LANrev
Optimization Guide

HEAT software

www.heatsoftware.com

LANrev Optimization Guide version 6.7 – Document release 3

Contents

Chapter 1   *About this guide*

The LANrev suite of applications is a client management solution for managing all of your Windows and macOS computers (traditional laptops and desktops), as well as Android, iOS, and Windows Phone mobile devices, from a single, unified administration application (admin). You can mix and match LANrev components, including the server and admin. For example, you can install LANrev on a macOS or Windows platforms, and manage traditional and mobile devices from either platform.

This guide outlines some basic strategies for configuring LANrev to implement the built-in, fail-safe features to your maximum advantage for your everyday operation and when you need to recover from a catastrophic failure.

This guide provides instructions for backing up your servers, including those hosting the Admin application and the Agents. This guide provides you with a method to use LANrev to its best advantage in your organization.

Following the guidance provided in this guide also simplifies and expedites your disaster recovery response. Using LANrev's features provides you with the quickest way to resolve a catastrophic failure of your equipment, which is described in the *LANrev Disaster Recovery Guide*.

NOTE All instructions in this guide apply to a LANrev server running on Windows 2008 Server or above, or on or macOS.

This chapter includes information on the following topics:
- Audience
- Using this guide
- Conventions used in this guide
- Contacting support

Audience

This guide provides instructions for advanced users of LANrev who are designated to implement their organizations' use of LANrev to its fullest advantage. This guide presumes that advanced users have a high level of familiarity with LANrev.

If you do not have a technical resource that fulfills this requirement, you may want to consider engaging HEAT Professional Services to have a technical consultant assist you by sending an e-mail message to lanrev.services@heatsoftware.com.

Using this guide

The LANrev Optimization Guide contains the following chapters:
- Chapter 1: "About this guide" on page 5 (this chapter) provides an overview about this document.
- Chapter 2: "Understanding LANrev System recommendations" on page 7 provides information about the minimum system requirements and what to do when you reach certain thresholds in your managed device population.

- provides specific tasks that help you optimize your LANrev system.
- provides information about how to set up database maintenance checks and backups.
- The Glossary provides definitions for specific terms used in this guide.

Conventions used in this guide

The following conventions are used throughout this guide:

- Directory names, file names, field names, and UI objects are represented using bold; for example:
  - The **notepad.exe** executable file is located in the **windows\system32** directory.
  - **UserID** – enter your user identification number in this field.
  - Click **Apply**.
- When using checkboxes:
  - Click an empty checkbox to activate it.
  - Click an activated checkbox to clear it (ensure there is nothing in the checkbox), which deactivates it.
- Cross references to other locations within this user guide are indicated in green text with an underscore; for example: see Conventions used in this guide. Clicking a cross reference takes you to that location in the guide.
- References to other locations in the guide are expressed in one of following possible ways:
  - For more information, see – indicates that there is information that provides more context on this topic.
  - See – indicates there is more information, but it's not required to understand what is presented here.
  - See the task – indicates where to find specific instructions.
- References to other documents are shown in italic text and the heading is surrounded by quotation marks, as follows:

  For more information, see the *LANrev User Guide*, under the heading "Initial configuration of LANrev Server".

Contacting support

If you have difficulty using LANrev or installing the Agent, contact HEAT support at http://www.heatsoftware.com/support. We welcome your questions, comments, and feature requests.

Chapter 2   *Understanding LANrev System recommendations*

The LANrev client management system is highly configurable and you can customize it to installations of any size. The default configuration is best suited for a site of less than 1,000 clients. If your LANrev installation is larger than this size, we suggest that you adjust your server and Agent configurations to those suggested in Table 1 on page 10.

The recommendations in this guide are meant as the first step in helping you fine-tune LANrev for optimal performance in your network. The information provided is meant to help maximize server performance, while maintaining the highest level of stability. You may find that you need to adjust some of these settings from the recommended values to take into account the various contrasting factors in your organization's network and computer environments.

You can adjust many of the noted configurable Agent settings with the **Agent Settings** command or you can preconfigure these settings in the LANrev Agent installer itself. You must make the server configuration changes directly to the LANrev server preferences or settings in either the LANrev server **com.polepositionsw. lanrev_server.plist** preferences file or the **LANrev Server registry key**.

This chapter includes the following information:
- Minimum system requirements
- Splitting the LANrev server functionality
- Hardware recommendations when reaching server thresholds for your managed device population
- Setting up a split DNS
- Network bandwidth use

Minimum system requirements

For the system requirements for the desktop and mobile device software components required for LANrev, which is installed in a Windows or macOS server environment, see the *LANrev User Guide*, under the heading "System requirements". Managed devices include traditional macOS and Windows desktop or laptop computers and mobile devices, which include iOS, Android, and Windows Phone.

You can mix Windows and macOS components between the platforms. For example, you could configure an Admin application running on Windows that can control a server running on macOS to work with Agents running on Windows clients. For more information, read the *LANrev User Guide*, "Choosing a computer for LANrev Server" section.

Fast disk input and output (I/O) is critical to server performance. Therefore, carefully evaluate the performance requirements before implementing LANrev or mobile device management as a production system "in the cloud". Default server configurations from companies such as Amazon (EC2) and Microsoft (Azure) are usually sufficient for managing a low number of endpoints (less than a thousand), but for more endpoints than that, we recommend fast disks into the cloud solutions. We highly recommend using SSD drives and RAID controllers with at least 256 MB of battery-backed, write-back cache.

All LANrev components require a working IP network connection. The built-in firewalls for macOS and Windows are fully supported.

I/O on the Admin workstation is also important, but not as much as it is on the server. The recommended processor for the workstation on which the Admin application is installed depends on how many clients are managed. For a client population of 10,000, we recommend a system with a 2.6 GHz Intel Core 2 Duo processor and 4 GB RAM. For more information, see Table 1 on page 10.

