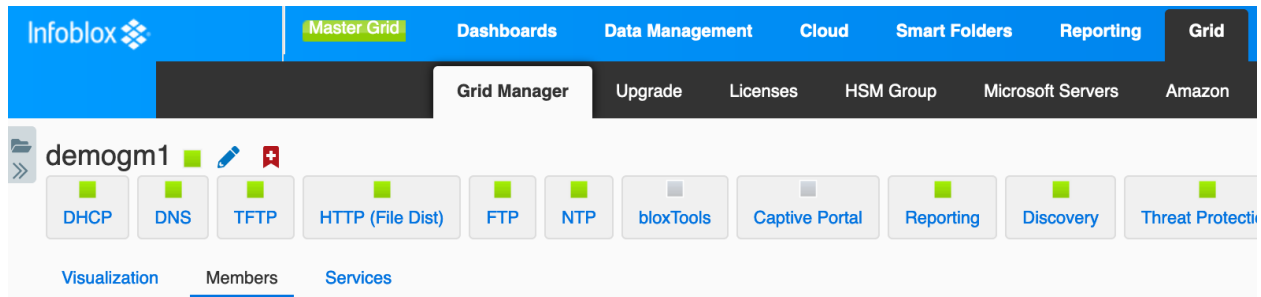
The following steps are required to enable Identity Mapping feature and view user data on the NIOS appliance:

- Enable Identity Mapping on the Grid.
- View user data from Microsoft servers.

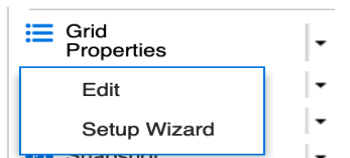
Enabling Identity Mapping

This section describes how to enable Identity Mapping on the Grid.

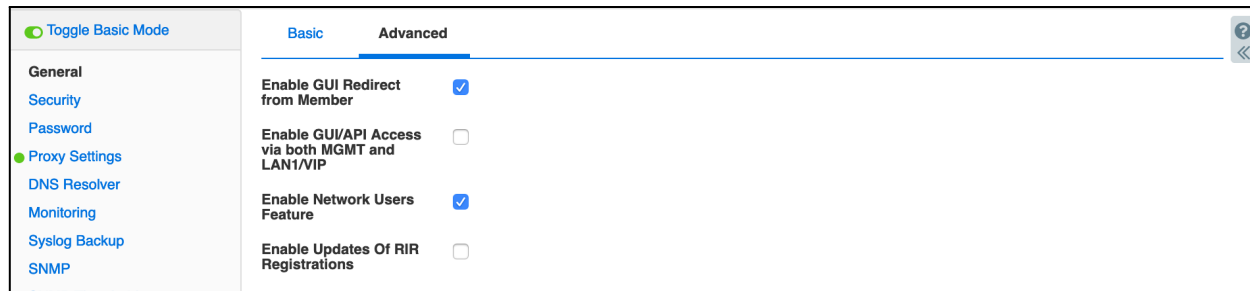
1. Go to **Grid** → **Grid Manager** → **Members**.



