



LANDesk® Management Suite 8.7 Extended Device Discovery

Revision 1.0

**Roy Meyer
Feb. 7, 2007**

Information in this document is provided in connection with LANDesk Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in terms and conditions for such products, LANDesk Software, Ltd. and its affiliates (collectively, "LANDesk Software") assume no liability whatsoever, and LANDesk Software disclaims any express or implied warranty, relating to sale and/or use of LANDesk Software products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. LANDesk Software products are not intended for use in medical, life saving, or life sustaining applications.

Information regarding third-party products is provided solely for educational purposes. LANDesk Software is not responsible for the performance or support of third-party products and does not make any representations or warranties whatsoever regarding the quality, reliability, functionality or compatibility of these products. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of LANDesk Software.

LANDesk Software retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. LANDesk Software makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Copyright © 2007, LANDesk Software, Ltd. All rights reserved.

LANDesk, Targeted Multicast, Peer Download, and Trusted Access are registered trademarks or trademarks of LANDesk Software, Ltd. or its controlled subsidiaries in the United States and/or other countries.

Avocent is a registered trademark of Avocent Corporation.

*Other brands and names may be claimed as the property of others.

Table of Contents

| | |
|---|----|
| Introduction..... | 4 |
| Assumptions..... | 4 |
| Overview..... | 4 |
| Configuring XDD Settings Window..... | 5 |
| Configuring the ARP discovery history settings..... | 7 |
| Understanding XDD IP address filtering..... | 9 |
| Deploying the XDD Agent..... | 9 |
| Working with devices found through XDD..... | 11 |
| BKM for Configuring and Deploying XDD..... | 12 |
| Troubleshooting XDD..... | 12 |
| FAQ for XDD..... | 13 |

Introduction

Extended Device Discovery (XDD) is a new feature added in LANDesk® Management Suite 8.7 to help discover unmanaged devices on the network. This document is a guide to configuring and deploying the XDD agent.

Assumptions

This document assumes that the reader has a working knowledge of LANDesk® Management Suite 8.7, its functionality, and deployment.

Overview

XDD works outside the normal scan-based discovery methods used by Unmanaged Device Discovery (UDD). Managed devices with the XDD agent on them listen for Address Resolution Protocol (ARP) broadcasts and maintain a cache (both in memory and in a file on the local drive) of devices they discover. Networked devices use ARP to associate a TCP/IP address with a specific device's network hardware MAC address. This communication happens at a very low level and doesn't rely on devices responding to pings or agent communication on specific network ports. Even heavily firewalled devices rely on ARP. Because of this, XDD can help find devices that normal discovery scans can't find. When a new ARP broadcast is recognized by a device with the XDD agent, the XDD agents that hear the ARP wait two minutes for the detected device to boot and each agent waits a random amount of time. The agent with the shortest random wait will ping the new device first, checking for LANDesk agents and then UDP broadcast to the subnet to let the other agents know that it took care of the ping for that device. If multiple XDD agents are installed, this prevents devices from generating excess traffic by all pinging at the same time. The ARP tables stored by the XDD agent timeout after 48 hours by default. Every network device will be pinged once per time out period. Even devices that generate a lot of ARP traffic are only pinged once per timeout period. All discovered devices are reported to the core server. XDD does a CBA8 ping to determine if the LANDesk agent is installed. Devices that respond to the CBA8 ping are not added to UDD even if they are not in the database. Devices that are not already in the LANDesk® Management Suite database and do not have the LANDesk agent installed appear in the **Unmanaged device discovery** window's **Computers** list. ARP-discovered devices show **True** in the **ARP Discovered** column.

The following columns are also populated:

- Device Name
- IP Address
- MAC Address
- First scanned
- Last scanned
- Times scanned

Configuring XDD Settings Window

The Configure XDD settings window configures how the LANDesk XDD agent uses the ARP to discover devices that do not have the agent installed.

Configure XDD settings

These settings configure how the LANDesk agent uses the address resolution protocol (ARP) to discover devices that do not have the agent installed.

