Exinda How To Guide:

Identify Users on the Network

Exinda User Client 1.1.1

exinda

Copyright

Document Built on Thursday, October 21, 2015 at 02:15AM

Using this guide

Before using this guide, become familiar with the Exinda documentation system.

Documentation conventions

- **bold** - Interface element such as buttons or menus. For example: Select the **Enable** checkbox.
- *italics* - Reference to other documents. For example: Refer to the *Exinda Application List*.
- **>** - Separates navigation elements. For example: Select **File > Save**.
- `monospace text` - Command line text.
- `<variable>` - Command line arguments.
- [x] - An optional CLI keyword or argument. `n {x}` - A required CLI element.
- | - Separates choices within an optional or required element.

Notes, Tips, Examples, and Cautions

Throughout the manual the following text styles are used to highlight important points:

- **Notes** include useful features, important issues. They are identified by a light blue background.

  Note: Text

- **Tips** include hints and shortcuts. They are identified by a light blue box.

Tip Tip text

- **Examples** are presented throughout the manual for deeper understanding of specific concepts. Examples are identified by a light gray background.

EXAMPLE

Text

- **Cautions** and warnings that can cause damage to the device are included when necessary, and are highlighted in yellow.

Caution: Text

Table of Contents

Chapter 1: Integrate the Exinda Appliance with Active Directory

Using the Exinda Active Directory Connector, customers can:

- Expose Active Directory usernames in monitoring and reporting, no longer having to view users as IP addresses.
- Use Active Directory groups and usernames in optimization policies, thereby implementing QoS and Optimization Polices based on individual users or entire groups.

The Exinda Active Directory Connector needs to be installed onto a server in the network that has access to the Active Directory server. Each install of the Exinda Active Directory Connector can talk to up to 20 Exinda appliances.

Complete the following tasks to connect the Exinda Active Directory Connector to the Active Directory server, and view user names in monitoring reports.

1. "Install the Exinda Active Directory Connector" on page 6
    a. "Add Exinda appliances to the Active Directory Connector" on page 9
    b. (Optional) "Configure the connection to the Active Directory server" on page 11
    c. "Select the information sent between the Exinda appliance and the Active Directory server" on page 11
    d. "Change the Active Directory Connector port number" on page 10
2. "Identify users using applications on a Citrix XenApp server" on page 14
3. "Verify communication between the Active Directory server and the Exinda Appliance" on page 12
4. "Report on Network Activity by User" on page 18
5. "Controlling Traffic based on Users" on page 28

> **Note** If you encounter any issues, see "Troubleshoot issues with Active Directory configuration" on page 31

Install the Exinda Active Directory Connector

The Exinda Active Directory Connector needs to be installed onto a Windows server that can connect to the Active Directory server. Each Exinda Active Directory Connector can talk to up to 20 Exinda appliances. When you first install the Exinda Active Directory Connector, it may take 24 hours or longer to get all user to IP address mappings as users progressively login.

Notes

- The Exinda Active Directory Connector is supported on the following platforms:
  - Windows Server 2003 SP2

    When the Active Directory server is running Windows Server 2003 R2, the Exinda Active Directory Connector must be installed on the Active Directory server and cannot be installed on a remote server.
  - Windows Server 2008 SP2
  - Windows Server 2008 R2
  - Windows Server 2012
- The Exinda Active Directory Connector requires .NET Framework 4.0.
- The Logon Auditing must be enabled on the Active Directory server to install the Exinda Active Directory Connector.
- The WMI service must be started on the Active Directory server and on the server where the Exinda Active Directory Connector is installed.
- The Active Directory server and the server where the Exinda Active Directory Connector is installed require the RPC Endpoint Mapper and LDAP ports open in your firewall. These ports are open by default. To verify your settings, see http://support.microsoft.com/kb/179442.

1. Download the installer the Exinda appliance.
   a. Click **Configuration > System > Network**, and switch to the **Active Directory** tab.
   b. Download the **Microsoft Installer Executable**.
2. Save the Exinda Active Directory Connector install to a location that can be accessed by all Windows servers in the network.
3. On the server where the Exinda Active Directory Connector should be installed, locate and double-click installation file.
4. On the Welcome dialog, click **Next**.
5. Read the End-User License Agreement. Select the **I accept...** checkbox and click **Next**.
6. Specify the directory where the Exinda Active Directory Connector should be installed.
7. Select whether the Active Directory server is on **this server** or **another server**.

   If the connector is not installed on the server with Active Directory, type the IP address or hostname of the Active Directory server, and type the username and password of the Administrator account on the Active Directory server.

Caution When the Active Directory server is running Windows Server 2003 R2, the Exinda Active Directory Connector must be installed on the Active Directory server and cannot be installed on a remote server.

Caution When installing the Exinda AD Connector on a server that is not a domain controller, ensure that the account in charge of running the service is an Active Directory domain admin account. See *To ensure the Exinda AD service has the appropriate permissions* below.

8. Click **Next**.
9. (Optional) Type the Exinda appliance IP address or hostname, port number, and administrator password.

   Adding an Exinda appliance can be completed after the Exinda Active Directory Connector is installed.
10. In the **Include log entries newer than the specified age** field, specify the maximum age of log entries (in seconds) to be analyzed and sent to the Exinda appliance when the Exinda Active Directory Connector service starts.
11. Click **Next**.
12. On the Check for Required Services dialog, click **Next**.

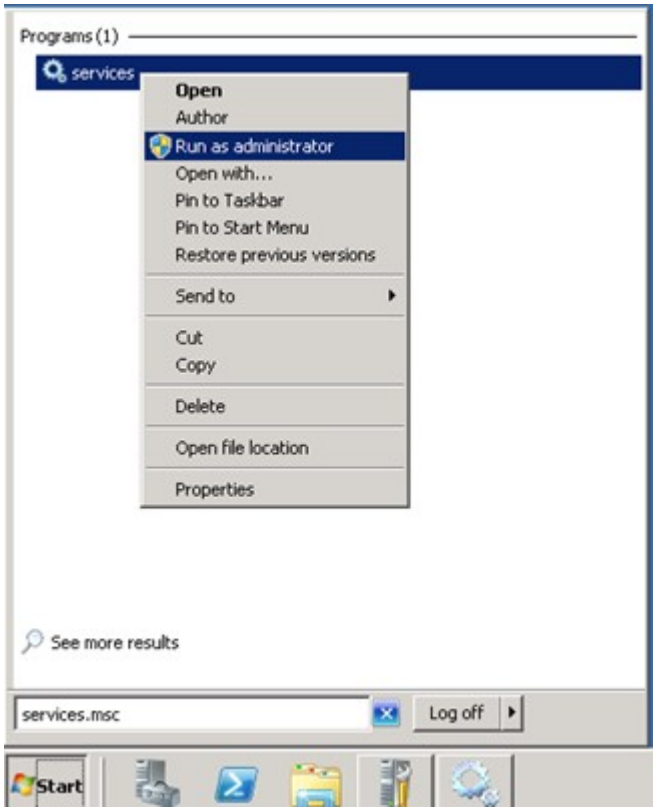
    If any warnings are displayed on the page, resolve the issues as specified in the dialog.
13. Click **Install**.
14. Ensure **Launch Exinda Active Directory Connector** is selected, and click **Finish**.

    After the installation is finished, the Exinda Active Directory Connector starts automatically and attempts to communicate with the configured Exinda appliance.