2. Select the **Grid Properties** → **Edit** from the toolbar.



3. Select the **General** tab in the Grid Properties Editor and ensure that Advanced Mode is **on**.



4. Select the **Enable Network Users Feature**

5. Click **Save & Close** to save the configuration.

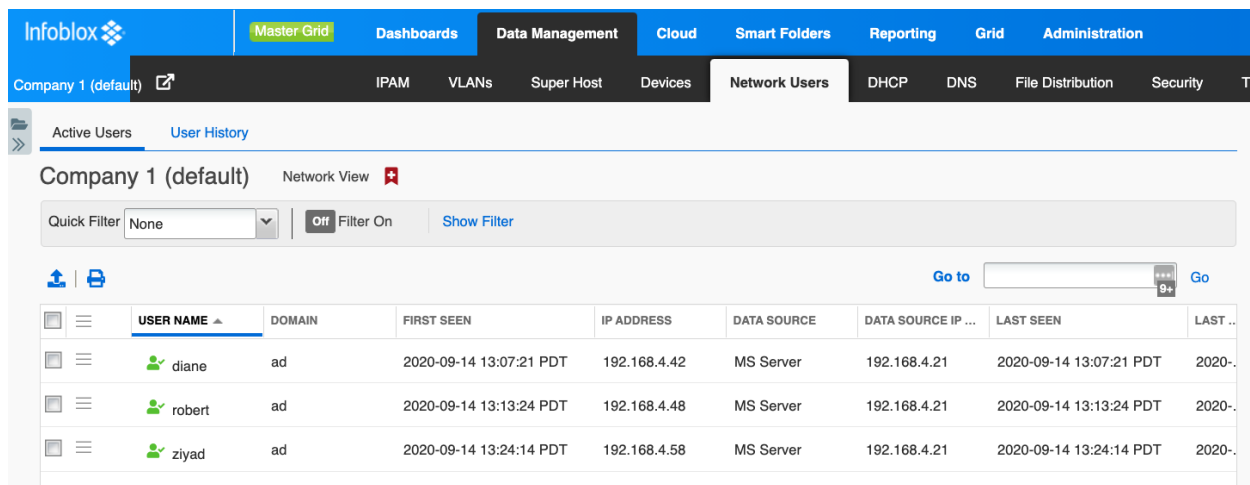
Note: Identity Mapping does not require a MS_MANAGEMENT license to operate. With NIOS 8.4, you can add a Microsoft server even without having a MS_MANAGEMENT license. However, you cannot configure DNS, DHCP, and Microsoft AD Sites synchronization unless a MS_MANAGEMENT license is installed. Without a MS_MANAGEMENT license, only Microsoft AD user configuration settings are displayed in UI and only those configurations are allowed from the UI and PAPI.

Viewing User Data

After enabling Infoblox Identity Mapping as described above, an administrator can view all the active users currently logged into the Microsoft AD domain services as well as user login history.

Active Users

To view active users, go to **Data Management** → **Network Users** → **Active Users**.



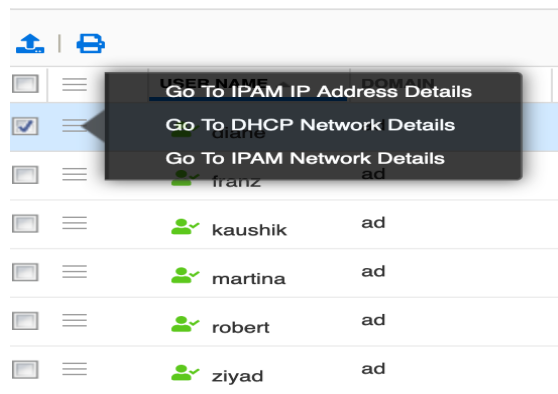
The Active Users tab shows the following Network User objects;

- **Username**—The name of the user logged into the Microsoft server as a user or as a service
- **Domain**—The domain name on Microsoft server that the user is logged into