Configuration Download Frequency (In seconds)
604800

Duration ARP entry stats cached (in seconds)
86400

Maximum delay before pinging an unknown device for the LANDesk agent (in seconds)
3600

Frequency the cached ARP table is refreshed (in seconds)
300

Logging Level
1 - Errors only Force logging level

Extended device discovery is enabled

Accept Cancel Help

The Configure XDD settings window has the following options:

Note: *These settings are found in the **ARPCFG.XML** file in the **C:\WINDOWS\System32** directory on computers with the XDD agent installed.*

- **Configuration download frequency (in seconds):** How often managed devices with the XDD agent check with the Core Server for an updated XDD configuration. The agent always updates its configuration from the Core Server when it first loads. The default value is one week (604,800 seconds). Setting this too high will cause configuration changes to take a long time to propagate to devices. Setting this too low will cause more load on the Core Server and the network.
- **Duration ARP entry stats cached (in seconds):** How long devices with the XDD agent keep an address in the ARP table. Devices in the ARP cache won't be pinged after the initial discovery ping. The default is 24 hours (86,400 seconds). The minimum value is 900 seconds.
- **Maximum delay before pinging an unknown device for the LANDesk agent (in seconds):** When a new ARP is recognized by a device with the XDD agent, the device waits two minutes for the detected device to boot and then waits a random amount of time within the value specified here. The agent with the shortest random wait will ping first and then UDP broadcast to the subnet that it took care of the ping for that device. If there are multiple XDD agents installed, this prevents devices from generating excess traffic by all pinging at the same time. Setting this too high may cause unmanaged devices to not be discovered because they may leave the network before they can be pinged. Setting this too low could cause multiple agents to ping and report the same device. The default is one hour (3,600 seconds).
- **Frequency the cached ARP table is refreshed (in seconds):** How often the device writes the ARP cache to disk so the data isn't lost in case the device shuts off, crashes, or reboots. The default value is five minutes (300 seconds).
- **Logging level:** The local XDD logging level for errors (1), warnings (2), everything (3). The default level is 1- errors only. Logs are stored locally in C:\Program Files\LANDesk\LDClient\XDDCLIENT.LOG.
- **Force logging level:** Overrides the log level setting from the core server. Clearing this option, allows the log level to be set manually on a particular device. This can be useful for troubleshooting a particular device without having to change the log level on all devices. This is enabled by default.

- **Extended device discovery is enabled:** When cleared, turns off XDD on all devices. The next time an XDD-enabled device checks with the core for an XDD configuration update, this setting takes effect. Even when discovery is disabled, the agent still checks with the core for configuration updates. This is enabled by default.

To configure XDD agent settings:

1. From the Console, click **Tools | Configuration | Unmanaged Device Discovery**.
2. Click the **Configure Extended Device Discovery** toolbar icon.
3. Change any options needed.

