Exinda's Active Directory Integration

Exinda ExOS Version 6.3

Table of Contents

Part

1 Introduction

Exinda's Active Directory Integration

Exinda Firmware Version: 6.3

1.1 Using this Guide

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

- Useful features, hints and important issues are called "notes" and they are identified in a light blue background.

Note: This is a note.

- Practical examples are presented throughout the manual for deeper understanding of specific concepts. These are called "examples" and are identified with a light green background.

This is an example.

- Warnings that can cause damage to the device are included when necessary. These are indicated by the word "caution" and are highlighted in yellow.

Caution: This is a caution.

Part II

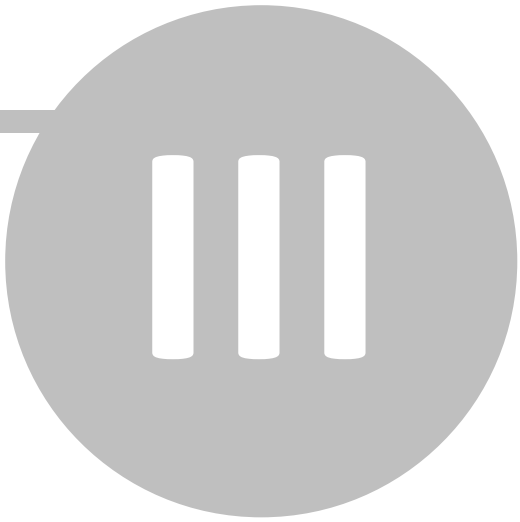
2 Overview

Using the Exinda AD service, customers can:

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

This How to Guide explains how to install and configure the Exinda AD service.

Part



3 Active Directory Environment

Exinda's Active Directory integration requires the Exinda AD service be installed on one or more Active Directory servers (supports Windows Server 2003 and Windows Server 2008). Each AD server can talk to one or more Exinda appliances using the Exinda AD service.

