Configuring Identity Mapping

You can enable Identity Mapping on the NIOS appliance to provide Active Directory domain user information if the NIOS appliance is connected to a Microsoft server. This feature supports Active Directory domains whose domain controller is running Windows 2008 server, Windows 2008 R2 server, Windows 2012 server, or Windows 2012 R2 server, or Windows 2016 server. Note that Identity Mapping is not supported for the Windows 2003 server and earlier editions. Note that Identity Mapping is not supported on the TE-810, TE-820, IB-VM-810 and IB-VM-820 appliances.

Each network user being mapped can use different devices to access the Windows environment. So using the identity mapping feature and synchronizing all Microsoft servers on the Infoblox appliance provide visibility of user interaction with their environments. By enabling this feature, you can monitor Active Directory domain users, the IP addresses they log on to, the login status, and the time duration of their current status in the IPAM tab.

To view user information, you must first enable this feature at the Grid level. You can enable this feature even when you have not installed an MS Management license on the appliance. However, you cannot configure DNS, DHCP, and Active Directory sites synchronization unless you install an MS Management license on the appliance.

When you enable this feature, the appliance remotely communicates with all synchronized Microsoft servers (Domain Controllers, an Exchange server, or a domain member) to pull event logs. The identity mapping information displayed is as accurate as these event logs are available in the Microsoft authentication logs. Therefore, it is necessary to assign Grid members to Microsoft servers to collect user information from Windows event logs. For information, see Assigning Grid Members to Microsoft Servers.

**Note:** The identity mapping information displayed on NIOS completely depends on live event logs that are available on the Microsoft servers. The appliance pulls event logs incrementally. So subsequent requests pull only the latest logs since the last successful synchronization. To avoid data loss, depending on the expected activities, you must consider the size of the event log file on the Microsoft server and how often you want to synchronize the data with the appliance before the event log file rolls over.

Prerequisites on the Microsoft Server


The identity mapping information is collected successfully only when the Microsoft users belonging to a Domain User group and Event Log Reader group start a RPC session and access MS-EVEN6. The synchronization process is successful when they have this permission. The synchronization process fails unless appropriate permissions are granted. The failed operations are logged in the Microsoft logs. The NIOS appliance tries to collect user information again in the next synchronization.

Administrative Permissions

Only superusers can view identity mapping information. Limited-access admin groups can view identity mapping information only if they have network permissions. For example, if the users have permissions to only DNS zones, they may not be able to view identity mapping information because they do not have network permissions. The appliance does not display a warning message if admins do not have correct permissions. For information about network permissions, see Administrative Permissions for IPv4 and IPv6 Networks and Shared Networks.

About User Sessions

A user session is an abstract concept to specify a single user logging with a network address for a finite period of time. A user session starts when a Kerberos account authentication event or login event is received and ends when a logout is received, although such an event may never be received. In such cases, a session is considered to be timed out. Network user associations are unique for a finite period of time. A single login involves a number of login and logout events. In order to consolidate and improve system performance, Infoblox uses the concept of consolidation window. If a login event or Kerberos service ticket is received within the consolidation window, then that session is considered as an extension from the previous session. If a login event is received outside this window, it is considered as a new session. The number of network users you see depends on the length of the consolidation window.

For example, consider the following sample events occurred on the Microsoft server when the consolidation window is set to 10 minutes:

```
Kerberos Authentication Request: 10:00:00
Kerberos Service Ticket Request: 10:00:01
Account Logon: 10:00:02
Account Logoff: 10:00:03
Account Logon: 10:00:05
Account Logoff: 10:00:07
Account Logon: 10:00:10
Account Logoff: 10:00:11
```

The sample user session for the above events:

<table>
<thead>
<tr>
<th>User Name</th>
<th>IP Address</th>
<th>First Seen Time (UTC)</th>
<th>Last Seen Time (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>10:00:02</td>
<td>10:00:11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10:00:03</td>
<td>10:00:05</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10:00:07</td>
<td>10:00:10</td>
</tr>
</tbody>
</table>
If another login request is received at 10:30 AM (10 minutes after the last seen event), then it is considered as a different session:

<table>
<thead>
<tr>
<th>User Name</th>
<th>IP Address</th>
<th>First Seen Time (UTC)</th>
<th>Last Seen Time (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>John</td>
<td>10.10.10.10</td>
<td>10:00:00 AM (UTC)</td>
<td>10:00:11 AM (UTC)</td>
</tr>
<tr>
<td>John</td>
<td>10.10.10.10</td>
<td>10:30:00 AM (UTC)</td>
<td></td>
</tr>
</tbody>
</table>

If a Kerberos service ticket is received instead of a login event, then the previous session is extended and is updated as **Last Seen Time** in the first user session.