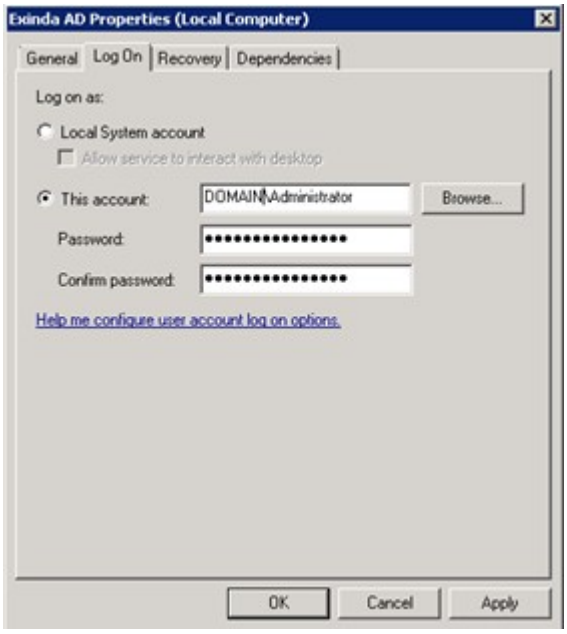
To ensure the Exinda AD service has the appropriate permissions

When installing the Exinda AD Connector on a server that is not a domain controller, ensure that the account in charge of running the service is an Active Directory domain admin account.

1. Run Services.msc as an Administrator.



2. Find **Exinda AD** service and right click on it and select **Properties**.
3. On the **Log On** tab, select the Administrative account of the domain with its password.



Note that the domain and slash (\) is required.

4. Press OK or Apply to save the changes.
5. Restart theservice.

Add Exinda appliances to the Active Directory Connector

Identify the Exinda appliance using this Active Directory Connector to retrieve user and group information.

> **Note** Each installation of the Active Directory Connector can have a maximum of 20 Exinda appliances connected to it.
>
> If there are more than 20 Exinda appliances, install the connector on multiple Windows servers and divide the appliances across multiple instances of the Active Directory Connector.

1. In the **Start** menu click **All Programs > Exinda Networks > Exinda AD Configuration Utility**.
2. Switch to the **Exinda Appliances** tab.
3. To add the Exinda appliances that communicate with this Active Directory Connector, type the IP Address or Hostname into an empty row, and type the Admin password for the appliance.
4. Modify the port number as needed. The default port number of the Active Directory Client is 8015.

When changing the port number, all Exinda appliances using the Exinda Active Directory Connector must use the same port number. See "Change the Active Directory Connector port number" on page 10.

5. In the **Sync interval** field, identify how frequently the Exinda Active Directory Connector contacts the Exinda appliances to synchronize Active Directory user and group information. The default is 5 minutes.
6. Click **OK**.

Change the Active Directory Connector port number

Identify the port on which the Exinda Active Directory Connector is communicating to the connected Exinda appliances. Changing the port number is optional, and the default port 8015 automatically communicates with the Exinda Active Directory Connector and Exinda appliances.

> **Note** The port number must be the same on all installed Exinda Active Directory Connector instances, and all Exinda appliances using the Exinda Active Directory Connector.
>
> Ensure firewall on the server running the Exinda Active Directory Connector is configured to allow inbound and outbound traffic on configured port.

1. Change the port number on the Exinda Active Directory Connector.
   a. In the **Start** menu click **All Programs > Exinda Networks > Exinda AD Configuration Utility**.
   b. Switch to the **Exinda Appliances** tab.
   c. Type the port number in the field.

      The default port number is 8015.
   d. Click **OK**.
2. Change the port number on the Exinda appliances.

   > **Note** The port number must be changed on each Exinda appliance using to the Exinda Active Directory Connector.

   a. Launch Exinda Web UI.
      a. In a browser, enter `https://Exinda_IP_address`.
      b. Enter the appliance **User Name** and **Password**. Click **Login**.

         The Exinda Web UI is displayed.
      c. Ensure you are in **Advanced** mode.
   b. Click **System > Network**, and switch to the **Active Directory** tab.
   c. In the **Active Directory** area, type the port number of the Exinda Active Directory Connector.

      The default port number is 8015.
   d. Click **Apply Changes**.

When the Exinda appliance successfully communicates with the Exinda Active Directory Connector, the following information is displayed in the table:

- **Agent Name**—The Exinda Active Directory Connector name.
- **IP Address**—The IP address of the server running the Exinda Active Directory Connector.
- **Version**—The Exinda Active Directory Connector version.
- **Windows Version**—The version of Windows on the Active Directory server.
- **Last Contact**—The last time the Active Directory server was contacted.

Select the information sent between the Exinda appliance and the Active Directory server

Specify what information is sent between the Active Directory server and the Exinda appliance. When you first install the Exinda Active Directory Connector, it may take up to 24 hours (or longer) to get all user to IP address mappings as users progressively login.

> **Note** User accounts that have been disabled on the Active Directory server are not included in the data sent to the Exinda appliances.

1. In the Exinda Active Directory Connector, switch to the **AD Server** tab.
2. To send a list of users and groups to Exinda appliances when the service starts, select **Send Active Directory user and group information to Exinda appliances**. The list of users and groups that is sent to the appliance can be used to create user or group-based policy.

   If this is not selected, only logged on users will be available to your Exinda appliances. Information about groups will not be available. This information is obtained through an LDAP query against the Active Directory server.

   > **Caution** If there are multiple domain controllers, Send users/groups to Exinda appliances on startup should only be selected on one of the domain controllers.

3. To include user names in monitoring reports, allow the login history to be analyzed.
   a. To enable this option, select **Analyze login history and send to Exinda appliances**.

      This information is obtained through a Windows Event Log query against the Active Directory server.

   b. In the **Include log entries newer than the specified age** field, specify the maximum age of log entries (in seconds) to be analyzed and sent to the Exinda appliance when the Exinda Active Directory Connector service starts.
4. Click **OK**.

Configure the connection to the Active Directory server

The Exinda Active Directory Connector can be installed on any server in the network that has access to the

Active Directory server. If the connector is installed somewhere other than on the Active Directory server, specify the location and authentication credentials of the Active Directory server.

1. In the **Start** menu click **All Programs > Exinda Networks > Exinda AD Configuration Utility**.
2. Switch to the **AD Server** tab.
3. In the Active Directory Server area, select whether the Active Directory server is **this server** or **another server**.
4. Type the IP address or hostname of the Active Directory server.
5. Type the username and password of the Administrator account on the Active Directory server.
6. Click **OK**.

Verify communication between the Active Directory server and the Exinda Appliance

Ensure the communication between the Active Directory server and the Exinda appliance is active.

> **Note** User accounts that have been disabled on the Active Directory server are not included in the data sent to the Exinda appliances.

1. Click **System > Network**, and switch to the **Active Directory** tab.
2. Verify the Active Directory server is listed, and that the service is **Running**.

   When the Exinda appliance successfully communicates with the Active Directory Client, the following information is displayed in the table:

   - **Agent Name**—The Active Directory server name.
   - **IP Address**—The IP address of the Active Directory server.
   - **Version**—The Exinda Active Directory Windows client version.
   - **Windows Version**—The Active Directory server Windows version.
   - **Last Contact**—The last time the Active Directory server was contacted.
3. If the service is not visible on the list, run the Event Viewer program on your Active Directory server, and examine Windows logs.
   a. In the Start menu select **Control Panel > Administrative Tools**.
   b. Double-click **Services**, and verify the status of the **Exinda AD** service. If the service is stopped, restart the service.
   c. In the **Windows Logs > Application** area, the “Service started successfully” message should be displayed from Exinda Networks Active Directory Connector.