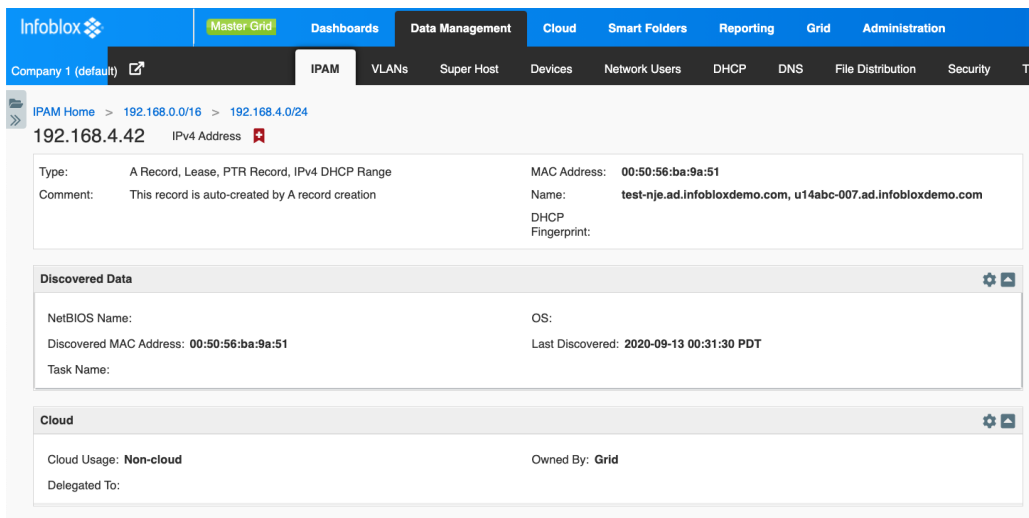
- **First Seen**—The time the user first logged into the domain
- **IP Address**—The IP address of the user machine the user logged into
- **Data Source**—The IP address of the Microsoft server reporting user login
- **Last Seen**—The time the user was last seen active by the sync process
- **Last Updated**—The time of last sync

The times are displayed in the time one configured for the Infoblox user viewing this data. For example, if an administrator is viewing the data, then the time stamps reflect the time zone configured for the admin.

To view detailed Identity Mapping data on a particular active user, click on the hamburger icon next to the active user name.