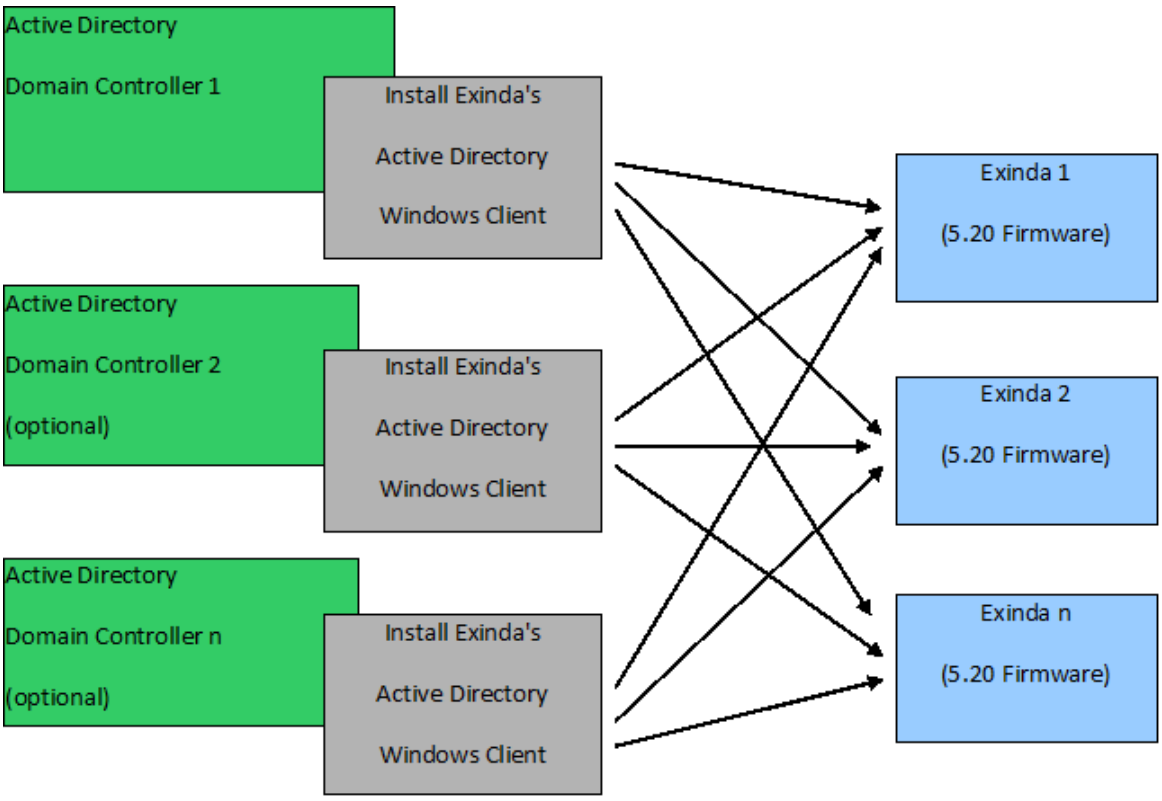


Figure 1: Overview of how multiple AD servers can connect to multiple Exinda appliances using the Exinda AD service.

Part IV

4 Exinda AD Service Installation

Exinda posts new appliance firmware and new versions of the AD service online, at http://www.exinda.com.

Note: You must login to access software downloads from www.exinda.com.

The Exinda AD service needs to be installed onto all Domain Controllers that have AD capabilities. Each AD server can talk to up to 20 Exinda appliances.

4.1 Install the Exinda AD Service on Active Directory Server(s)

After downloading the Exinda AD service installer, double-click the .msi or .exe file to launch the Exinda AD service installation program. During the installation process, you will be asked to enter basic configuration.

- IP address of your Exinda appliance,
- Port number (8015 by default),
- 'admin' password, and
- the maximum age of the log history retrieved from the Security Event Log.

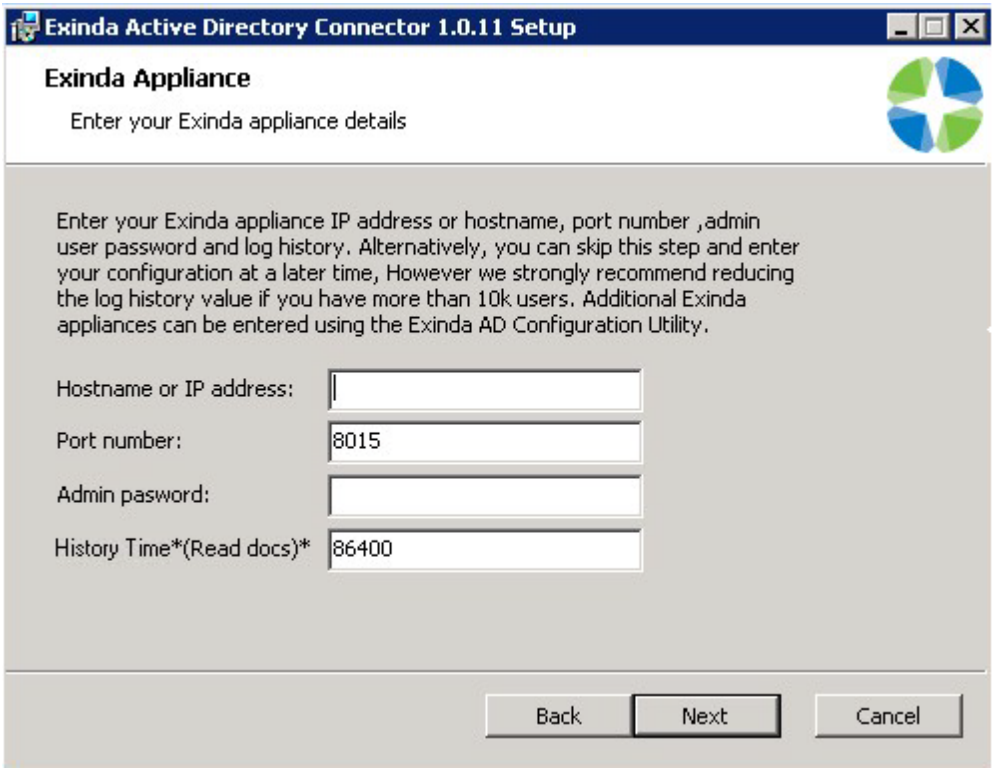


Figure 2: The AD service installer.