      If the communication between the Active Director and the Exinda appliance is failing, an error message from the Exinda Networks Active Directory Connector appears in these logs.

Request updated user and group information from the Active Directory server

If the list of users and groups using the Active Directory client appears to be out of date, erase all username to IP address mappings and refresh the list sent from the Active Directory server.

1. Click **Configuration > System > Network**, and switch to the **Active Directory** tab.
2. To clear user, group, and login data from the appliance and requests an update from the Active Directory clients click **Renumerate**.

Exclude specific usernames from reports

You may have user accounts that should not be linked to IP addresses when reporting on the Exinda appliance,such as the account used for signing SMB traffic. SMB signing was introduced with the 6.4.1 release. Configure the Exinda Active Directory Connector to prevent the IP address to username mapping being sent to the Exinda appliance.

1. In the **Start** menu click **All Programs > Exinda Networks > Exinda AD Configuration Utility**.
2. Switch to the **Excluded Users** tab.
3. Click in the Ignored Users area, type the full username of each user to ignore.

   The username is case sensitive. If the Active Directory has the user Domain/Test.User, and the excluded list has the user as Domain/test.user, the traffic is not excluded.

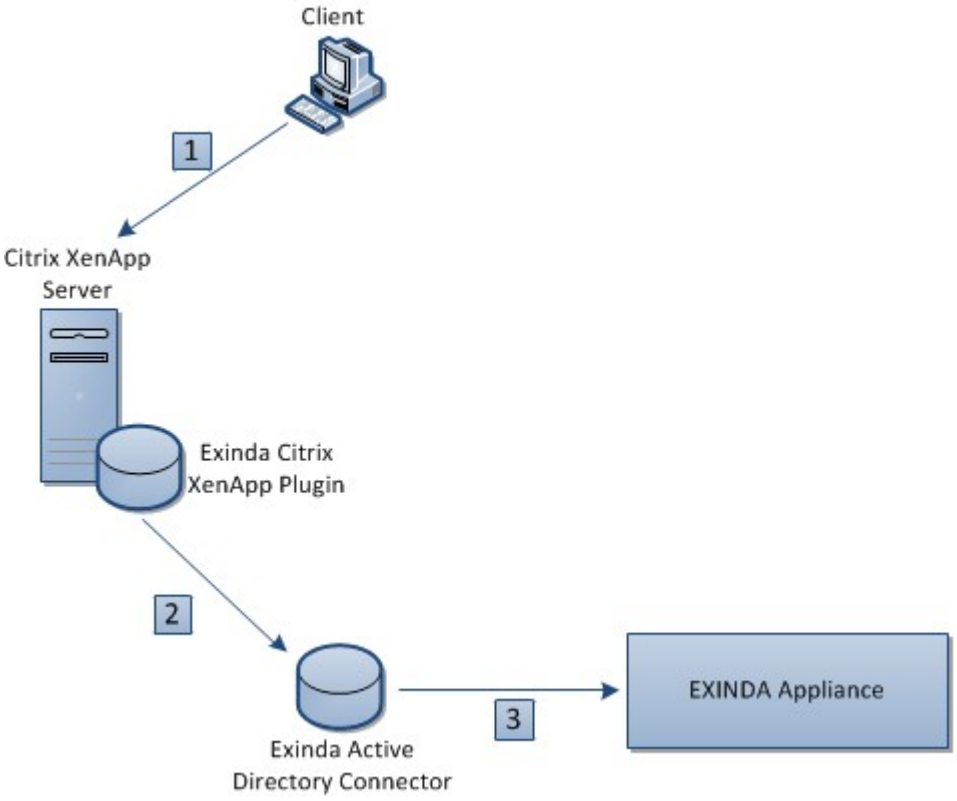
   > **Note** Regardless of the case of usernames in Active Directory, the Exinda appliance displays the usernames with the first name capitalized and the surname in lower case; for example Domain/Test.user. Do not use the value in the Exinda appliance when adding a username to the Excluded list.

4. Click **Apply**.
5. "Request updated user and group information from the Active Directory server" on page 13.
6. Restart the Active Directory service. See "Change the state of the Exinda Active Directory Connector" on page 17.

Chapter 2: Identify users using applications on a Citrix XenApp server

A Citrix XenApp server hosts a virtual desktop with pre-installed software that users with the correct credentials can access as needed. This allows the company to provide access to commonly used software without having to maintain and upgrade installations on each client computer in the network.

Because the Citrix XenApp server is treated as a single IP address by the Exinda appliance, and the IP address of the clients connecting to the server are ignored, the Exinda appliance cannot include the names of users whom are accessing the applications on the XenApp server. Exinda has created a plug-in for the Citrix XenApp server that sends the IP address of the client computer and the user name used to authenticate with the XenApp server to the Exinda Active Directory Connector when a user accesses an application through the XenApp server.



When a user on a client computer logs into a Citrix XenApp server (1), their IP address and user name are captured by the Exinda Citrix XenApp Plugin and sent on to the Exinda Active Directory Connector (2). The connector then sends the user name and IP address of the XenApp user to the Exinda appliance to include in reports (3).

Install and configure the Exinda Citrix XenApp Plugin to identify activity by specific users on the XenApp server.

Install the Exinda Citrix XenApp Plugin

The Exinda Citrix XenApp Plugin sends the IP address and username of the user using the application on the XenApp server to the Exinda Active Directory Connector so the user names can be displayed in reports on the Exinda appliances. The Exinda Citrix XenApp Plugin must be installed on each Citrix XenApp server in the network.

Note The Exinda Citrix XenApp Plugin is supported on Citrix XenApp Servers version 6.0.

1. Download the installer the Exinda appliance.
   a. Click **Configuration > System > Network**, and switch to the **Active Directory** tab.
   b. Download the **Microsoft Installer Executable**.
2. Save the Exinda Citrix XenApp Plugin install to a location that can be accessed by the Citrix XenApp server.
3. On the server where the Exinda Citrix XenApp Plugin should be installed, locate and double-click installation file.
4. At the Welcome dialog, click **Next**.
5. Specify the directory where the Exinda Citrix XenApp Plugin should be installed. Click **Next**.
6. Read the End-User License Agreement. Select **I Agree** and click **Next**.
7. To confirm the installation, click **Next**.

   The Exinda Citrix XenApp Plugin is installed.
8. When the installation is completed, click **Close**.

Add the Exinda Active Directory Connector to the Exinda Citrix XenApp Plugin

To ensure user activity on the Citrix XenApp server is reported on the Exinda appliance, add the connection details for the Exinda Active Directory Connector to the Exinda Citrix XenApp Plugin.

1. Open the Exinda Citrix XenApp Plugin.
2. On the **Synchronization** tab double-click in the **Location** area of the first blank line.
3. Type the IP address or hostname and port number of the computer where the Exinda Active Directory Connector is installed.

> **Note** The port number used to communicate between the Exinda Active Directory Connector and the Exinda Citrix XenApp Plugin cannot be the same as the port number used to communicate between the Exinda Active Directory Connector and the Exinda appliances.

4. In the **Sync Interval** field, identify how frequently the Exinda Active Directory Connector sends XenApp server user information to the Exinda Active Directory Connector. The default is 1 minute.
5. Click **Apply**.