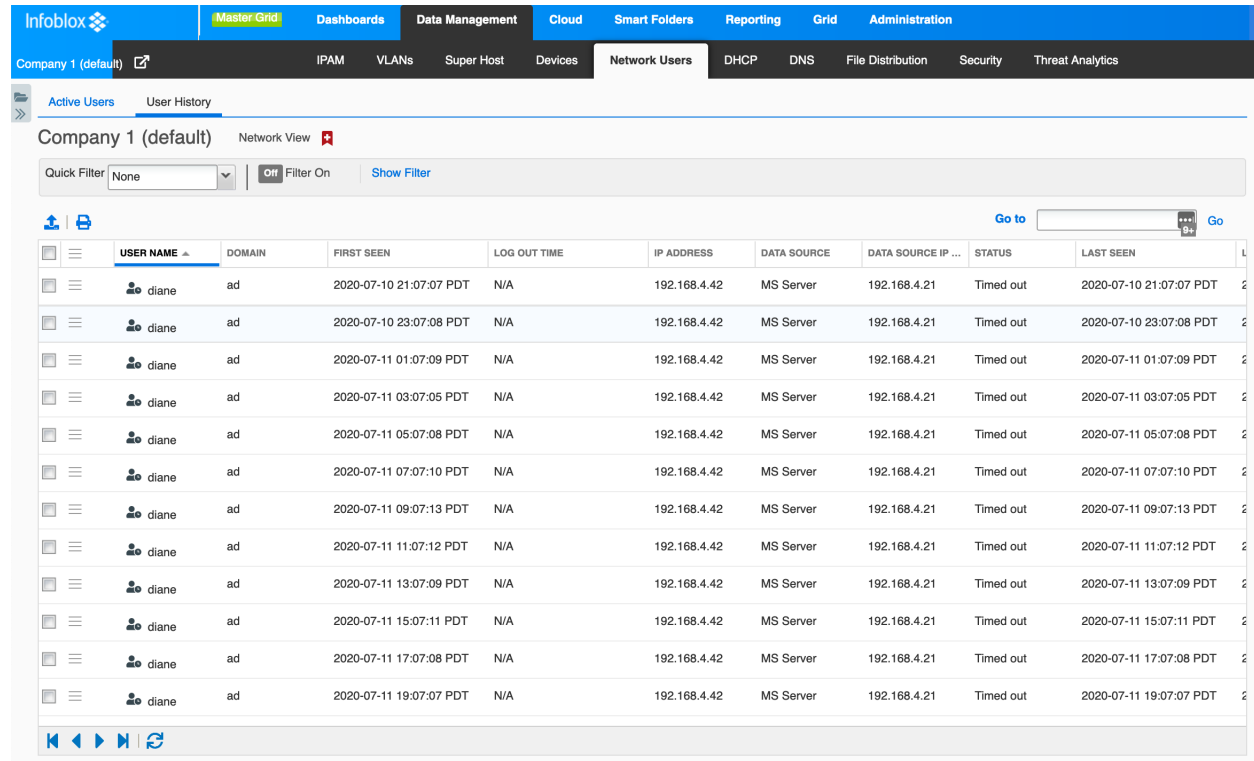


Select **Go to IPAM IP Address Details** to view the network address of the device and any DNS or DHCP-related data associated with the device, such as A records and lease information.



User Login History

To view network users login history, go to **Data Management** → **Network Users** → **User History**.



The screenshot shows the Infoblox User History interface. The top navigation bar includes 'Infoblox', 'Master Grid', 'Dashboards', 'Data Management', 'Cloud', 'Smart Folders', 'Reporting', 'Grid', and 'Administration'. The 'Data Management' section is active, with sub-menus for 'IPAM', 'VLANs', 'Super Host', 'Devices', 'Network Users', 'DHCP', 'DNS', 'File Distribution', 'Security', and 'Threat Analytics'. The 'Network Users' sub-menu is selected, and the 'User History' tab is active. The interface displays 'Company 1 (default)' and 'Network View'. A 'Quick Filter' dropdown is set to 'None', with 'Filter On' and 'Show Filter' options. Below the filter is a table with columns: USER NAME, DOMAIN, FIRST SEEN, LOG OUT TIME, IP ADDRESS, DATA SOURCE, DATA SOURCE IP, STATUS, and LAST SEEN. The table contains 12 rows of data for user 'diane' from domain 'ad', all with a status of 'Timed out'. The 'LAST SEEN' column shows various timestamps from 2020-07-10 21:07:07 PDT to 2020-07-11 19:07:07 PDT. The table has a 'Go to' search bar and pagination controls at the bottom.

USER NAME	DOMAIN	FIRST SEEN	LOG OUT TIME	IP ADDRESS	DATA SOURCE	DATA SOURCE IP	STATUS	LAST SEEN
diane	ad	2020-07-10 21:07:07 PDT	N/A	192.168.4.42	MS Server	192.168.4.21	Timed out	2020-07-10 21:07:07 PDT
diane	ad	2020-07-10 23:07:08 PDT	N/A	192.168.4.42	MS Server	192.168.4.21	Timed out	2020-07-10 23:07:08 PDT
diane	ad	2020-07-11 01:07:09 PDT	N/A	192.168.4.42	MS Server	192.168.4.21	Timed out	2020-07-11 01:07:09 PDT
diane	ad	2020-07-11 03:07:05 PDT	N/A	192.168.4.42	MS Server	192.168.4.21	Timed out	2020-07-11 03:07:05 PDT
diane	ad	2020-07-11 05:07:08 PDT	N/A	192.168.4.42	MS Server	192.168.4.21	Timed out	2020-07-11 05:07:08 PDT
diane	ad	2020-07-11 07:07:10 PDT	N/A	192.168.4.42	MS Server	192.168.4.21	Timed out	2020-07-11 07:07:10 PDT
diane	ad	2020-07-11 09:07:13 PDT	N/A	192.168.4.42	MS Server	192.168.4.21	Timed out	2020-07-11 09:07:13 PDT
diane	ad	2020-07-11 11:07:12 PDT	N/A	192.168.4.42	MS Server	192.168.4.21	Timed out	2020-07-11 11:07:12 PDT
diane	ad	2020-07-11 13:07:09 PDT	N/A	192.168.4.42	MS Server	192.168.4.21	Timed out	2020-07-11 13:07:09 PDT
diane	ad	2020-07-11 15:07:11 PDT	N/A	192.168.4.42	MS Server	192.168.4.21	Timed out	2020-07-11 15:07:11 PDT
diane	ad	2020-07-11 17:07:08 PDT	N/A	192.168.4.42	MS Server	192.168.4.21	Timed out	2020-07-11 17:07:08 PDT
diane	ad	2020-07-11 19:07:07 PDT	N/A	192.168.4.42	MS Server	192.168.4.21	Timed out	2020-07-11 19:07:07 PDT

