# Infoblox Identity Mapping

Infoblox
NEXT LEVEL NETWORKING

## Key Features

- Correlation of IP address and MAC address with username information, all mapped to the Infoblox authoritative IPAM database
- Integration of username information in DNS and DHCP, making Infoblox DDI identity aware. Additional information in the DNS, DHCP, and IPAM management UI and dashboard widgets with correlated username information
- Agentless communication with Microsoft AD, Exchange, and other servers for data aggregation and integration
- Easy setup process via the existing Infoblox Add Microsoft Server wizard
- Extended historical user information available via Trinzic Reporting

## Bringing Together User Identities and Network Data

Infoblox Identity Mapping enables unprecedented visibility for enterprise network and security administrators by adding username information to the existing wealth of network device information in the IPAM database, thus providing a single authoritative data source. Access to user information related to networks and end-host devices helps connect administrators to the information they need more quickly, resulting in more informed network administrators with a richer understanding of how network resources are consumed and by whom.

## The Challenge

The correlation of users to network devices and network data is typically a cumbersome task, leading to less-than-optimal operations. Network teams struggle to gather the information needed to perform their own operations, trouble-shoot, and strategically plan and support other IT teams. Even with sophisticated network discovery tools the end result is still a network-centric view, which limits the level of information network teams can provide to security, server, cloud, desktop, and other IT teams—who are all delivering IT services at the user level.

## The Infoblox Solution

Infoblox Identity Mapping, available in Infoblox DDI, enables identity-aware DDI. This is a significant step forward in bridging the gap between network-centric management tools and user-focused network administrators. Infoblox gives network administrators and security teams next-level visibility by relating username information to IP and MAC address information in one IPAM database. Providing improved visibility into networks and end-host devices and associating them with specific users improves trouble-shooting and accelerates isolation of and response to security incidents.

Infoblox Identity Mapping analyzes the Microsoft Server Event Logs and captures user log in, log out, and authentication events from Microsoft services including Exchange, SharePoint, file shares, and others services that leverage Active Directory authentication. The improved IPAM data includes the combined username, IP address, and MAC address, allowing administrators to view:

- Users per network
- Users per range/scope
- Users associated with DNS records
- Users triggering DNS security events (with the Infoblox Reporting Server)

Setup is a snap. The setup process for Identity Mapping is enabled via the Infoblox Add Microsoft Server feature. This easy-to-use step-by-step wizard includes extensions for configuring user mapping options.

Identity Mapping data is integrated into the DDI management UI and provides valuable historical data via the Infoblox Reporting Server.

# Infoblox Identity Mapping

## Benefits

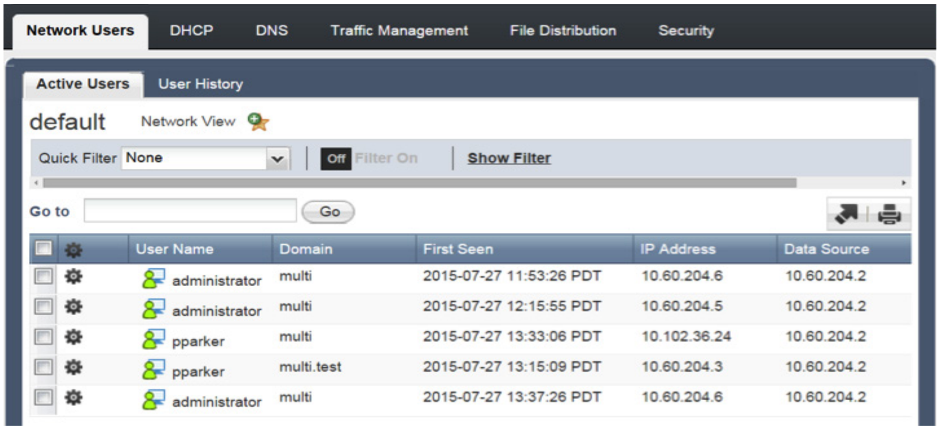
- **Visibility**: User information related to network devices and end-host devices connects administrators to the information they need more quickly.
- **Richer Information**: Better informed network administrators have a richer understanding of how network resources are consumed and by whom.
- **Faster Response Times**: Security and operations teams can mitigate, operate, and trouble-shoot using a network-user-focused approach.