Capture the Exinda Citrix XenApp Plugin activity in a log file

Depending on the logging level selected, the Exinda Citrix XenApp Plugin records various types of data in a log file. The available log levels include Error, Warning, Info, and Verbose. By default, the log sensitivity is Warning. The location of the log file and the level of detail recorded in the log file are configurable.

1. Open the Exinda Citrix XenApp Plugin.
2. On the **AD Server** tab, specify the location where log files should be stored.
3. Switch to the **Console** tab and select the level of messages that are recorded in the log file from the **Log Sensitivity** list.
4. Click **Apply**.
5. To view the contents of the log, on the **Console** tab click **Open Log**.

Change the Exinda Citrix XenApp Plugin port number

Identify the port on which the Exinda Active Directory Connector is communicating to the connected Exinda Citrix XenApp Plugins. The default port number is 8016.

1. Change the port number on the Exinda Citrix XenApp Plugin.
    a. In the **Start** menu click **All Programs > Exinda Networks > Exinda Citrix XenApp Plugin Configuration**.
    b. Switch to the **Synchronization** tab.
    c. Double-click the port number for the appropriate Exinda Active Directory Connector and type the new port number in the field.
    d. Click **OK**.
2. Change the port number on the Exinda Active Directory Connector.
    a. In the **Start** menu click **All Programs > Exinda Networks > Exinda AD Configuration Utility**.
    b. Switch to the **XenApp** tab.
    c. Type the port number in the field.
    d. Click **OK**.

Request updated user information from the Exinda Citrix XenApp Plugin

If the synchronizations of the user data between the Exinda Citrix XenApp Plugin and the Exinda Active Directory Connector is infrequent, trigger the Exinda Citrix XenApp Plugin to send the data to the Exinda Active Directory Connector immediately.

1. In the **Start** menu click **All Programs > Exinda Networks > Exinda AD Configuration Utility**.
2. Switch to the **XenApp** tab.
3. Click **Renumerate**.

   The latest data is sent from the Exinda Citrix XenApp Plugin to the Exinda Active Directory Connector.

Change the state of the Exinda Active Directory Connector

Temporarily stop or disable the Active Directory integration to help with troubleshooting and to avoid errors when modifying the Exinda Active Directory Connector settings.

1. Click **Configuration > System > Network**, and switch to the **Active Directory** tab.
2. Modify the state of the Active Directory service.
   - To temporarily stop the Exinda Active Directory Connector, click **Stop**.
   - If you are experiencing issues with the Exinda Active Directory Connector, **Restart** the service.
   - If you no longer need the Exinda Active Directory Connector running, click **Disable**.
   - If the service has been disabled, to start it again click **Enable**.

Chapter 3: Report on Network Activity by User

Use the information in reports to determine how the policies on your Exinda can improve the quality of service and the experience of your network users.

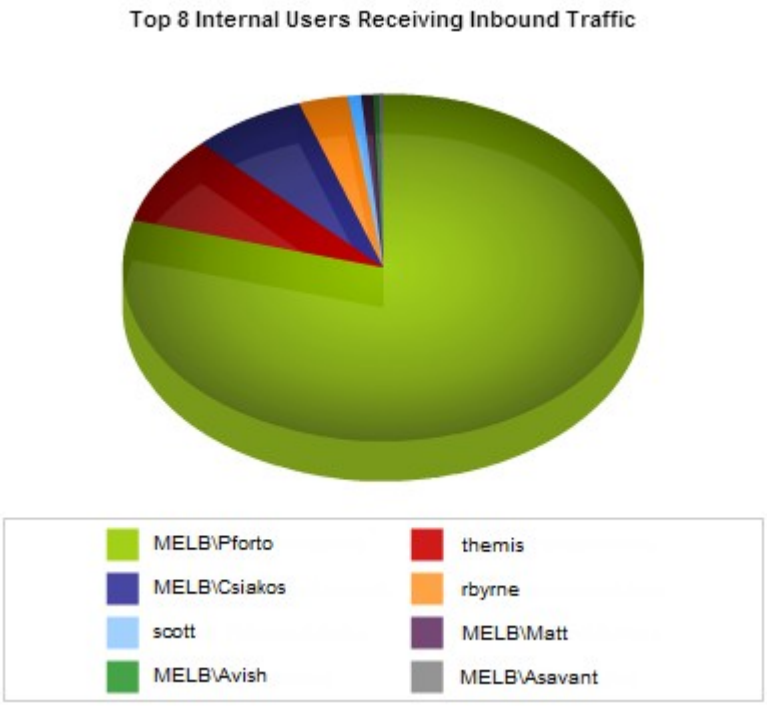
The following reports identify user activity on the network:

Users Report

The users report shows the top users by data volume for the selected time period. Traffic inbound into your LAN is reported separately from the outbound traffic. You can choose to view either the internal users or the external users on the users report. These charts can answer questions such as, “What internal users are the top talkers and top listeners? Which external users are top talkers from which internal hosts are retrieving information and which external users are top listeners from which internal hosts are sending information to? Could one user be choking out my network?" Using this information you can determine if you need to create policies for these high data volume users. You may want to create protection policies for your important users, like your CEO or finance department, or create control policies to limit users who are abusing the network.

Users are associated with an IP address. During a flow, traffic flows from one host to another. Typically, one host is considered internal to your network; the other is external. Hosts that fall into a network object that was defined as internal are considered internal to your network; Hosts that fall into a network object that was defined as external are considered external to your network. Keep in mind that the traffic is inbound and outbound relative to your LAN – not relative to the host or user. Therefore, inbound traffic for an external user means that user was sending data inbound into your network.

You can drill into the user by clicking on the user name in the tables below the charts. This will show the Applications Report for the user that you drilled into. You can then use the selector on the Applications Report page to show URLs or conversations or hosts that involved the user.



The tables at the bottom of the report shows for each of the top users, the total amount of data, and the maximum and average throughput rates, the number of packets, and the number of flows for the selected time period. More network metrics, such as, round-trip time (RTT), network and server delays, and TCP efficiency can be shown by clicking on the **Show Details** link in the tables.

Top 50 Internal Users Receiving Inbound Traffic

Name [+] Show Details	Packets	Data (MB)	Throughput (kbps) Average	Max	Flows
MELB\Pforto	256599	328.319	264.20	4034.39	224
themis	224420	142.290	28.87	1656.61	1194
MELB\Kdeikos	76578	101.077	79.85	887.10	433
MELB\Csiakos	90826	89.588	21.56	3961.84	564
rbyrne	55507	75.806	167.84	946.30	84
MELB\Asavant	110339	71.434	7.47	612.92	1124
scott	60506	54.297	12.48	695.97	689
MELB\Matt	33342	27.351	9.67	1854.87	455
salah-pc	34944	26.560	11.65	855.17	498
MELB\Avish	41831	14.614	1.58	172.73	2243

Where do I find this report?

Go to **Monitor > Users**.

To show only internal users or external users

Use the **Select Users to View** selector at the top of the page.

How do I interact with the pie-based reports?

You can hover over the pie slices to view the amount of data transferred as well as view the percentage of the pie. Note that the pie is showing only the top items, so the proportion is relative to the top items - not relative to all the traffic through the appliance. That is, if one wedge showed 50% of the traffic that means it is 50% of the top items, not 50% through the appliance.

To understand how to set the desired time range for a chart, see Setting the Time Range.