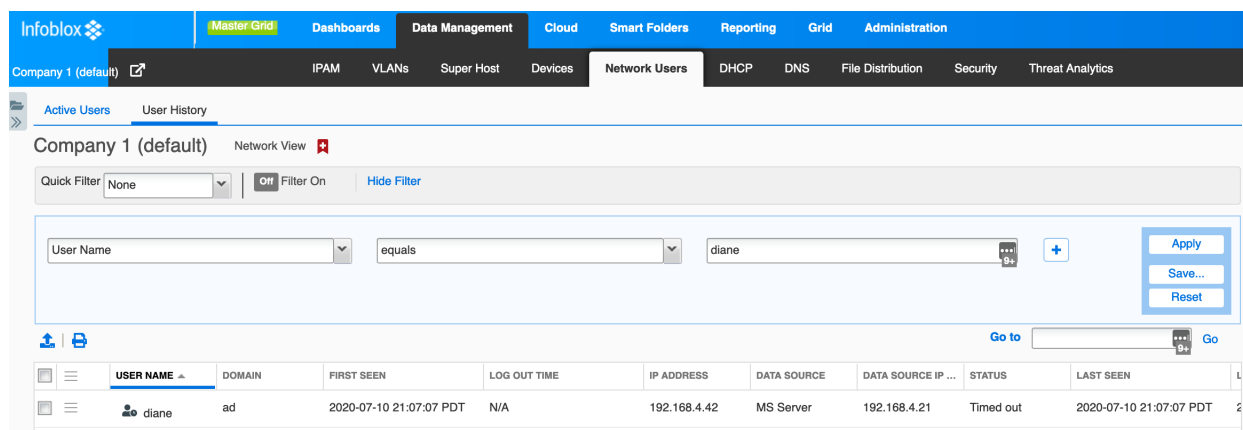
The Status in the User History tab will display one of these three values:

- Active (user is logged in and active at the time)
- Logged out (user has logged out of the system with logout time stamp set)
- Timed out (user is logged in but has been idle* for a certain time, default is 2 hours)

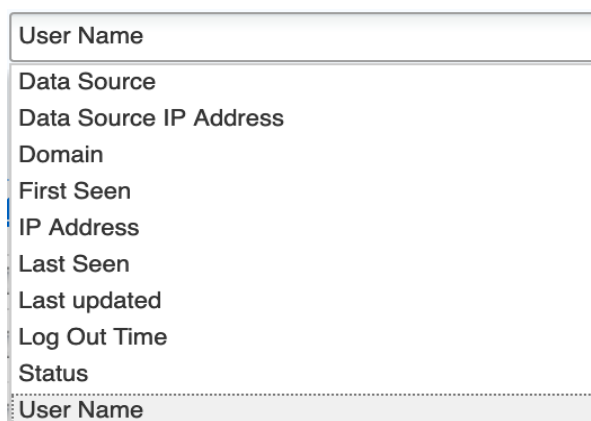
**Idle means no additional authentications for the users are found within the given time frame.*

Search Filters

One powerful feature of the Infoblox Grid is its ability to search for data using filters. For example, if you want to search for a particular user name, He or she can do so as shown below.