## Updated Reports and User Interface (UI) Screens

- The DHCP Lease History report includes leased IP address/username data over time.
- The Top Response Policy Zone (RPZ) Hits report identifies usernames associated with IP addresses making queries hitting the RPZ, an indicator of users attempting to reach possibly malicious destinations.
- The Data Management tab in the DDI management UI has a Network Users tab to correlate users to networks. UI data is limited to recent activity. Historical data is retrieved via the Infoblox Reporting Server.
- Networks and scopes/ranges in the IPAM and DHCP screens have an Active Users column providing visibility in network usage across networks.
- DNS screens show users associated with select DNS records.

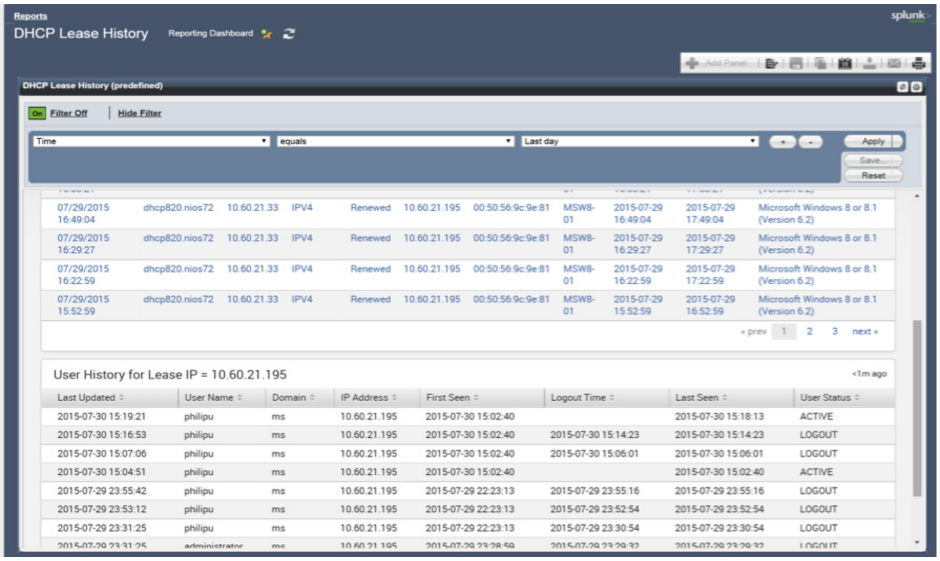
## New Report and Widget

The User Login History report shows a history of user logins over time—filtered by time, username, IP address, domain, etc. The new Active Network Users widget is an easy-to-read addition to the Infoblox dashboard showing the active user count by network.



| ☐ | | User Name | Domain | First Seen | IP Address | Data Source |
|---|---|---|---|---|---|---|
| ☐ | | administrator | multi | 2015-07-27 11:53:26 PDT | 10.60.204.6 | 10.60.204.2 |
| ☐ | | administrator | multi | 2015-07-27 12:15:55 PDT | 10.60.204.5 | 10.60.204.2 |
| ☐ | | pparker | multi | 2015-07-27 13:33:06 PDT | 10.102.36.24 | 10.60.204.2 |
| ☐ | | pparker | multi.test | 2015-07-27 13:15:09 PDT | 10.60.204.3 | 10.60.204.2 |
| ☐ | | administrator | multi | 2015-07-27 13:37:26 PDT | 10.60.204.6 | 10.60.204.2 |