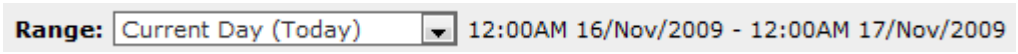
To understand how to drill into the data to find particular filtered data, see Drilling into the Data.

To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Set the Time Period Reflected in the Report

The data displayed in the reports can be focused on specific periods of time. Date ranges are available on all reports except the Real Time reports.

1. Select a report from the Monitor list.
2. Beside the title of the report, select the desired date range from the drop down list.



3. To specify a custom date range, in the drop down list select **Custom**. Select the start and end date and time to include in the report.

After the date range is select, the graphs and charts are immediately updated.

Data Granularity

The Exinda appliance stores data for the following amount of time:

- 2 years of data - this year, previous year & last 12 months
- 2 months of data - this month, previous month & last 30 days
- 2 weeks of data - this week, previous week & last 7 days
- 2 days of data - today, yesterday & last 24 hours
- 1 day of data - this hour, last hour & last 60 minutes, last 5 minutes

For the Applications, URLs, Users, Hosts, Conversations and Subnets Reports, the data is stored at:

- Hourly granularity for up to 2 days (today, yesterday, this hour, previous hour)
- Daily granularity for up to 2 months (this week, last week, this month and last month)
- Monthly granularity for up to 2 years (this year, last year)

For the Interface, Network, Reduction, Optimizer, Service Levels, System the data is stored at:

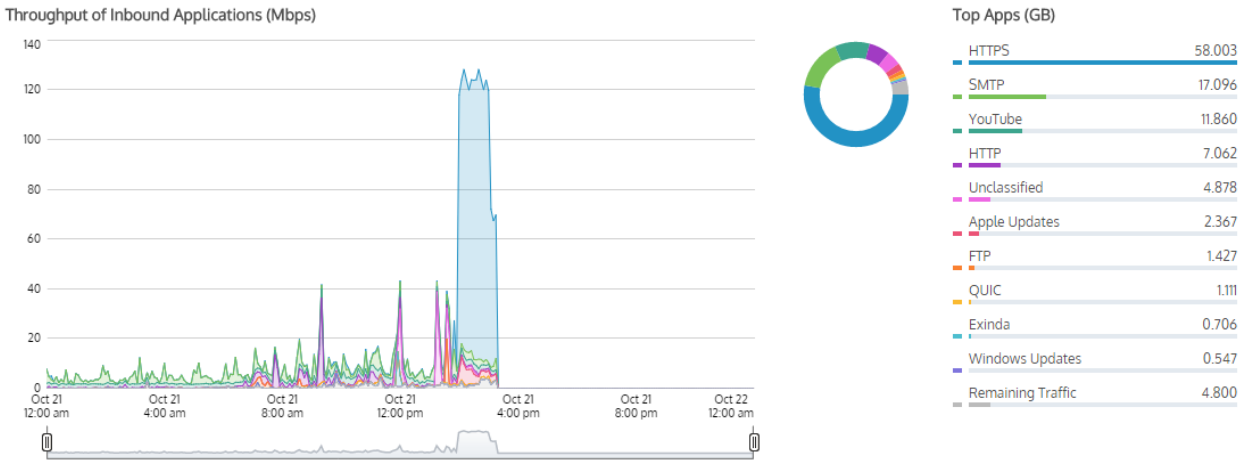
- 10 second granularity for 1 day (except Network)
- 5 minute granularity for 2 weeks

- 30 minute granularity for 2 months
- 60 minute granularity for 6 months
- 24 hour granularity for 2 years

Application Report

The applications groups report shows the top applications by data volume for the selected time period. The applications report shows inbound traffic separately from outbound application traffic. These charts can answer questions such as, “Which applications may be overrunning my network? Is the proportion of traffic for a particular application what I am expecting?” Using this information you can determine if you need to create policies to control or protect these high data volume applications.

You can drill into the application by clicking on the application name in the tables below the charts. This will show a report with the top listeners and talkers for that specific application.



The tables at the bottom of the report shows for each of the top applications, the total volume of data, and the average throughput rates.

Inbound Applications

Name	Total Volume	Avg Throughput
HTTPS	61.789 GB	6.143 Mbps
SMTP	17.466 GB	1.736 Mbps
YouTube	11.969 GB	1.190 Mbps
HTTP	7.218 GB	0.718 Mbps
Unclassified	4.880 GB	0.485 Mbps
Apple Updates	2.528 GB	0.251 Mbps
FTP	1.427 GB	0.142 Mbps
QUIC	1.122 GB	0.112 Mbps

Where do I find this report?

Go to **Monitor > Applications**

Top Internal and External Users on the Network

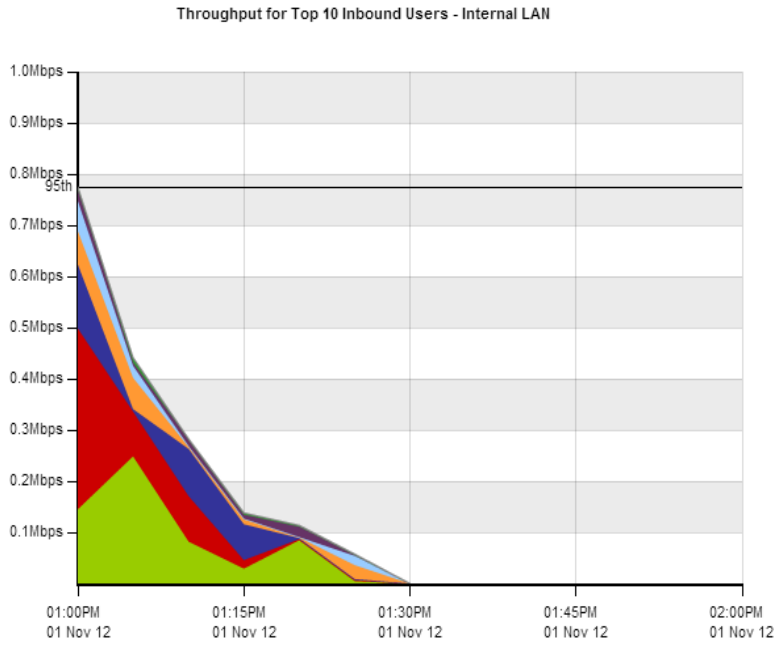
The Network - Users (Internal) and Users (External) reports displays the top users sending traffic through the network.

1. Click **Monitor > Network**.
2. In the Select Graph to Display list, select **Users - Internal** or **Users - External**.
3. "Set the Time Period Reflected in the Report" on page 20.

   After the date range is select, the graphs and charts are immediately updated.
4. Remove specific types of traffic from the graph by deselecting their checkbox in the legend below the graph.
5. To determine what the size of your WAN link should be configured to, from the **Select Percentile**

Marker to Display select **95th**.

Use the 95th percentile mark for throughput speed to configure your WAN link.



Name	Total Data (MB)	Throughput Max (Mbps)	Throughput Avg (Mbps)
EXANET\Brad	8.866	0.249	0.020
EXANET\Dale	14.765	0.354	0.033
EXANET\Jan	9.689	0.125	0.022
EXANET\Micheal	4.834	0.065	0.011
EXANET\Ian	0.228	0.008	0.001
EXANET\Vince	0.152	0.002	0.000

Hosts/Users in Real Time

The Hosts in Real Time monitor shows the top internal hosts by bandwidth consumption observed by the Exinda appliance during the last 10 seconds. This report can answer questions such as, “My link is congested; Which hosts are on my network right now?”