The search operators used in the example above are “User Name”, “equals”, and then the actual user name. Multiple search operators are available to help you search for data as shown below.



User Session

Infoblox considers the following login scenarios as different user sessions:

- A different user at the same IP is a different session.
- The same user at a different IP is a different session.
- The same user at the same IP at a different point in time is a different session.

Logged Event Types Read by Infoblox

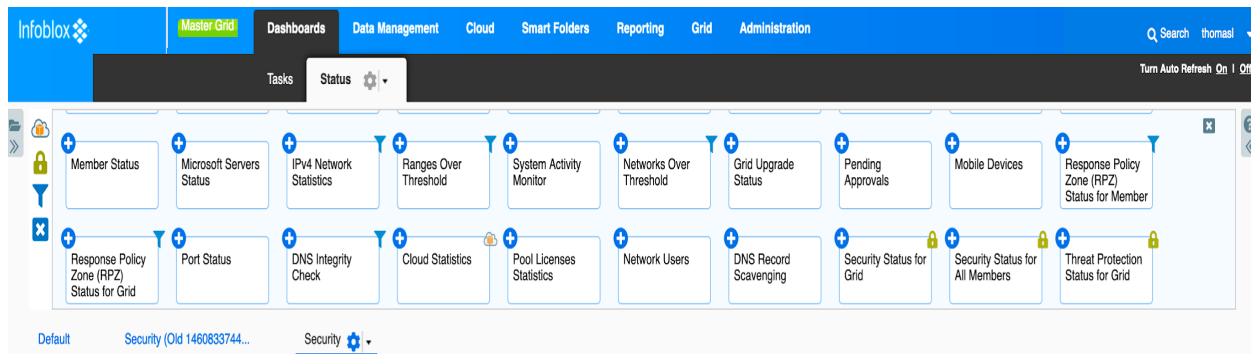
Since Identity Mapping looks at user logins in the Microsoft security event logs, Infoblox is interested in the following events and reads only these events,

- **Kerberos Authentication Event** (event id 4768): Seen when a user enters a user name and password (logs in). It is seen only on the domain controller (DC). The user name and password are authenticated on the domain controller, a TGT (ticket granting ticket) is issued, and event 4768 is logged.

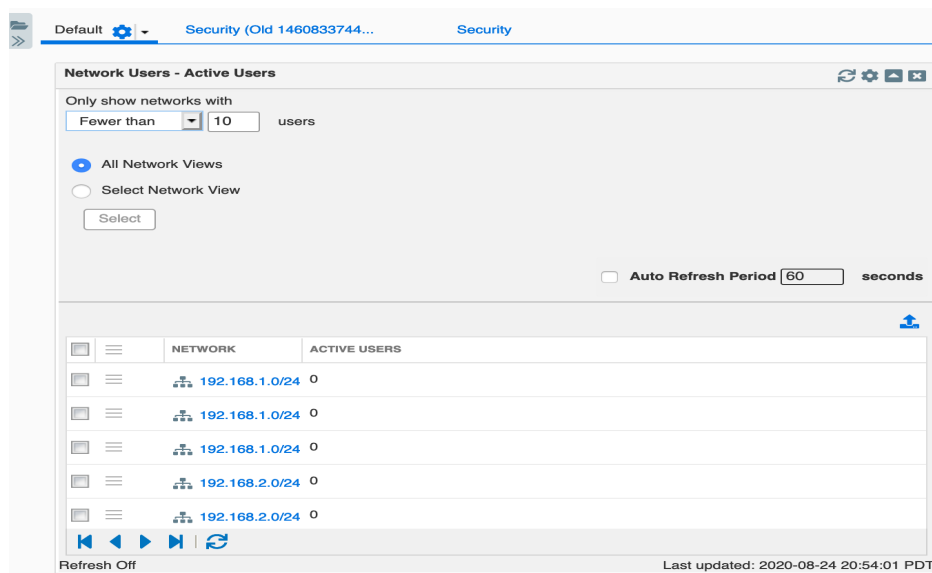
- **Kerberos Service Ticket Request** (event id 4769): Logged when a service ticket is requested. Service tickets are issued whenever a user or computer accesses a server on the network. For example, when a user maps a drive to a file server, the resulting service ticket request generates event ID 4769 on the DC.
- **Kerberos Service Ticket Renewal** (event id 4770): Logged when a service ticket is renewed. Kerberos limits how long a ticket is valid. If a ticket expires when the user is still logged on, Windows automatically contacts the domain controller to renew the ticket, which triggers this event.
- **Account Login Request** (event 4624): Logged when a user logs in or a service logs in the user successfully.
- **Account Logoff Request** (event 4634): Logged when a login session ends.