Splitting the LANrev server functionality

LANrev Server can fulfill four distinct functions:
- Managing inventory
- Executing commands on managed devices
- Distributing software
- Monitoring software licenses

LANrev can receive inventory data from desktop devices and mobile devices. In general, inventory data coming from desktop devices can be more substantial than that coming from mobile devices, because there is more potential datapoints that can be collected from desktop devices currently. This means that collecting installed software data, printer, font, process, and service data from desktops is possible. The total amount of inventory collected has a huge impact on the functionality of the server and needs to be considered when configuring a multi-server solution.

In this section of the guide, recommendations are made in Table 1 on page 10 regarding total client count (desktop devices plus mobile devices). That being said, at a certain point, it may be feasible to separate the inventory data received by desktop devices and that of mobile devices into two separate inventory servers.

For installations managing 3,000–5,000 clients (desktop and mobile combined), we recommend you deploy two LANrev servers, one to handle running commands and managing inventory and another one to handle distributing software and monitoring licenses. If you are collecting a heavy load of inventory data (installed software, fonts, printer info, process info, startup info, missing OS patch info), it is especially important to configure a dedicated server to handle this additional data that is collected. If collecting installed software data, the recommended splitting point for a two-server implementation would be 2,000 total clients.

For installations over 10,000 clients, you may want to consider adding a third server to handle just the license monitoring, while the second server handles software distribution. For more information about reaching various hardware thresholds and what to do to keep LANrev working optimally, see Table 1 on page 10.

Hardware recommendations when reaching server thresholds for your managed device population

When your organization reaches certain thresholds for the number of managed devices hosted on servers, you need to migrate various systems and servers to new additional hardware. The term "endpoints" is used to describe the total of both desktop devices and mobile devices that are hosted on the LANrev servers.

This section provides information on the following topics:
- Disk space use
- Distribution point recommendations

Table 1 provides general hardware recommendations and disk storage requirements guidelines for suggested thresholds based on the total number of traditional computer and mobile device endpoints hosted, which can change depending on how heavily you use various LANrev features.

IMPORTANT   Although Table 1 presents information for threshold ranges for both types of hosted clients (desktop devices and mobile devices), make sure that you use the total of both types of devices when you determine the recommended hardware thresholds. For example, if you want to host 1,000 desktop devices and 1,750 mobile devices, look at the information for 2,750 devices on each table and go with the maximum recommendations.

For example, to implement a population of 2000 desktop clients (from which you are collecting full inventory) and 1000 mobile devices, you may want to split the inventory sources so the mobile devices talk to their own database inventory server to offload the potential load coming from the desktop clients.

Table 1. Recommended hardware thresholds for optimum LANrev functionality

Total number of (desktop and mobile) endpoints	Hardware recommendations for servers		MDM server	Hardware recommendations for LANrev Admin	Number of distribution points[a]	Server database – approximate disk space required to store inventory data[b]	
	LANrev Server		**MDM server**				
	Processor, memory, disk	Suggested number of servers [c]	Processor, memory, disk			Main database	Total space (with 7 backups)[d]
0–1000	2 Xeon, 2.6 GHz# 2 GB RAM	**1** # Full desktop/mobile inventory, SD, and LM	2 Xeon, 2.6 GHz# 2 GB RAM	Core 2 Duo, 2.6 GHz# 2 GB RAM	**1** at least;# recommend **2** for redundancy	**300 MB** for full inventory;# **150 MB** for standard inventory	**2.4 GB**
1001–2500	2 Xeon, 2.6 GHz# 2 GB RAM	**2** # 1 full desktop/mobile inventory# 1 SD/LM (collects basic inventory only)	2 Xeon, 2.6 GHz# 2 GB RAM	Core 2 Duo, 2.6 GHz# 2 GB RAM	**2**	**500 MB** for full inventory;# **250 MB** for standard inventory	**4 GB**
2501–5000	2 Xeon, 2.6 GHz# 4 GB RAM# RAID array, 256MB WBC	**3** # 1 full desktop inventory# 1mobile device inventory,# 1 SD/LM[e] (collects basic inventory)	2 Xeon, 2.6 GHz# 2 GB RAM	Core 2 Duo, 2.6 GHz# 2 GB RAM	**5**	**1 GB** for full inventory;# **500 MB** for standard inventory	**8 GB**
5001–10000	2 Xeon, 2.6 GHz# 4 GB RAM# RAID array, 256MB WBC	**4** # 1 full desktop inventory# 1mobile device inventory# 1 SD (collects basic inventory only)# 1 LM[e] (collects basic inventory only)	2 Xeon, 2.6 GHz# 2 GB RAM	Core 2 Duo, 2.6 GHz# 4 GB RAM	**10**	**1.5 GB** for full inventory;# **750 MB** for standard inventory	**12 GB**