<table>
<thead>
<tr>
<th>User Name</th>
<th>IP Address</th>
<th>First Seen Time (UTC)</th>
<th>Last Seen Time (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>John</td>
<td>10.10.10.10</td>
<td>10:00:00 AM (UTC)</td>
<td>10:30:00 AM (UTC)</td>
</tr>
</tbody>
</table>

The appliance displays separate entries (counts) for the following scenarios:

- Multiple users logging in from the same IP address. For example, User 1 logged in with 10.10.10.10 address counts as one network user and User 2 logged in with 10.10.10.10 address counts as another network user.
- Same user logging in from multiple IP addresses. For example, a single user can log in to multiple workstations, each with a different IP address.
- Same user logging from the same IP address at a different time intervals.

**Network User Count Displayed for Different Login Scenarios**

If you are configuring multiple Domain Controllers belonging to different organizations, then you must configure them in different network views. For example, if the same user logs in to multiple Domain Controllers with the same IP, it creates multiple entries for each login. In this case, there is a chance of overwriting an entry by subsequent events. If Domain Controllers are configured in different views, then separate entries are displayed for different network views. You can configure multiple Domain Controllers within the same network view if they serve the same organization, possibly using a load balancing method.

**Note:** The appliance displays user information only for the managed networks.

The following table illustrates how the appliance displays counts for different login scenarios:

<table>
<thead>
<tr>
<th>Login Scenarios</th>
<th>Appliance Displaying User Mapping Information</th>
</tr>
</thead>
</table>
| Mobile user logging in to the Microsoft Exchange server | Note that you must first synchronize both the Domain Controller and Microsoft Exchange server with the appliance to get user mapping information for this scenario. For this example, two entries are displayed.  
1. User name and IP address of the Microsoft Exchange server on the Domain Controller.  
2. User name and IP address of the mobile device on the Microsoft Exchange server. |
| Multiple users from the same IP address | Appliance displays separate entry (user name and IP address) for each user. |
| Same user from multiple IP address | Appliance displays separate entry (user name and IP address) for each user. |

**Login and Logout Timestamps**

Note that all timestamps are displayed in the time zone of the admin account that you use to log in to the appliance. There is a possibility of missing the login and logout events as described in the following cases:

- There is a chance of missing a login event when NIOS retrieves event logs from the Microsoft server after a user logs in and the event log has already rolled over.
- There is a possibility of missing a logout or session end notifications when the user shuts down the workstation or leaves the system. In such cases, the Microsoft event log does not specifically indicate a logout. The logout events that are missed on the Domain Controller or Exchange server are missed on NIOS as well.

To maintain accuracy, the login timestamp is estimated as logout timestamp minus (-) the idle timeout. However, when a login or Kerberos Authentication event is received, the login timestamp is updated to the value available in the Kerberos authentication event or the login event.

To maintain accuracy of the logout time data, the appliance allows you to configure the length of idle time in the Grid Properties Editor wizard. After this time interval, the status of the user changes to **Timed Out**. For information about how to set timeout length, see Configuring Active User Timeout Session.
Note: The Timed Out and Logged Out user information is periodically removed from the database.

Viewing Active Directory User Information

To view Active Directory user information, you must first enable identity mapping feature at the Grid level. For information about enabling Identity Mapping feature, see Enabling Identity Mapping. After you enable the identity mapping feature, you must synchronize the appliance with all Microsoft servers in order for the appliance to gather user and device mapping information from the Microsoft servers. You can view Active Directory user information in the Network Users tab. For more information, see Viewing Active Network Users.

To synchronize the appliance with Microsoft servers:

1. From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar.
2. Select the Microsoft Integration tab in the Grid Properties Editor wizard, and complete the following:
   - Synchronize Network Users with all MS servers: Select this check box to synchronize users with all Microsoft servers that are managed by the Grid in order for the appliance to gather user and device mapping information from the Microsoft server authentication logs. You can override this value at the Microsoft server level.

Note: On an Infoblox appliance, the Enable Network Users Feature and Synchronize Network Users with all MS servers options are disabled by default for all new installations.

3. Save the configuration.