The Hosts in Real Time monitor shows inbound host traffic separately from outbound host traffic. The traffic is sorted by transfer rate. The packet rate and number of flows for each application in that 10 second period is also shown and optionally the user name of the internal hosts. The Distribution percentage shows the proportion of bandwidth consumption of each host relative to all hosts. You can set the chart to refresh frequently or infrequently or not at all. Each refresh shows 10 seconds of data.

Inbound Hosts/Users				
IP Address (User)	Transfer Rate (kbps)	Packet Rate (pps)	Flows	Distribution (%)
Total	**138.037**	**46**	**117**	
172.16.0.246 (Ksiakou)	105.324	10	5	
172.16.0.134 (Pforto)	13.909	3	4	
172.16.1.70 (Selfservice)	6.639	18	3	
172.16.1.240	3.771	6	34	
172.16.0.211	3.554	3	12	
172.16.0.244 (Cniko)	1.295	2	15	
172.16.0.127 (Sshannon)	1.060	2	20	
172.16.1.74	0.684	0	1	
172.16.0.239 (Jbothe)	0.593	1	5	
172.16.0.63 (Lenehan)	0.493	0	1	
Other	0.715	2	9	

Where do I find this report?

Go to **Monitor > Real Time > Hosts/Users**.

To show the user associated with the internal hosts

Check the **Show Users** checkbox.

> **Note** Active Directory must be configured on the Exinda appliances before user names can be displayed in reports. See "Integrate the Exinda Appliance with Active Directory" on page 6.

Conversations in Real Time

The Conversations in Real Time monitor shows the top conversations by throughput observed by the Exinda appliance during the last 10 seconds. This report can answer questions such as, “My link is congested; who's doing what on my network right now? I think I have a problem with a particular host or subnet; what is that host or subnet doing right now? Is the traffic being accelerated or processed by Edge Cache properly? Is the traffic passing through my High Availability or Cluster correctly?"

The Conversations in Real Time monitor shows inbound conversation traffic separately from outbound conversation traffic. The conversations are represented as external IP, internal IP, and application. Some traffic types will show extra information, such as the URL for example, in square brackets following the application. The traffic is sorted by transfer rate. The packet rate and number of flows for each conversation in that 10 second period is also shown. You can set the chart to refresh frequently or infrequently or not at all. Each refresh shows 10 seconds of data.

The Conversations in Real Time monitor can help you diagnose an issue:

- by allowing you to filter the conversations by IP address or subnet,
- by showing the user name associated with the internal IP address,
- by showing which policy the conversation falls into,
- by allowing connections within a flow to either be shown individually or to be grouped together,
- by highlighting accelerated conversations (in yellow) and indicating the acceleration technique being used,
- by highlighting conversations that have been processed by Edge Cache (in blue), and
- by indicating how the conversations is flowing through the high availability cluster
- by indicating if you're seeing asymmetric traffic.

Inbound Conversations						
	External IP	Internal IP	Application	Transfer Rate (kbps)	Packet Rate (pps)	Flows
	Total			**1408.428**	**284**	**24**
	192.168.10.1	192.168.10.128	MAPI	570.834	82	1
	192.168.10.9	192.168.10.128	MAPI	483.247	54	2
	192.168.10.7	192.168.10.128	MAPI	275.334	92	2
	192.168.10.10	192.168.10.128	MAPI	65.153	51	2
	192.168.10.7	192.168.10.128	HTTPS[perf-win2k8]	5.496	1	1
	192.168.10.9	192.168.10.128	LDAP	2.939	1	1
	10.20.4.1	239.255.255.250	udp ports 62612 -> 3702	1.097	0	1
	10.20.4.1	239.255.255.250	udp ports 62610 -> 3702	1.069	0	1
	192.168.10.1	192.168.0.1	NetBIOS	0.623	1	1
	192.168.10.10	192.168.10.128	LDAP	0.556	0	2
	192.168.10.132	255.255.255.255	DHCP	0.541	0	1
	192.168.10.9	192.168.0.1	NetBIOS	0.225	0	1
	10.20.3.118	10.20.255.255	NetBIOS	0.225	0	1
	192.168.10.9	192.168.255.255	NetBIOS	0.225	0	1
	10.20.11.100	224.0.0.252	udp ports 58633 -> 5355	0.212	0	1
	10.20.0.14	10.20.255.255	NetBIOS	0.193	0	1
	192.168.10.9	192.168.10.128	LDAP	0.174	0	1
	192.168.10.1	192.168.10.128	MSRPC	0.106	0	1
	192.168.10.9	192.168.0.1	DNS	0.102	0	1
	10.20.0.181	10.20.255.255	NetBIOS	0.075	0	1

Where do I find this report?

Go to **Monitor > Real Time > Conversations**.

To understand the acceleration and high availability icons & coloring

When a conversation has been accelerated by the Exinda appliance, the conversation is highlighted in yellow and the application acceleration technologies being applied to that conversation are displayed on the left-hand side as a series on icons.

For example, the FTP connection below is accelerated (shown in yellow) and is also been processed by WAN Memory (indicated by the icon).

	172.16.101.30	172.16.1.71	FTP

When a conversation has been processed by Edge Cache, it is highlighted in blue.

The following legend describes the meaning of each acceleration icon.

	WAN Memory: The connection is been processed by WAN Memory.
	CIFS Acceleration: The connection is been processed by CIFS Acceleration.
	SSL Acceleration: The connection is been processed by SSL Acceleration.
	NCP Acceleration: The connection is been processed by NCP Acceleration.
	MAPI Acceleration: The connection is been processed by MAPI Acceleration.

When an appliance is deployed in a High Availability (HA) or Clustering mode, the following icons may also appear next to each conversation.

	Asymmetric: The traffic is asymmetric, and is not being accelerated.
	Local: The connection is passing through this appliance in the cluster.
	Remote: The connection is passing through another appliance in the cluster.
	Local/Remote: The connection is passing though both this and other appliances in the cluster.

To filter by IP address or subnet

Simply type the IP address or subnet in the **IP/Subnet Filter** field at the top of the screen and click **Apply**. The conversations can be filtered by IPv4 or IPv6 addresses.

To show the user associated with the internal hosts

Check the **Show Users** checkbox.

To group individual connections within a flow as a single line item or to show each connection as a separate line item

Toggle on or off the **Group** checkbox at the top of the screen.

To display the policy the conversation falls into

Select **Show Policies** checkbox at the top of the screen.

Trouble-shooting virtual circuits and policies

If you are unsure whether traffic is being processed properly by the virtual circuit or the policies within your virtual circuit, it is best to use real time monitoring to determine if traffic is hitting your virtual circuit as you would expect.

1. On the Real **Time Conversations** screen.
2. Select **Show Policies** checkbox at the top of the screen to group the conversations by virtual circuit and policy.
3. Look at the traffic falling under your virtual circuit to decide if the correct traffic is in there.
4. If there is traffic that you were expecting that is not there, look in other virtual circuit groups to see where you expected traffic is.
5. If your traffic is falling into the wrong virtual circuit, check the definition of the affected virtual circuits and ensure the most specific virtual circuit is higher in the policy tree.