Table 1. Recommended hardware thresholds for optimum LANrev functionality

Total number of (desktop and mobile) endpoints	Hardware recommendations for servers		MDM server	Hardware recommendations for LANrev Admin	Number of distribution points[a]	Server database – approximate disk space required to store inventory data[b]	
	LANrev Server						
	Processor, memory, disk	Suggested number of servers [c]	Processor, memory, disk			Main database	Total space (with 7 backups)[d]
10001–20000	2 Xeon, 2.6 GHz# 4 GB RAM# RAID array, 256MB WBC	**4** # 1 full desktop inventory# 1mobile device inventory# 1 SD (collects basic inventory only)# 1 LM (collects basic inventory only)	2 Xeon, 2.6 GHz# 4 GB RAM	Core 2 Duo, 2.6 GHz# 4 GB RAM	**20**	**3 GB** for full inventory;# **1.5 GB** for standard inventory	**24 GB**
20001–30000	Xeon Quad Core, 3 GHz# 6 GB RAM# RAID array, 512MB WBC	**4** # 1 full desktop inventory# 1mobile device inventory# 1 SD (collects basic inventory only)# 1 LM (collects basic inventory only)	2 Xeon, 2.6 GHz# 4 GB RAM	Core 2 Duo, 2.6 GHz# 6 GB RAM	**30**	**3.5 GB** for full inventory;# **1.75 GB** for standard inventory	**48 GB**
30001–40000	Xeon Quad Core, 3 GHz# 8 GB RAM# RAID array, 512MB WBC	**4** # 1 standard desktop inventory# 1mobile device inventory# 1 SD (collects basic inventory only)# 1 LM (collects basic inventory only)	2 Xeon, 2.6 GHz# 4 GB RAM	Core 2 Quad, 3 GHz# 6 GB RAM	**40**	**2.5 GB** for standard inventory	**20 GB**
40001–50000	2 Xeon Quad Core, 3 GHz# 8 GB RAM# RAID array, 512MB WBC	**4** # 1 standard desktop inventory# 1mobile device inventory# 1 SD (collects basic inventory only)# 1 LM (collects basic inventory only)	2 Xeon, 2.6 GHz# 4 GB RAM	Core 2 Quad, 3 GHz# 8 GB RAM	**50**	**3 GB** for standard inventory	**24 GB**
50001+	4 Xeon Quad Core, 3 GHz# 16 GB RAM# RAID array, 1GB WBC	**4** # 1 standard desktop inventory# 1mobile device inventory# 1 SD (collects basic inventory only)# 1 LM (collects basic inventory only)	2 Xeon, 2.6 GHz# 4 GB RAM	Core 2 Quad, 3 GHz# 8 GB RAM	**60 or more**	**4 GB** for standard inventory	**32 GB**

a. Assumes a 100 Mbit/s network connection. Faster network connections require fewer distribution points. For more information, see "Distribution point recommendations" on page 13.

b. These numbers are typical values. The space required by the database depends on the devices managed and the features used. For example, custom fields with a lot of data, wallpaper assignments for mobile devices, or an unpurged command history can increase these requirements. We recommend that you set up the server to allow for larger database sizes.

c. In addition to the listed servers, we recommend setting up an additional server as the master distribution point. That server does not necessarily need to meet the main servers' hardware specification. (Although using the same type of computer for this server may make managing and swapping servers easier.)

d. The listed space requirements do not include space for user-uploaded content such as installation packages, patches, or downloadable media. The size of this content varies too widely; you need to evaluate how much additional space these data will require in your system.

e. If you are only collecting standard inventory, which is basic inventory and custom fields with no additional inventory items collected, you can use a single inventory server to store inventory data for both your desktop and mobile device population. Full inventory includes selecting standard inventory and any options you selected when you first installed.

Table 1 uses these abbreviations (in addition to industry-standard terms, such as GHz):

- LM: license monitoring
- N/R: not recommended
- SD: software distribution
- VM: virtual machine

Disk space use

The average amount of disk space required to store inventory data for a single client is about 300 KB to 1 MB. This space includes all inventory data including optional information such as installed software, missing OS patches, fonts, processes, startup items, and printers. This estimate does not, however, include computer tracking information such as screenshots. Screenshots typically start with sizes of around 48 KB (for 800 by 600 pixels) and go up depending on desktop resolution and picture content.

For 10,000 clients, your LANrev server database without computer tracking data would average around 3 GB in size. For 1,000 clients, your LANrev server database without computer tracking data would average about 300 MB in size. LANrev's automated database backup allows you to keep as many backup copies of your LANrev database as you want for disaster recovery. In general we recommend you keep at least seven copies and use a three-day backup interval.

The LANrev server also maintains a commands database that stores a complete history of all remote management and configuration commands issued to Agents. A single entry consumes about 3.3 KB of space. If you do not keep entries older than 30 days, the space consumed by the commands database should be negligible. For more information, see "Purging the command history" on page 28.

With the preceding information in mind, see Table 1 on page 10, which shows the recommended disk space sizes for storing static and live inventory databases. You can also change the path to where LANrev stores the current active database and backup sets (**DatabaseBackupDirectory**) independent of each other. For more information, see "Backing up the database to a different location" on page 16.

Distribution point recommendations

Distribution points are Agent computers that are designated to host software packages for the purposes of software distribution, image deployment and patch management. These distribution point computers should have sufficiently fast hard disks and at least a 100 Mbit network connection for serving packages during software deployments.

The distribution point configuration should support 10 concurrent client computer requests per 1 Mbit of available network connection. The concurrency of client computer check-ins will be highly determined by the frequency of software distribution check-in settings (which are user-definable), the applicability of new software packages, and the percentages of devices that are on at a specific time. Given the somewhat random nature of client machine check-ins (based on different startup times, different patch and package applicability, package size, end so on), high levels of concurrency are atypical. Concurrency can be monitored in the Server Center window of LANrev Admin.

When setting up distribution points, note that LANrev Agent supports a maximum of about 1300 concurrent connections. Therefore, if you have a large client population with a potentially large number of simultaneous connections to a distribution point, you should consider adding additional distribution points to reduce the possibility of overloading the distribution point computers. Additionally, adding distribution points at locations with significant numbers of endpoints can greatly reduce bandwidth needs across WAN links with low bandwidth availability.

The recommended number of distribution points can vary widely based the factors discussed above. The best practice is to start small, analyze performance and concurrency levels in your environment, and adjust the number of distribution points accordingly. Distribution points only require an agent license, and are easy both to add and to remove.

Setting up a split DNS

LANrev lets you manage endpoints that are located outside of your internal LAN (behind a firewall or remote NAT). To do this, you need to configure your inventory server address to be resolved both internally and externally. When this is done, agents can communicate with the server when outside of the internal network on the interval that is defined by the heartbeat. In order for this to work, you must still port forward port 3971 to the internal IP address of your LANrev server.

For the purposes of patch management and software distribution, when you set up a distribution point to be used with your Software Distribution server, it is required that at least one distribution point is made accessible over the network (in a DMZ or by forwarding port 3970 to an internal IP).

We also recommend that you assign a separate DNS name to each server role (inventory server, software distribution, license management, master distribution point), even if they all resolve to the same server initially. This way, any future expansion that involves splitting the roles among servers will require only a minor DNS change instead of widespread agent reconfiguration.