Figure 1: Network Active User view



| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 07/29/2015 16:49:04 | dhcp820.nios72 | 10.60.21.33 | IPV4 | Renewed | 10.60.21.195 | 00:50:56:9c:9e:81 | MSW8-01 | 2015-07-29 16:49:04 | 2015-07-29 17:49:04 | Microsoft Windows 8 or 8.1 (Version 6.2) |
| 07/29/2015 16:29:27 | dhcp820.nios72 | 10.60.21.33 | IPV4 | Renewed | 10.60.21.195 | 00:50:56:9c:9e:81 | MSW8-01 | 2015-07-29 16:29:27 | 2015-07-29 17:29:27 | Microsoft Windows 8 or 8.1 (Version 6.2) |
| 07/29/2015 16:22:59 | dhcp820.nios72 | 10.60.21.33 | IPV4 | Renewed | 10.60.21.195 | 00:50:56:9c:9e:81 | MSW8-01 | 2015-07-29 16:22:59 | 2015-07-29 17:22:59 | Microsoft Windows 8 or 8.1 (Version 6.2) |
| 07/29/2015 15:52:59 | dhcp820.nios72 | 10.60.21.33 | IPV4 | Renewed | 10.60.21.195 | 00:50:56:9c:9e:81 | MSW8-01 | 2015-07-29 15:52:59 | 2015-07-29 16:52:59 | Microsoft Windows 8 or 8.1 (Version 6.2) |

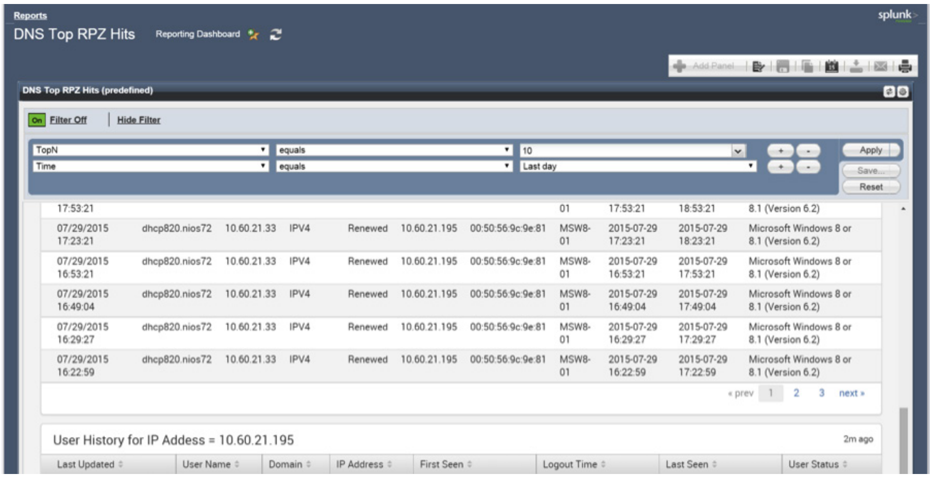
User History for Lease IP = 10.60.21.195