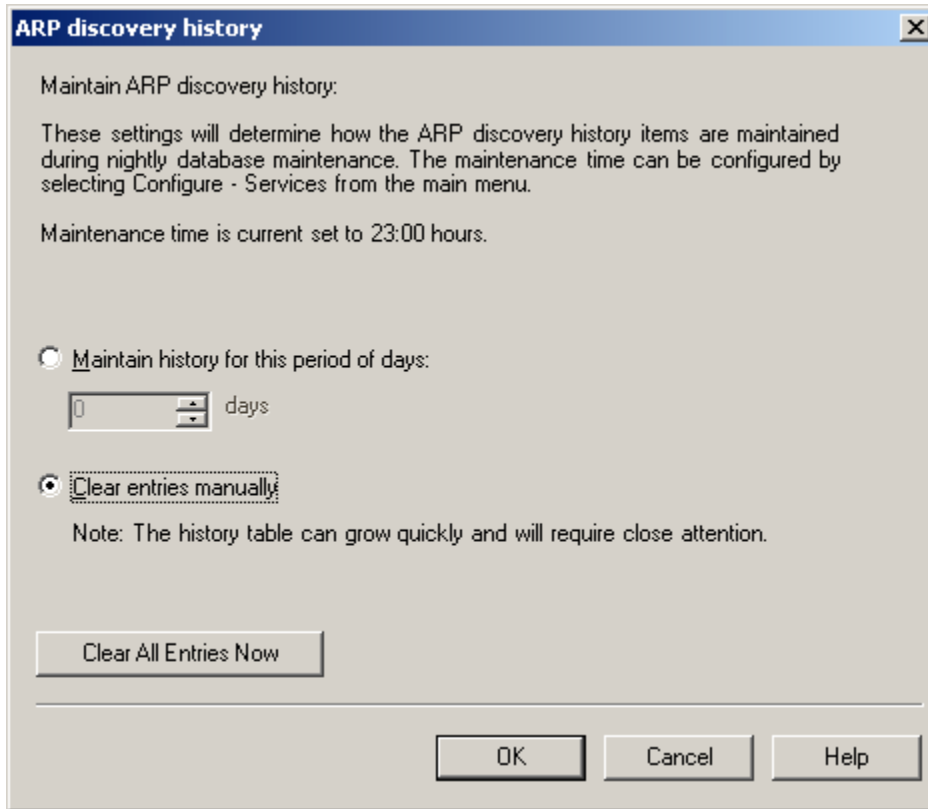
Note: Click **Help** for more information.

4. Click **Accept**.

The next time XDD agents synchronize with the core server, the changes will be applied.

Configuring the ARP discovery history settings

Use the ARP discovery history window to configure how the Core Server maintains the ARP discovery history. This history data is used for generating XDD reports. The options in this window don't affect the discovered devices seen in the main Unmanaged device discovery window. This history only applies to devices that were discovered through ARP discovery and that don't have LANDesk agents installed on them.



The ARP discovery history window has the following options:

- **Maintain history for this period of days:** Specifies how many days of ARP discovery history data are saved in the database. ARP discovery history data older than the number of days specified will be deleted from the database during maintenance.
- **Clear entries manually:** This is the default. The ARP discovery history won't be deleted during maintenance.
- **Clear All Entries Now:** Click to immediately delete the ARP discovery history from the database.

To configure the ARP discovery history:

1. From the Console, click **Tools | Configuration | Unmanaged Device Discovery**.
2. Click the **Configure ARP Discovery History** toolbar icon.
3. Change the options you want.
*Note: Click **Help** for more information.*
4. Click **OK**.

Understanding XDD IP address filtering

It is not recommended to install the XDD agent on notebook computers, since they may connect to other networks that should not be monitored, such as hotel or airport networks. To help prevent discovery of devices that aren't on your network, the Core Server ignores IP addresses where the first and second IP address octets are plus or minus 10 from that of the core server. For example, if the Core Server's IP address is 192.168.20.17, XDD on the Core Server will ignore addresses above 203.179.0.0 and addresses below 181.157.0.0. This feature can be disabled by adding the following DWORD registry key to the core server and setting its value to 0:

- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\Filter

Set the Filter value to 1 to enable filtering again.