Network bandwidth use

Usually there is minimal traffic from LANrev, with the exception of when you are deploying software. Most of that traffic is in the form of bandwidth used for the purpose of sending software packages to Agent computers. You can significantly reduce the amount of WAN bandwidth used by configuring your distribution points to be located in the same geographical location as the populations of your Agents.

For example, if you have four geographically separate locations with Agents that are downloading software patch packages, this activity can consume a large amount of WAN bandwidth, as each

Agent has to download the same patch over WAN. A much better solution is to place mirrored distribution points at each of your remote sites. With this type of configuration, an Agent would only have to download a new patch once. After that point, the Agent uploads the patch package to the master distribution point, which is then mirrored to all of the remote distribution points. By using either smart computer distribution groups or IP address range restrictions, you can successfully ensure that Agents pull down patch packages from the appropriate local distribution point only.

From there the Agents at that site download the packages from that local distribution point computer. You can also control the bandwidth for software distribution on the distribution point and restrict the number of connections it accepts. You can also restrict the replication of software packages and payloads between distribution points to a particular time window.

IMPORTANT   The first time a mirror takes place, it must successfully complete a full mirroring process. So, if you have a very small mirroring window defined, the mirroring process continues outside of the time window specified to ensure that all data was copied successfully. Successive delta mirrors adhere to the time window as long as the full copy of data can be achieved.

In terms of the amount of traffic used for the automatic OS and hardware inventory that comes in every 12 hours by default, it's normally less than 10 KB per computer for the initial full inventory. Subsequent delta inventories after that are typically less than 2 KB per computer. This delta inventory estimate excludes optional items, such as installed software, missing OS patches, fonts, processes, startup items, and printers. Normally these must be requested manually unless you preconfigure LANrev Agent to send them in automatically with the hardware and OS inventory every 12 hours.

The LANrev Agent heartbeat, which comes in every 15 minutes by default, is less than 1 KB per computer and only contains a few pieces of information, such as the Agent's GUID, serial number, IP address, MAC hardware address, name of the current logged-in user, and other miscellaneous pieces of information.

In larger environments, we recommend that you change these intervals to better fit your network and installation size. For more information, please see "Optimizing agent settings" on page 17.

Chapter 3   *Setting up an optimized LANrev system*

There are numerous ways to set up an optimized LANrev system, which includes the LANrev server and all of its components, and the MDM server and all of its components.

For example, replacing or switching out a LANrev server when the hardware fails is much easier when you assign a DNS name to your LANrev server and point Agents to the servers using this DNS name instead of its IP address.

Otherwise, when you move or replace LANrev server and assign it a new IP address, you need to point all of your Agents to the new IP address for the LANrev server using the **Set Inventory Server** command in the Agent Deployment Center.

This chapter provides information on the following topics that help you configure an optimized system:

- Considering various ways of optimizing your system
- Optimizing your LANrev installation
- Optimizing mobile device management server settings

Considering various ways of optimizing your system

This section provides the following topics for your consideration when looking at ways to optimize your LANrev system and its components:

- Assigning a DNS name to your LANrev servers and distribution points
- Setting up separate servers for inventory and software distribution
- Configuring two distribution points for load-balancing
- Backing up the database to a different location

Assigning a DNS name to your LANrev servers and distribution points

When you assign a DNS name to the LANrev servers and distribution points, you only need to change its entry on your DNS server to point the Agents again to the new IP address. This method lets you get up and running much quicker than having to again point all of your Agents to the new IP address for your LANrev server. For more information, see the *LANrev User Guide*, "Initial configuration of LANrev Server".

Using a DNS name also lets you seamlessly replace or move your LANrev servers to a different IP address without any repercussions. This practice minimizes the downtime for LANrev and guarantees maximum availability to your IT personnel.

Setting up separate servers for inventory and software distribution

In most circumstances, organizations with over 3,000 clients should consider setting up two LANrev servers – one to handle inventory and task implementation, and another to handle software distribution and license monitoring. As an organization's managed device population grows and based on the type of inventory data getting collected, thresholds are reached that require updates to your system. For more information about these thresholds, see Table 1 on page 10.

Configure all of your agents to call with their inventories to both servers or multiple inventory servers, as appropriate. (For more information, see the *LANrev User Guide*, "Assigning inventory servers to agents".) Therefore, when one of the servers fails for any reason, you still have a copy of the data on the second server. Also, you can continue to issue remote management commands to the Agents from this second server.

In addition to this, agents call in with updated inventory data at regular intervals so if you replace the failed server, the inventory data is rebuilt automatically on the replacement server over time without any intervention.

This situation does not apply to optional Agent information, such as font, printer, installed software, and process information. However, you can configure the Agent to call in with this information automatically or you can enforce the Agent settings globally, in which case the information is called in to all inventory servers. For more information, see the *LANrev User Guide*, "Gathering and updating information manually".

Configuring two distribution points for load-balancing

You can configure multiple distribution points for software distribution. LANrev will load-balance between them during a software distribution. In this way, if one server goes down, you can quickly replace it with another and have your software payloads replicate again.

As a best practice we recommend that you configure at least two distribution points – one master and one secondary mirror distribution point. This method ensures that there is always a backup copy of your software payloads, which lets you continue distributing software even when one of the distribution points is lost.

For more information, see the following headings in the *LANrev User Guide*:
- "Updating distribution points"
- "Specifying the distribution point in the Software Distribution Center"

Backing up the database to a different location

To optimize the efficiency of your database backups, we recommend that you back up to a network location or to an external hard drive or USB stick, and that you change the path to another location on another physical or network drive that is backed up on a regular basis to provide some extra redundancy. The point is to store your backup databases on a different drive than the one that hosts your live databases. If that hard disk fails for any reason, all of your database backups are fine.

For instructions about changing the database backup location, see "Changing the database backup location" on page 38.

Optimizing your LANrev installation

Many settings on the server, Admin application, and Agent computers can be fine-tuned to maximize performance in your particular environment.