Understanding the Conversation Report

When a conversation has been accelerated by the Exinda appliance, the Conversation are highlighted in yellow and the Application Acceleration technologies being applied to that conversation are displayed on the left-hand side as a series on icons. For example, the FTP connection below is accelerated and is also been process by WAN Memory.

When a conversation has been processed by Edge Cache it is highlighted in blue.

The following legend describes the meaning of each icon.

	WAN Memory: The connection is been processed by WAN Memory.
	CIFS Acceleration: The connection is been processed by CIFS Acceleration.
	SSL Acceleration: The connection is been processed by SSL Acceleration.
	NCP Acceleration: The connection is been processed by NCP Acceleration.
	MAPI Acceleration: The connection is been processed by MAPI Acceleration.

When an appliance is deployed in a High Availability (HA) or Clustering mode, the following icons may also appear next to each conversation.

A	Asymmetric: The traffic is asymmetric, and is not being accelerated.
L	Local: The connection is passing through this appliance in the cluster.
R	Remote: The connection is passing through another appliance in the cluster.
L R	Local/Remote: The connection is passing though both this and other appliances in the cluster.

Chapter 4: Controlling Traffic based on Users

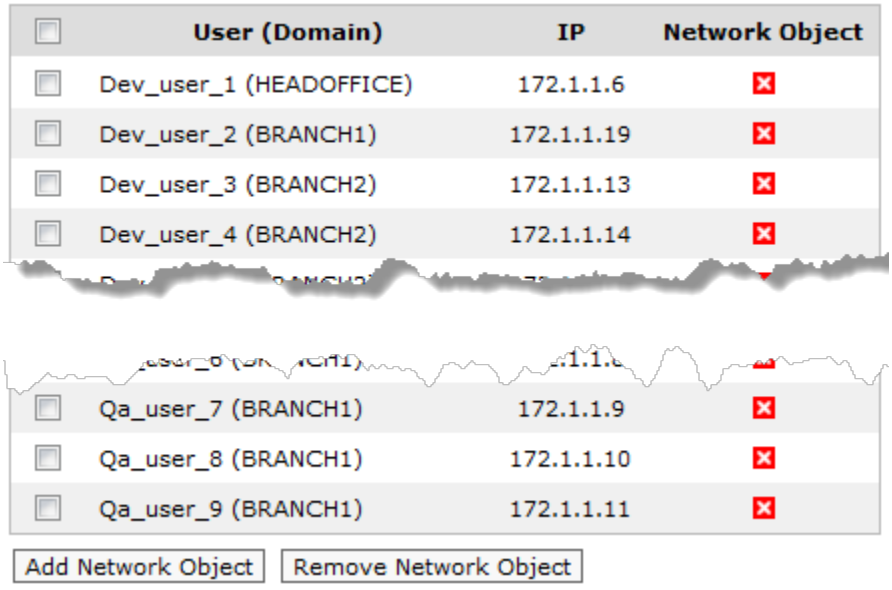
After reviewing the traffic patterns of the users, it may be necessary to implement optimization policies to ensure a positive user experience for key applications or traffic types. By limiting the traffic usage for a specific group of users, network availability can be increased for other user groups.

> **Note** Active Directory must be configured before optimization policies can target specific users and groups. See "Integrate the Exinda Appliance with Active Directory" on page 6.

1. "Configure Network User Objects" on page 28 and "Configure Network User Groups" on page 29.
2. "Optimize Traffic Based on Users and Groups" on page 29

Configure Network User Objects

The Network Users page displays a pre-populated list of users (and their associated IP addresses) from either the Exinda Active Directory Connector, or from static users entered using the CLI. Select which individual users you want to define as dynamic network objects. Once a user is defined as a dynamic network object, it can be used in the Optimizer policies.



Where do I find this configuration?

Go to Objects **> Users & Groups > Network Users**.

To define a user as a dynamic network object

1. Select the checkbox for the user.
2. Click **Add Network Object**.

   The Network Status icon for the user changes to , indicating it is a network object.

To stop identifying a user as a dynamic network object

1. Select the checkbox for the user.
2. Click **Remove Network Object**.

   The Network Status icon for the user changes to , indicating it is no longer a network object.

Configure Network User Groups

The Network Groups page displays a pre-populated list of groups from either the Exinda Active Directory Connector, or from static groups entered using the CLI. This page allows you to select which groups you want to define as dynamic network objects. Once a group is defined as a dynamic network object, it can be used in the Optimizer policies.

Where do I find this configuration?

Go to **Configuration > Objects > Users & Groups > Network Groups**.

To define a group as a dynamic network object

1. Locate the group in the list, and click **Edit**.
2. To map all users within the selected network group to the network object, select **Map to Network Object**.
3. Select **Ignore Domain** to exclude the domain prefix.
4. Click **Apply**.

   The Network Status icon for the group changes to , indicating it is a network object.

   If the dynamic network object is created from multiple groups, the groups are combined into a single entry and each domain is identified after the group name.

To stop identifying a group as a dynamic network object

1. Locate the group in the list, and click **Delete**.

   The Network Status icon for the user changes to , indicating it is no longer a network object.

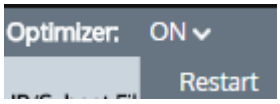
   If the dynamic network object was created from multiple groups, each group is again listed individually in the list.

Optimize Traffic Based on Users and Groups

Create policies that affect the traffic based on the source or destination host.

Note Active Directory must be configured before optimization policies can target specific users and groups. See "Integrate the Exinda Appliance with Active Directory" on page 6.

1. Click **Configuration > Optimizer > Policies**.
2. Type a name for the policy.
3. Set the required bandwidth and acceleration parameters.
4. In the Filter Rules area, select the network user or network group object in the Host source and destination fields, and specify the ToS/DSCP or Application traffic to be affected.
5. Click **Create New Policy**.
6. Once the desired policies are in place on all Exinda appliances, restart the Optimizer. In the appliance status bar, click on the down arrow next to “Optimizer” and select “Restart”



Chapter 5: Troubleshoot issues with Active Directory configuration

If you are experiencing issues with the Active Directory integration, these troubleshooting topics may help resolve the issue.

The Exinda appliance reboots every night

Problem

When multiple installations of the Exinda Active Directory Connector have the **Send Active Directory user and group information to Exinda appliance(s) at startup** option selected, the Exinda appliance is overwhelmed with duplicate data from the connectors and causes the appliance to shut down.

Resolution

1. On each instance of the Exinda Active Directory Connector, check whether the **Send Active Directory user and group information to Exinda appliance(s) at startup** option is selected.
2. If the option is selected on more than one instance, deselect the option on all Exinda Active Directory Connectors.
3. Choose one instance of the Exinda Active Directory Connector, and select the **Send Active Directory user and group information to Exinda appliance(s) at startup** checkbox, and click **OK**.

WMI Service is not running

Problem

When I try to access the Exinda Active Directory Connector, the message “The installer has detected that WMI Service is not running. Consult Windows Help files to find information on how to start WMI Service.” is

displayed.

Resolution

This message indicates that Windows Management Information (WMI) service is disabled. The Exinda Active Directory Connector will not be able run correctly until the WMI service is started.

To start the WMI service, at a command prompt type the following command: `net start winmgmt`

System account showing in traffic reports

Problem

When viewing conversations, the IP address and username of an account created for signing SMB traffic is being displayed as generating traffic rather than the actual user generating the traffic.