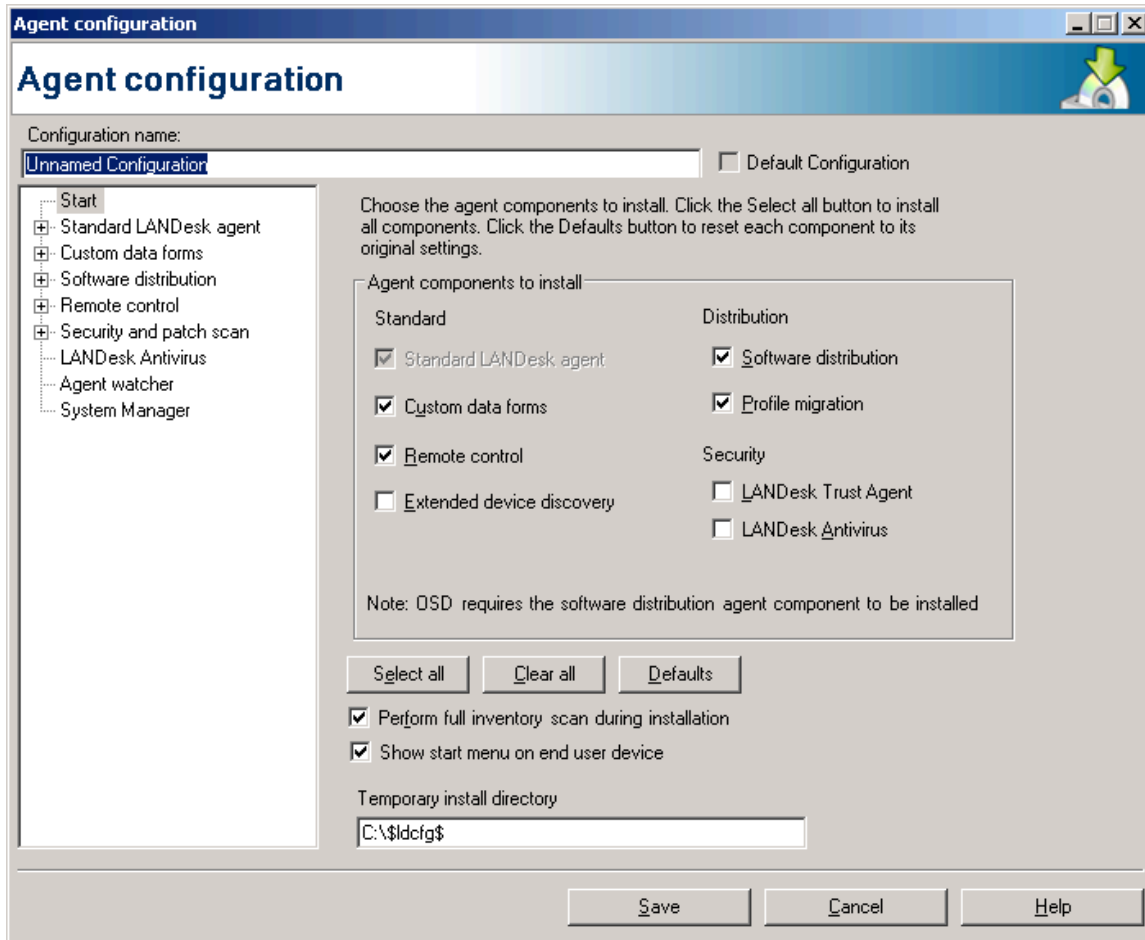
The first and second octet monitoring ranges can be adjusted by adding the following DWORD registry keys to the Core Server and setting their values to the numeric range to be monitored (the default is 10 for the first and second octets):

- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\FilterThreshold1
- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\FilterThreshold2

FilterThreshold1 contains the range for the first octet and **FilterThreshold2** contains the range for the second octet.

Deploying the XDD Agent

The XDD agent can be deployed to every managed device, although it is not necessary and not recommended. Deploying the agent to several devices on each subnet should be sufficient to discover unmanaged nodes on the subnet.



To deploy the XDD agent:

1. From the Console, click **Tools | Configuration | Agent configuration**.
The Agent Configuration window appears.
2. Click the **New** toolbar icon.
3. Type a **Configuration name** in the Configuration name field.
4. From the Agent configuration window's **Start** page, select the agents to be deployed.
5. Click to place a checkmark in the **Extended device discovery** checkbox.
Note: *The Agent configuration dialog doesn't have any other options relating to XDD.*
6. Use the tree to navigate the windows relating to the options selected.
Note: *Click Help for more information about any of the options.*
7. Click **Save**.
8. Click **Close**.

9. Deploy the agent configuration to several devices on each subnet.

There are various XDD settings that can be configured for the agent. This agent periodically synchronizes its settings with the Core Server. The client machine does not need a new agent to get this new XDD configuration. It requests it through the **ldlogon** web share. This can be seen in the **ProxyHost.log** file. The client machine makes a request for the **ARPCFG.XML** file, and updates its settings. This occurs automatically over time and is controlled by the **Configuration Download Frequency** setting. It will download the **ARPCFG.XML** configuration with a restart of the XDD Service on the client machine.