Some of these settings are exposed in the Admin application user interface, whereas others must be applied directly to the Admin or Server preferences. Table 2 provides a list of the locations of the Admin and Server preferences for those settings that have no user interface and must be applied directly.

Table 2. Locations of the Admin and Server preferences for settings with no user interface

LANrev component	Mac	Windows
Admin application	~/Library/Preferences/ com.polepositionsw.lanrev_admin.plist	HKCU\Software\Pole Position Software\LANrev Admin
Server	/Library/Preferences/ com.polepositionsw.lanrev_server.plist	HKLM\Software\Pole Position Software\LANrev Server

For Windows regedit settings, when you make numeric value settings as instructed throughout this chapter, use **Decimal** as the **Base** option, which is shown here.
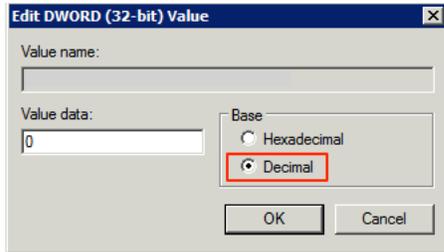
IMPORTANT   It's extremely important that you use the **Decimal** option when specifying numeric registry entries.

This section provides information on the following topics:

- Optimizing agent settings
- Optimizing LANrev Admin settings
- Optimizing server role settings
- Purging the command history
- Implementing agent preference settings globally

Optimizing agent settings

The most obvious settings you can optimize are the Agent heartbeat, automatic inventory, and package and license check intervals for managed desktop devices. You can preconfigure these settings in the Agent and change them later using the Admin application.

Table 3 also shows additional settings (Agent License Monitoring Disk Scans and License Monitoring Process Reports) that are set on the **License Monitoring** tab, not the **Agent Settings** tab.

Table 3. Recommended Agent interval settings for managed desktop devices

Number of managed desktop devices	Heartbeat (minutes)	Inventory (minutes)	Software distribution package checks (minutes)	License monitoring		
				Checks (minutes)	Agent disk scans	Process reports
Default	15	720	60	60	Mon-Fri# 9–6, 12 hrs	Mon-Fri# 9–6, 3 hrs
1,000	15	720	180	480	Mon, Wed, Fri# 9–6, 12 hrs	Mon, Wed, Fri# 9–6, 6 hrs
2,500	30	720	360	960	Mon, Wed, Fri# 9–6, 12 hrs	Mon, Wed, Fri# 9–6, 8 hrs
5,000	60	1440	720	2160	Tue, Thurs# 9–6, 24 hrs	Tue, Thurs# 9–6, 12 hrs
10,000	120	1440	1440	4320	Tue, Thurs# 9–6, 24 hrs	Tue, Thurs# 9–6, 24 hrs
20,000	180	2880	1440	4320	Tue, Thurs# 9–6, 48 hrs	Tue, Thurs# 9–6, 24 hrs
30,000	270	2880	2160	5760	Tue, Thurs# 9–6, 48 hrs	Tue, Thurs# 9–6, 48 hrs
40,000	360	4320	2160	5760	Tue, Thurs# 9–6, 72 hrs	Tue, Thurs# 9–6, 48 hrs
50,000	480	4320	2880	7200	Tue, Thurs# 9–6, 72 hrs	Tue, Thurs# 9–6, 72 hrs
80,000	720	5760	3600	7200	Tue, Thurs# 9–6, 96 hrs	Tue, Thurs# 9–6, 96 hrs

Optimizing LANrev Admin settings

You can fine-tune many settings on the LANrev server, Admin application, and Agent computers to maximize performance in your particular environment. Some of these settings are exposed in the Admin application's user interface, whereas you must apply others directly to the server or Admin preferences. Table 2 on page 17 provides a list of the locations for the Admin and server preferences for those settings with no user interface, which you need to apply directly.

Table 4 shows the settings you can change to optimize the Admin application's performance. All settings provided in the following table are Boolean values for the macOS platform, and DWORD values for the Windows platforms. Making the following suggested settings optimizes the performance of your Admin applications.

Table 4. Changing the LANrev Admin default settings to optimize performance

plist setting or registry key	macOS platform		Windows platforms		Description
	Default Settings	Suggested Settings	Default Settings	Suggested Settings	
AllowMultipleInstances	n/a	n/a	DWORD: 0	DWORD: 1	Allows multiple instances of LANrev Admin to run simultaneously, which lets you connect to multiple servers from the same admin workstation.
AllowTabsInServerCenter	Boolean: False	Boolean: True	DWORD: 0	DWORD: 1	Lets you work with tabs in the Server Center window. This allows you to create one tab for each task category, such as license management, software deployment, and so on.
AutoGenerateMissingPatchesStatistics	Boolean: True	Boolean: False	DWORD: 1	DWORD: 0	Auto Generating Missing Patches and Installed Software Statistics are very expensive from a data load perspective. Add the plist or registry value, and enter the suggested setting to turn off the automatic generation of these statistics.
AutoGenerateInstalledSoftwareStatistics	Boolean: True	Boolean: False	DWORD: 1	DWORD: 0	
					When these settings are turned off, the Admin application prompts you to update the settings each time the appropriate dialog is opened, instead of constantly synchronizing this data.
DatabaseSyncManagerEnable	Boolean: False	Boolean: True	DWORD: 0	DWORD: 1	The suggested setting turns on database journalling of synchronization within the Admin application, which is a more efficient method of synchronizing.
DisplayServerAddressInWindowTitles	Boolean: False	Boolean: True	DWORD: 0	DWORD: 1	Displays the connected server in window titles.