Additional Exinda appliances can be added after the installation is finished with the Exinda AD Configuration Utility. After the installation is finished, the Exinda AD service will start automatically and will attempt to communicate with the configured Exinda appliance.

The following problems may be reported during installation:

1. "The installer has detected that WMI Service is not running. Consult Windows Help files to find information on how to start WMI Service."
   This message indicates that Windows Management Information (WMI) service is disabled. The Exinda AD service will not be able run correctly until the WMI service is started.

2. "The installer has detected that Logon Auditing is disabled. Consult Windows Help files to find information on how to enable Logon Auditing."
   Logon Auditing is required to obtain information about user log-ons and log-offs. The installer will offerer you the option to enable Logon Auditing on your behalf. Alternatively, you can run 'Start Menu | Administrative Tools | Local Security Policy' (Windows 2008) or 'Start Menu | Administrative Tools | Domain Security Policy' (Windows 2003), navigate to 'Local Policies | Audit Policy' and enable 'Audit logon events'.

3. "The installer has detected that Active Directory Domain Controller role is disabled. Consult Windows Help files to find information on how to configure your system as a Domain Controller."
   This error message indicates that the Active Directory role is not installed on this machine. The Exinda AD service will not be able run on this machine as it is not an AD server.

Note: On Windows Server 2008 or newer, the installer must be run as Administrator.

4.2 Configure the Exinda AD Service

Once the installation is finished, you can run the Exinda AD Configuration Utility from the Windows Start Menu (All Programs\Exinda Networks\Exinda AD Configuration Utility).

The first tab allows you to change the basic configuration and add or remove Exinda appliances .

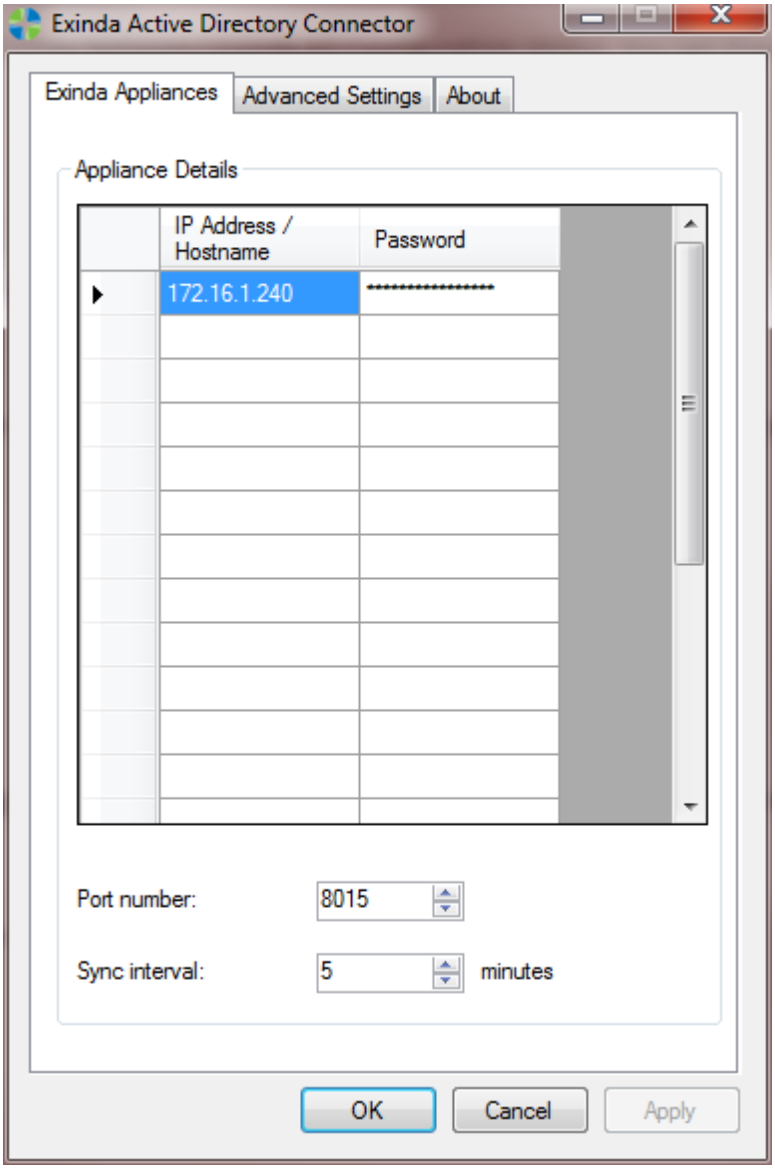


Figure 3: The Exinda AD service configuration utility.