Dashboard Widget

A new Dashboard widget, called Network Users, is available with Identity Mapping.



You can find networks with active users; for example, if an administrator wants to know the networks that have at least one active user, then he can configure this widget as shown below,



Reporting

A new report, called User Login History, has been added in the reporting section for Identity Mapping. This report shows user login activities over time to help you audit user logins. With this report, you can get data such as:

- List all user machine IPs, that is, domains used by a user to log in.
- Number of active users
- User login activities during a specific period of time

To generate this report, go to **Reporting** → **Dashboards** → **User Login History**.

Infoblox Reporting & Analytics

App: Infoblox Reporting & Analytics

thomasl | Messages | Settings | Activity | Help | Find

Home Dashboard | Dashboards | Reports | Quick filter | Demo Dashboards | Alerts | Search | Pivot | Administration | Reporting Help

User Login History

System-created dashboard. Please clone before editing.

Hide Filters | Edit | More Info | Download

Last Updated: Last 1 week | IP Address: All | User Name: All | User Status: All | Submit

	Last Updated	User Name	Domain	IP Address	First Seen	Logout Time	Last Seen	User Status
1	2020-08-24 20:55:19	niosadmin	ad	192.168.1.3	2019-12-08 01:16:25	2020-08-24 20:32:07	2020-08-24 20:32:17	LOGOUT
2	2020-08-24 20:49:00	niosadmin	ad	192.168.1.3	2019-12-08 01:16:25	2020-08-24 20:25:38	2020-08-24 20:25:48	LOGOUT
3	2020-08-24 20:42:52	niosadmin	ad	192.168.1.3	2019-12-08 01:16:25	2020-08-24 20:19:55	2020-08-24 20:19:55	LOGOUT
4	2020-08-24 20:36:39	niosadmin	ad	192.168.1.3	2019-12-08 01:16:25	2020-08-24 20:13:38	2020-08-24 20:13:38	LOGOUT
5	2020-08-24 20:30:17	niosadmin	ad	192.168.1.3	2019-12-08 01:16:25	2020-08-24 20:07:06	2020-08-24 20:07:16	LOGOUT
6	2020-08-24 20:23:56	niosadmin	ad	192.168.1.3	2019-12-08 01:16:25	2020-08-24 20:00:37	2020-08-24 20:00:47	LOGOUT
7	2020-08-24 20:17:48	niosadmin	ad	192.168.1.3	2019-12-08 01:16:25	2020-08-24 19:54:51	2020-08-24 19:54:51	LOGOUT
8	2020-08-24 20:17:48	franz	ad	192.168.4.53	2020-08-24 19:54:03		2020-08-24 19:54:03	ACTIVE
9	2020-08-24 20:11:32	niosadmin	ad	192.168.1.3	2019-12-08 01:16:25	2020-08-24 19:48:37	2020-08-24 19:48:37	LOGOUT
10	2020-08-24 20:05:10	niosadmin	ad	192.168.1.3	2019-12-08 01:16:25	2020-08-24 19:42:07	2020-08-24 19:42:07	LOGOUT

< prev | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | next >



Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com