Table 4. Changing the LANrev Admin default settings to optimize performance (continued)

plist setting or registry key	macOS platform		Windows platforms		Description
	Default Settings	Suggested Settings	Default Settings	Suggested Settings	
ForcePermanentNotificationConnection	Boolean: False	Boolean: True	DWORD: 0	DWORD: 1	This setting traps the outbound port from the Admin that was first used to negotiate the connection to the server. Making this setting helps in situations where a connection is torn down abruptly in the non-permanent case. You may also see this situation as a result of commands not updating correctly on the Admin, or slow and/or incomplete synchronizations.
ListenForNotificationPort	(none)	Number: 3973	missing	DWORD: 3973# **Base** option > **Decimal**	Using this setting always tells the server on which port to return a reply to the Admin. In an environment where the LANrev server is in a DMZ that is very specific about what traffic may move from the DMZ to the LAN, make this setting and open TCP 3973 from DMZ -> LAN to ensure that the server can notify Admins about updates to the inventories.
SyncLicenseStatusAgentRecords	Boolean: True	Boolean: False	DWORD: 1	DWORD: 0	If you are not collecting license monitoring information, use this setting. It turns off licensing status information from being synchronized. When the default setting is left, it collects the licensing information and the **lc_license_status_agent** table is synchronized with the Admin application.

In your **Deployment Center preferences** or settings, disable the **autoscan** option for the Windows Networking and Active Directory protocols to improve the response time. If you don't disable the **autoscan** option, you see an autoscan bar. Disabling the **autoscan** option doesn't remove its functionality, but it applies only when you open the Agent Deployment Center.

Reducing LANrev Admin synchronization

In larger deployments with more than 15 admin applications connected to the same LANrev server simultaneously, you can sometimes experience excessive database synchronizing. One admin application can make a change to the database that causes all other admin applications to unnecessarily synchronize with the server.

Excessive synchronizing can tie up the server and cause inventories and heartbeats to be cached, which can delay this information being processed and committed to the database, as well as making the server less responsive until the database synchronizations have completed.

IMPORTANT Concurrent changes to administrator accounts, license monitoring settings, or software distribution settings are handled such that users are allowed to make changes simultaneously to the same areas within the Server Center. When one user attempts to commit a change, the changes are intelligently merged. However, if there are conflicting changes within the same specific area of Server Center, the admin application provides a warning that notifies users that there are conflicting changes. The users are then asked to manually resolve the conflict.

This section provides information on the following topics:

- Minimizing synchronization for all connected admin applications
- Minimizing synchronization for a specific admin application

Minimizing synchronization for all connected admin applications

One way to alleviate the problems caused by excessive synchronizations is to increase the **InventoryTableNotificationDelay** setting found in the server's plist keys (macOS) or registry keys (Windows). This server setting affects the synchronization of all inventory tables for all connected Admin applications, which may not be specific enough for your needs.

To implement the **InventoryTableNotificationDelay** settings to minimize synchronizations on the Admin:

1. Close all Admin applications on all workstations.

2. Stop the LANrev Server service on the server as follows:
   - For Mac, open the **Extras** folder and select **Stop LANrev Server.command**.
   - For Windows, using the Windows Services applet, **stop** the LANrev Server service.

3. Edit the registry value **InventoryTableNotificationDelay** at **HKEY_LOCAL_MACHINE\SOFTWARE\Pole Position Software\LANrev Server** as set out below:

Registry value	Default setting	Recommended setting
InventoryTableNotificationDelay	DWORD: 3	For Inventory: DWORD: **300#** **Base** option > **Decimal**
		For Software Distribution: DWORD: **150#** **Base** option > **Decimal**
		For License Monitoring: DWORD: **120** # **Base** option > **Decimal**

4. Start the LANrev Server service on the server as follows:
    - For Mac, open the **Extras** folder and select **Start LANrev Server.command**.
    - For Windows, using the Windows Services applet, **start** the LANrev Server service.

      To force the LANrev server to reload its configuration data, change the 'trigger' registry value to **1**:

      HKEY_LOCAL_MACHINE\Software\Pole Position Software\LANrev Server\Trigger

5. Repeat steps 1 through 4 for all other servers.

Minimizing synchronization for a specific admin application

Another way to reduce synchronizations is to configure LANrev Admin using a **DatabaseTableSyncDelays.plist** file. The database tables are then synchronized according to a schedule, instead of every time any change is made. You can configure each database table separately so it is either synchronized at a specific interval or not synchronized at all (ignored).

To implement a customized **DatabaseTableSyncDelay.plist** to reduce the amount of database synchronizations:

1. Make sure that the **InventoryTableNotificationDelay** setting is either not present in the server preferences or, if present, that it is set to a value of at least 10 (decimal integer).

2. Create a new plist file named **DatabaseTableSyncDelays.plist**. The structure of the file should be:
    - **IgnoredTables**: This is an array of tables that are to be completely ignored. The values for the entries are the names of the tables to be ignored. Tables added here never synchronize.
    - **TableSyncDelays**: This is a dictionary of tables. The keys are the table names and the value for the keys is the synchronization delay in minutes.
    - **SeedValue**: The seed value must be incremented whenever **DatabaseTableSyncDelays.plist** is changed.

    You can specify the following tables for delay (**TableSyncDelays** dictionary) or ignore (**IgnoredTables** array), although certain tables should not be ignored; for example, **agent_info**, **hardware_info**, **software_info**.

    - commands
    - commandqueue
    - commandqueue_history
    - agent_info
    - agent_info_server
    - agent_powermanagement_settings
    - agent_custom_fields
    - hardware_info
    - hardware_battery_info
    - hardware_poweron_info
    - hardware_poweron_data
    - software_info
    - asset_modification_info
    - device_item_count
    - hardware_memory_info
    - volumes_info
    - ata_info
    - display_info
    - pci_info
    - scsi_info
    - firewire_info
    - usb_info
    - network_adapter_info
    - fonts_info
    - printers_info
    - startup_items_info
    - installed_software_info
    - missing_patches_info
    - win_services_info
    - machine_tracking_info
    - agent_processes
    - agent_files
    - agent_registry

The following screen capture illustrates a sample of the .plist file.

Property List	Class	Value
▼ Root	Dictionary	3 key/value pairs
▼ IgnoredTables	Array	2 ordered objects
0	String	fonts_info
1	String	agent_processes
SeedValue	Number	1
▼ TableSyncDelays	Dictionary	2 key/value pairs
installed_software_info	Number	300
usb_info	Number	60

3. Place the **DatabaseTableSyncDelays.plist** in the following location for your Admin applications. Ensure that the Admin application is not running. The following table provides the location of the **DatabaseTableSyncDelays.plist** file for different versions of LANrev.