- **Appliance Details**: The list of Exinda appliances that the AD service communicates with. You can delete an appliance, add a new one or change the 'admin' password.

- **Port number**: The default port is 8015. If you need to change the port number, remember to set it to the same value on all Exinda appliances using the Exinda AD service. The port number can be changed on the Exinda appliance by nagivating to the System | Network | Active Directory page on the Web UI - Advanced mode.

- **Sync interval**: The sync interval tells the Exinda AD service how frequently to contact Exinda appliances to synchronize AD user and group information.

The second tab allows you to configure advanced options.

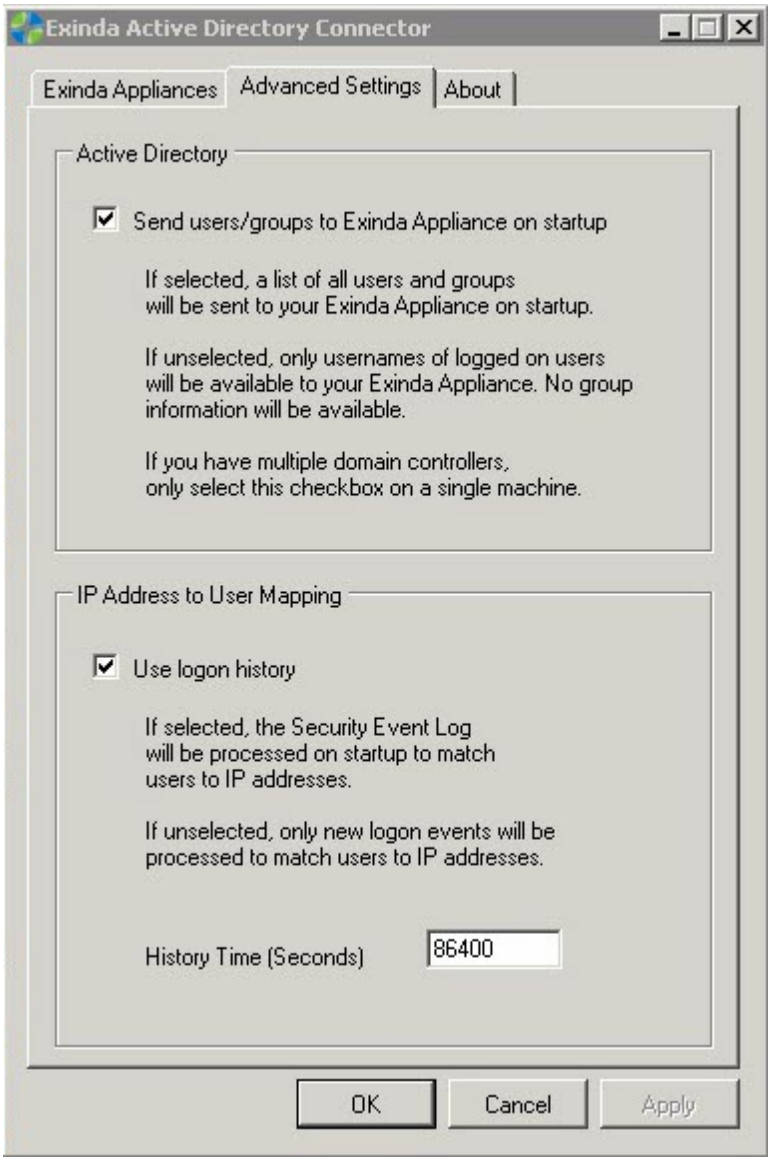


Figure 4: The Exinda AD service configuration utility.

- **Send users/groups to Exinda appliances on startup**: If this option is selected, a list of users and groups will be sent to Exinda appliances on service startup. Otherwise, only logged on users will be available to your Exinda appliances. Information about groups will not be available.