Resolution

When SMB signing is configured and enabled, the SMB signing account is the last user account registered as using an IP address, the Exinda Active Directory Connector transfers the SMB signing account as the username that is generating the traffic. To ignore the SMB signing account and report the traffic as being generated by the actual user, configure the Exinda Active Directory Connector to ignore the SMB signing account. See "Exclude specific usernames from reports" on page 13.

No communication between the Exinda Active Directory Connector and the Exinda appliance

Problem

You see one of the following symptoms:

- A connection cannot be established between the Exinda Active Directory Connector and the Exinda appliance.
- The Last Contact status on the **System > Network > Active Directory** tab is blank or red.

Resolution

Ensure your firewall allows incoming and outgoing traffic on the port configured for the Exinda appli- ance to communicate with the Exinda Active Directory Connector

The IP addresses are not being mapped to the AD users and groups

Problem

When integrating the AD client with the Exinda appliance, the IP addresses are not being mapped to the users and groups on the Exinda appliance.

Resolution

Logon auditing must be enabled for IP address to be mapped to the users.

You can investigate by verifying whether the domain controller is logging particular event IDs. If these events are absent then you will need to enable logon auditing.

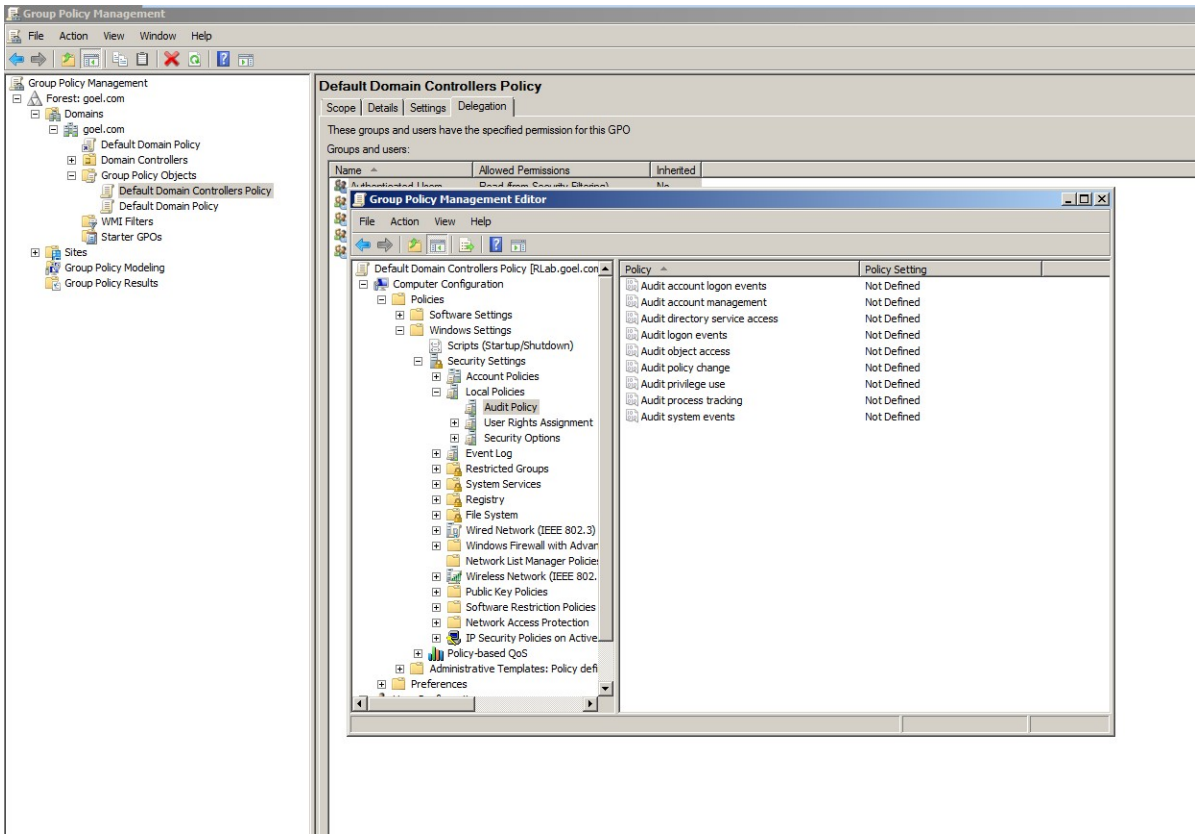
1. In the Domain Controller, go to **Event Viewer > Windows Logs > Security Logs**.

   For Windows Server 2008, 2008 R2, 2012, and 2012 R2, you should see Event ID #4624

   For Windows Server 2003, 2003 R2, you should see Event ID #528 and 540.

If the Domain Controller is not logging these events, then you need to enable **logon auditing** on the domain controller and renumerate the AD client on the Exinda appliance.

1. In the Domain Controller, go to **Start menu > Administrative Tools > Group Policy Management Snap-in**.
2. In the Group Policy Management tree, go to your domain, expand the **Group Policy Objects** node, and select **Default Domain Controllers Policy**.



3. Right click on **Default Domain Controllers Policy** and select **Edit** from the context menu.
4. In the **Group Policy Management Editor** dialog, in the tree control, go to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy**.
5. In the policy list on the right, click on **Audit logon events** and ensure that **Success** is checked.

6. On the Exinda appliance,go to **System > Network > Active Directory**.
7. Click the **Renumerate** button.
8. Apply the changes by executing the following command via a CMD console in the Domain Controller:

   ```
   gpupdate /force
   ```

Exinda Active Directory Connector stops running

Problem

Even after restarting the Exinda Active Directory Connector or the Exinda AD service the Exinda Active Directory Connector does not continue running, and requires constant restarts.

Resolution

1. The Exinda Active Directory Connector requires .NET version 4.0 for it to run successfully on a server other than the Active Directory server. Ensure .NET 4.0 or later is installed on the server running the Exinda Active Directory Connector.
2. If the Active Directory server is running Windows 2003 R2, ensure the Exinda Active Directory Connector is installed directly on the Active Directory server.
3. Review your event logs for .NET Run Time errors, and attempt to resolve those errors. The .NET installation may need to be reinstalled and the .NET 4.0 services and other environmental services such as WMI may need to be updated.

Excluded users still appear on the Exinda appliance

Problem

Even though a user name has been added to the Excluded list on the Exinda Active Directory Connector, the username continues to appear associated with traffic on the Exinda appliance.

Resolution

1. Verify that the username on the Excluded tab of the Exinda Active Directory Connector matches the username in Active Directory.

   The username is case sensitive. If the Active Directory has the user Domain/Test.User, and the excluded list has the user as Domain/test.user, the traffic is not excluded.

   Note Regardless of the case of usernames in Active Directory, the Exinda appliance displays the usernames with the first name capitalized and the surname in lower case; for example Domain/Test.user. Do not use the value in the Exinda appliance when adding a username to the Excluded list.

2. If the case matches on the usernames, restart the AD Client Service and renumerate the Exinda appliance. See "Change the state of the Exinda Active Directory Connector" on page 17 and "Request updated user and group information from the Active Directory server" on page 13.

Changes to the Exinda Active Directory Controller have no effect

Problem

After making changes to the configuration of the Exinda Active Directory Controller, the information reported on the Exinda appliance appears to be the same as before the changes.

Resolution

1. To ensure the latest configuration is being used, restart the AD Client Service and renumerate the Exinda appliance. See "Change the state of the Exinda Active Directory Connector" on page 17 and "Request updated user and group information from the Active Directory server" on page 13.