Table 5. Location for DatabaseTableSyncDelays.plist dependent on operating system and LANrev versions

LANrev version number	For macOS	For Windows XP, 2000, and 2003	For Windows Vista, 2008, and Windows 7 and later
6.6 and earlier	~/Library/Preferences/ com.poleposition- sw.lanrev_admin_Database TableSyncDelays.plist	C:\Program Files (x86)\Pole Position Software\LANrevAdmin\LANrev Admin.resources\DatabaseTableSyncDelays.plist	
6.7 and later	~/Library/Application Support/LANrev Admin/ DatabaseTableSyncDelays. plist	C:\Documents and Settings\<<username>>\ Application Data\Pole Position Software\LANrev Admin\DatabaseTableSyn cDelays.plist	C:\Users\<<username>>\AppData\ Roaming\Pole Position Software\LANrev Admin\DatabaseTableSyncDelays.p list

Table 6 shows some samples of delay settings. The delays are based on the amount of data in each table, where the largest table is assumed to be accessed the most often, and therefore should have the lowest synchronization delay (3 minutes). Database tables than contain less data are accessed less frequently and can be put on a 10-minute delay and tables with little to no data in them can be put on a one-hour delay.

NOTE It is important to avoid unnecessarily delaying the synchronization of any inventory data that is critical to your data access needs.

Table 6. Examples of settings and their delay times when synchronizing between LANrev Server and LANrev Admin

3 minute delay	10 minute delay	60 minute delay
agent_custom_fields	missing_patches_info	agent_files
agent_info	asset_modification_info	agent_processes
agent_info_server	ata_info	agent_powermanagement_settings
hardware_info	device_item_count	agent_registry
hardware_poweron_data	display_info	firewire_info
installed_software_info	hardware_poweron_info	fonts_info
pci_info	hardware_memory_info	machine_tracking_info
software_info	network_adapter_info	scsi_info
win_services_info	printers_info	startup_items_info

Table 6. Examples of settings and their delay times when synchronizing between LANrev Server and LANrev Admin

3 minute delay	10 minute delay	60 minute delay
	usb_info	
	volumes_info	

4. Synchronizations for a table are delayed for that table if there was already a previous synchronization for it within the last delay interval. You can always force the table to be updated with the **Sync Selected Records** command. Tables that are changed due to a command sent by an Admin application are synchronized immediately for that Admin application, but are delayed for other Admin applications connected at the same time.

5. These settings can also be preset within the LANrev Admin application's installer.
    - For Windows, place the **DatabaseTableSyncDelays.plist** file in the same folder as the **setup.exe** file.
    - For macOS, place the **DatabaseTableSyncDelays.plist** file inside the **Contents** folder of the LANrev Admin application bundle.

6. The **DatabaseTableSyncDelays.plist** file has a seed number that must be incremented when this file is changed. If the seed value in the preferences **plist** file (see Table 5 on page 24) is less than the one in the application bundle, the value from the application bundle is copied into the preferences **plist** file.

Optimizing server role settings

HEAT Software can work with customers on a case-by-case basis to fine-tune LANrev server settings if performance degrades due to frequent synchronizations. This commitment may require access to debug and statistics logging from the LANrev server. For more information, consider engaging HEAT Professional Services to have a technical consultant assist you by sending an e-mail message to lanrev.services@heatsoftware.com.

Table 7 provides the following settings to optimize the various LANrev server roles (inventory, software distribution, license monitoring) using registry key or plist settings. It is presumed that each server runs on its own hardware and only serves a single role assigned to it. Also make sure that agents only send basic inventory data to the software distribution and license monitoring servers.

Table 7. Registry key or plist settings used to optimize various LANrev server roles

Registry or plist key	Inventory server	Software distribution server	License monitoring server
AgentRequestCacheGetSDPackageIdlePriority	n/a	4	n/a
AgentRequestCacheGetSDPackagePriority	0	1	0
AgentRequestCacheGetSDPatchPackageIdlePriority	n/a	6	n/a
AgentRequestCacheGetSDPatchPackagePriority	0	1	0
AgentRequestCacheGetSLPackageIdlePriority	n/a	n/a	8
AgentRequestCacheGetSLPackagePriority	0	0	1
AgentRequestCacheSetSLStatusIdlePriority	n/a	n/a	14
AgentRequestCacheSetSLStatusPriority	0	0	1
AgentRequestCacheGetStagingServerIdlePriority	n/a	2	n/a
AgentRequestCacheGetStagingServerPriority	0	1	0
AgentRequestCacheMaxRequestsToFetch	n/a	100	100
AgentRequestCacheMaxWorkTime	n/a	1000	1000

Table 7. Registry key or plist settings used to optimize various LANrev server roles (continued)

Registry or plist key	Inventory server	Software distribution server	License monitoring server
AgentRequestCacheSleepTimeIfCommandsPending	n/a	50	50
AgentRequestCacheSleepTimeIfConnectionThreshold	n/a	200	200
AgentRequestCacheSoftwarePatchStatusIdlePriority	n/a	10	n/a
AgentRequestCacheSoftwarePatchStatusPriority	0	1	0
AgentRequestCacheSubmitThreshold	n/a	10	10
AgentRequestCacheUpdateInstallationStatusIdlePriority	n/a	6	n/a
AgentRequestCacheUpdateInstallationStatusPriority	0	1	0
GeneralTableNotificationDelay	150	100	100
InventoryImportInventoryChunkSize	200	n/a	n/a
InventoryImportInventoryCommandPriority	1	n/a	n/a
InventoryImportInventoryPriority	2	n/a	n/a
InventoryImportOtherCommandPriority	1	n/a	n/a
InventoryImportOtherDataChunkSize	50	n/a	n/a
InventoryImportOtherDataPriority	2	n/a	n/a
InventoryTableNotificationDelay	300	120	120
MaxCommandsToFetchFromCommandQueue	50	n/a	n/a
MaxNumberAgentRequests	400	400	400
MaxNumberConnection	400	400	400
MaxNumberTotalConnection	500	500	500
StatusUpdateTableNotificationDelay	10	10	300

This section also provides the following information:

- [Increasing the interval time for heartbeat notifications](#)
- [Adding the DatabaseJournalMode server registry value for Windows servers](#)

Increasing the interval time for heartbeat notifications

The **HeartbeatNotificationTaskInterval** server side setting is defined as the interval of time in seconds that the server sends notifications about new heartbeats to the Admin applications.