> **Note:** If the Exinda AD service is installed on multiple domain controllers, and those domain controllers share the same AD information (user and group information), then the **Send users/groups to Exinda appliances on startup** option only needs to be enabled on one of the Exinda AD service instances.

- **Use logon history**: If selected, the Security Event Log will be processed on startup in order to obtain information about users already logged in. If unselected, only newly logged-on users will be captured. The **History Time** field identifies the maximum age of the logon history retrieved from the Security Event Log, in seconds. The maximum value is 86400 seconds, or one day.
  The number of users logging in and out of the domain controller per day will affect the performance of the Active Directory client. When this option is selected on a busy server, the history updates can backup on the Exinda as events continue to be added. The transfer of logon history is only started at the initial start-up of the Exinda AD client, after a domain controller restart, or after the Exinda AD client service is restarted. After all the logon history has been sent, the history is not updated until one of the above events occur.

> **Note:** Active Directory environments that have more than 10,000 users and multiple domain controllers, **Use Logon History** must be disabled on all the servers. If **Use Logon History** is enabled, it can result in high memory usage on the appliance.
> If a single domain controller has over 60,000 users logging in and out per day, set the **History Time** value to a low number, for example between 3600 seconds (one hour) and 14400 seconds (4 hours).

4.3 Verify Communications Between AD Server and Exinda Appliance

On the Exinda appliance, navigate to the System | Network | Active Directory page on the Web UI - Advanced mode, and verify that the Exinda AD service is listed there.

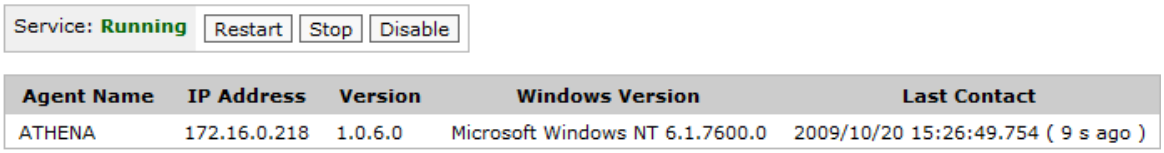


Figure 5: Check the status of connected Exinda AD services on the Exinda appliance.

In case the service is not visible on the list, run the Event Viewer program on your Active Directory server to examine Windows logs. The program is located under Administrative Tools in the Start Menu. You should be able to see “Service started successfully” message form Exinda Networks Active Directory Connector in the “Windows Logs | Application” sub tree. In case something is not working correctly, you will see error messages from the Exinda Networks Active Directory Connector in these logs.

4.4 Verify AD Users in Reports

On the Exinda appliance, navigate to the Monitor | Real Time page on the Web UI - Advanced mode, and ensure user names are showing up as expected. User statistics are also available on the Monitor | Users or Monitor | Network (select Users from the drop down list) reports.

Inbound Conversations					
External IP (User)	Internal IP (User)	Application	Transfer Rate (kbps)	Packet Rate (pps)	Flows
Total			**3251.270**	**395**	**121**
208.111.145.209	172.16.0.218 (john)	HTTP[download.microsoft.com]	2301.550	208	1

Figure 6: Example Real Time report showing AD usernames.

Note: The Exinda appliance relies on user logon events to capture the username. As such, when you first install the AD service, it may take up to 24 hours (or longer) to get all user to IP address mappings as users progressively login.

Part V

5 Using AD Groups and Users in Optimizer Policies

AD users and groups are listed on the Web UI - Advanced mode, under Objects | Users & Groups. On this page, you can create a Dynamic Network Object based on an AD groups or users. These Dynamic Network Objects are then available for for use when configuring Optimizer Policies.

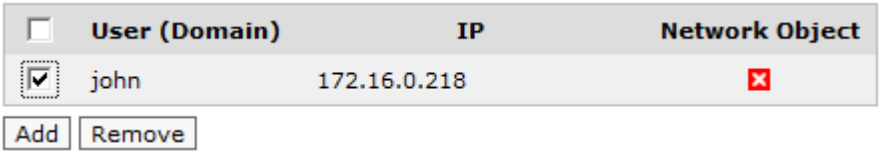


Figure 7: Select the AD user or group to create a dynamic network object, which can then be used in Optimizer Policies.