Working with devices found through XDD

When an XDD client needs to send data to the Core Server, it sends **XDDFILES.XDD** to the Core Server using the **POSTCGI.EXE** web service on the Core Server. This file is sent to the **C:\Program Files\LANDesk\ManagementSuite\XDDFILES** directory on the Core Server. The file is processed by **XDDFILES2DB.EXE** which is in the **C:\Program Files\LANDesk\ManagementSuite** directory. Devices found through XDD appear in the **Unmanaged device discovery** window's **Computers** list. From there normal UDD options can be performed, such as moving them to other groups. Also, XDD exceptions can be imported and exported. An exception is a device on the network that isn't manageable or that the administrator knows about but doesn't want XDD to report on. These exceptions are in a text **.CSV** file format that consists of comma-separated IP and MAC addresses, in that order, one pair per line. The exceptions export includes all exceptions stored in the database. The exceptions import replaces all exceptions stored in the database with the exceptions included in the import file.

To export all XDD exceptions:

1. From the Console, click **Tools | Configuration | Unmanaged Device Discovery**.
2. Click the **Export Extended Device Discovery Exceptions to CSV File** toolbar icon.
3. Browse to a **folder** and type a **file name** in the **File name** field.
4. Click **Save**.

To import all XDD exceptions

1. Create or update a comma-separated CSV file that contains the exceptions you want.
2. From the Console, click **Tools | Configuration | Unmanaged Device Discovery**.
3. Click the **Import Extended Device Discovery Exceptions from CSV File** toolbar icon.

4. Click to highlight the file and click **Open**.

BKM for Configuring and Deploying XDD

1. Set the desired XDD configuration settings.
2. Set the desired ARP discovery history settings.
3. Create an Agent Configuration which includes the XDD agent.
4. Deploy the XDD Agent to a couple of computers on each subnet.
Note: Do not install the XDD agent on laptops.
5. Wait for detected devices to show up under Computers in UDD.

Troubleshooting XDD

The current configuration for the XDD agent can be found in the **ARPCFG.XML** file located in the **C:\WINDOWS\System32** directory on computers that have the XDD agent installed.

Computers discovered by the XDD agent are stored on the computer in the **HOSTCACHE.XML** file in the **C:\WINDOWS\System32** directory.

Computers discovered by XDD are located in the **UNMANAGEDNODES** table in the database. Running the following SQL statement will return all computers that were discovered by XDD:

```
SELECT * from UNMANAGEDNODES where ARPDISCOVERED = 1
```

Computers discovered by XDD also show up in the UDD window under **COMPUTERS** and the column **ARP DISCOVERED** is **TRUE**.

Set the **LOGGING LEVEL** to “**3 - Debug**” for the XDD agent and check the log file **XDDCLIENT.LOG** for any useful information which is created in the **LDCLIENT** directory.

On the Core Server in the **C:\Program Files\LANdesk\ManagementSuite** directory, check the **XDDFILES2DB.LOG** file which is only created if any errors occur.

FAQ for XDD

1. Why doesn't a device show up in UDD that should have been discovered by XDD?

There are 3 common reasons why this may happen:

- a. The computer has the LANDesk® Management Suite agent installed.

Computers that have the LANDesk Management Suite agent installed and responded to the CBA8 ping from the XDD agent, will not show up in UDD.

- b. Devices outside the Core Servers IP address range will not show up.

Refer to the section titled "Understanding XDD IP address filtering" for more information on how to adjust the range of IP addresses that will be accepted.

- c. The device is already in the LANDesk Management Suite database.

2. How long does it take for devices to be discovered by XDD?

Only devices that send out ARP traffic will get discovered. Once a device ARPs, it will be sent to the Core Server within 1 hour by default. This time can be adjusted by changing the **Maximum delay before pinging an unknown device for the LANDesk agent**. Refer to the section titled "Configuring XDD Agent settings" for how to change this option.