<1m ago

| Last Updated | User Name | Domain | IP Address | First Seen | Logout Time | Last Seen | User Status |
|---|---|---|---|---|---|---|---|
| 2015-07-30 15:19:21 | philipu | ms | 10.60.21.195 | 2015-07-30 15:02:40 | | 2015-07-30 15:18:13 | ACTIVE |
| 2015-07-30 15:16:53 | philipu | ms | 10.60.21.195 | 2015-07-30 15:02:40 | 2015-07-30 15:14:23 | 2015-07-30 15:14:23 | LOGOUT |
| 2015-07-30 15:07:06 | philipu | ms | 10.60.21.195 | 2015-07-30 15:02:40 | 2015-07-30 15:06:01 | 2015-07-30 15:06:01 | LOGOUT |
| 2015-07-30 15:04:51 | philipu | ms | 10.60.21.195 | 2015-07-30 15:02:40 | | 2015-07-30 15:02:40 | ACTIVE |
| 2015-07-29 23:55:42 | philipu | ms | 10.60.21.195 | 2015-07-29 22:23:13 | 2015-07-29 23:55:16 | 2015-07-29 23:55:16 | LOGOUT |
| 2015-07-29 23:53:12 | philipu | ms | 10.60.21.195 | 2015-07-29 22:23:13 | 2015-07-29 23:52:54 | 2015-07-29 23:52:54 | LOGOUT |
| 2015-07-29 23:31:25 | philipu | ms | 10.60.21.195 | 2015-07-29 22:23:13 | 2015-07-29 23:30:54 | 2015-07-29 23:30:54 | LOGOUT |
| 2015-07-29 23:31:25 | administrator | ms | 10.60.21.195 | 2015-07-29 23:28:59 | 2015-07-29 23:29:32 | 2015-07-29 23:29:32 | LOGOUT |

Figure 2: DHCP Lease History including user data

# Infoblox Identity Mapping



DNS Top RPZ Hits

TopN equals 10

Time equals Last day

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 17:53:21 | | | | | | | 01 | 17:53:21 | 18:53:21 | 8.1 (Version 6.2) |
| 07/29/2015 17:23:21 | dhcp820.nios72 | 10.60.21.33 | IPV4 | Renewed | 10.60.21.195 | 00:50:56:9c:9e:81 | MSW8-01 | 2015-07-29 17:23:21 | 2015-07-29 18:23:21 | Microsoft Windows 8 or 8.1 (Version 6.2) |
| 07/29/2015 16:53:21 | dhcp820.nios72 | 10.60.21.33 | IPV4 | Renewed | 10.60.21.195 | 00:50:56:9c:9e:81 | MSW8-01 | 2015-07-29 16:53:21 | 2015-07-29 17:53:21 | Microsoft Windows 8 or 8.1 (Version 6.2) |
| 07/29/2015 16:49:04 | dhcp820.nios72 | 10.60.21.33 | IPV4 | Renewed | 10.60.21.195 | 00:50:56:9c:9e:81 | MSW8-01 | 2015-07-29 16:49:04 | 2015-07-29 17:49:04 | Microsoft Windows 8 or 8.1 (Version 6.2) |
| 07/29/2015 16:29:27 | dhcp820.nios72 | 10.60.21.33 | IPV4 | Renewed | 10.60.21.195 | 00:50:56:9c:9e:81 | MSW8-01 | 2015-07-29 16:29:27 | 2015-07-29 17:29:27 | Microsoft Windows 8 or 8.1 (Version 6.2) |
| 07/29/2015 16:22:59 | dhcp820.nios72 | 10.60.21.33 | IPV4 | Renewed | 10.60.21.195 | 00:50:56:9c:9e:81 | MSW8-01 | 2015-07-29 16:22:59 | 2015-07-29 17:22:59 | Microsoft Windows 8 or 8.1 (Version 6.2) |

User History for IP Addess = 10.60.21.195

| Last Updated | User Name | Domain | IP Address | First Seen | Logout Time | Last Seen | User Status |
|---|---|---|---|---|---|---|---|

Figure 3: Top RPZ hits including user data

## Why Infoblox

- Identity Mapping provides real-time and historical data supporting security-event investigations, correlating IP address and user information to identify the user responsible or the account compromised.
- Identity Mapping enables greater visibility into mobile devices accessing Microsoft Active Directory based services over corporate networks.
- Identity Mapping provides visibility into network usage allowing network teams to identify the active users, estimate the impact, and notify the users of a network outage.

## Conclusion

Infoblox Identity Mapping is powerful new technology that gives network administrators, security teams, and other IT groups rich user data to reduce the time to respond, simplify trouble-shooting, and make informed decisions to improve network administration capabilities.

### About Infoblox

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.