Depending on your organization's overall Agent population, you may want to change this setting to increase the interval so that heartbeats are not sent in rapid succession. The longer the interval, the more heartbeats are sent, but the frequency by which the updates occur is lessened.

- For a macOS platform, the setting is made in the following .plist file:

  Key: **HeartbeatNotificationTaskInterval**

  Type: **Number**

  Value: see [Table 8](#)

- For Windows platforms, the setting is made in the following registry key:

  Value: **HeartbeatNotificationTaskInterval**

  Type: **DWORD** (**Base** option > **Decimal**)

  Value: see [Table 8](#)

Table 8 provides the values to set based on the installed Agent population.

Table 8   HeartbeatNotificationTaskInterval Settings Based on Overall Installed Agent Population

Overall installed Agent population	Values to set (in seconds)
0 – 1000	5
1001 – 2500	60
2501 – 5000	120
5001 – 10000	240
10001 – 20000	360
20001 – 30000	480
30001 – 40000	600
40000+	900

Adding the DatabaseJournalMode server registry value for Windows servers

The DatabaseJournalMode server registry values impact LANrev and MDM installations on Windows server platforms by affecting the way the database transactions are handled by the SQLite back-end.

IMPORTANT   To implement the **DatabaseJournalMode** registry value, there should be at least # 5 GB of free space on the drive where the database resides.

Check the Server log to see if it is locked by looking at the following location:

%windir%\Temp\LANrev Server.log

When the server log shows many instances of **Database is locked**, set the **DatabaseJournalMode** value in the registry. If locked, continue with the following task.

To add the **DatabaseJournalMode** registry value:

1. Using the Windows Services applet, **stop** the LANrev Server service on the server.

2. Run **regedit** on the server.

3. Back up all of the following **.db** files:
   • **ServerCommandDatabase.db**
   • **ServerDatabase.db**
   • **AgentRequestCache.db**
   • **SoftwareLicenseControl.db**
   • **MobileDevices.db**
   • **EnumValues.db**

4. Navigate to the server registry path at **\\HKLM\Software\Pole Position Software\LANrev Server**

5. Add **DatabaseJournalMode** as follows:

    Registry Value = **DatabaseJournalMode**

    Type = **String**

    Value = **WAL**

    Do not set this key if you have less than 20% free disk space available on the volume where the production database is located.

6. Using the Windows Services applet, **start** the LANrev Server service on the server.

Purging the command history

Over time, processed commands can build up in the database, unnecessarily bloating its size.

You can instruct LANrev Server to automatically purge the command history whenever it performs database maintenance. Note that this will reduce the database size after the next maintenance, not immediately.)

The required steps are described below by platform:

- Purging the command history for a macOS server
- Purging the command history for a Windows server

Purging the command history for a macOS server

To purge the command history for macOS servers:

1. Stop the LANrev Server service by opening the **Extras** folder and clicking **Stop LANrev Server.command**.

2. Edit the **/Library/Preferences/com.poleposition-sw.lanrev_server.plist** in a plist editor to add the following content to the file:
   - **DiscardDesktopCommandHistory boolean: true**
   - **DiscardDesktopCommandHistoryMaxAge integer: 30**
   - **DiscardMobileCommandHistory boolean: true**
   - **DiscardMobileCommandHistoryMaxAge integer: 30**

3. Start the LANrev Server service by opening the **Extras** folder and clicking **Start LANrev Server.command**.

Purging the command history for a Windows server

To purge the command history for Windows 32 bit and 64 bit servers:

1. Using the Windows Services applet, **stop** the LANrev Server service on the server.

2. Run **regedit** on the server.

3. Navigate to the registry location **\\HKLM\Software\Pole Position Software\LANrev Server**

4. Add the following values to the LANrev Server key. You can set the value in days to keep anything you choose. The recommended setting is **30**. If this key is not added, then everything is kept and nothing gets purged.
   - **DiscardDesktopCommandHistory DWORD: 1**

- **DiscardDesktopCommandHistoryMaxAge DWORD: 30 (Base** option > **Decimal**)
- **DiscardMobileCommandHistory DWORD: 1**
- **DiscardMobileCommandHistoryMaxAge DWORD: 30 (Base** option > **Decimal**)

5. Using the Windows Services applet, **start** the LANrev Server service on the server.

   When you start the LANrev Server service again, these settings implement command history preservation of commands up to 30 days old. You can adjust this time frame as necessary.

Implementing agent preference settings globally

For information about how to implement the **GlobalAgentPrefs** settings, see the support site and search for article 20720.

IMPORTANT **GlobalAgentPrefs** settings should only be implemented on a single server if you have configured a multiserver environment. The server to which the dictionary is added must match the first server in the list of inventory servers in your **Agent Settings** > **Servers** dialog. It is imperative that the first server in the Inventory Servers list is uniform across all Agents. If you have mixed settings, with some servers listed in different positions than shown on the Inventory Servers list, you must issue a **Change Agent Settings** command to make sure that all of your Agents have the same inventory server showing as the first server in the list of Inventory Servers.

Table 9 provides the potential Agent settings that you can define globally on the LANrev server. These settings are intended primarily to reduce the Agent requests to the server for the given circumstances outlined in the table.

Table 9. Agent preference settings defined globally on the LANrev server

Global agent			Description
Setting name	**macOS .plist value**	**Windows registry value**	
IdleTimeThreshold	Number:1440	DWORD: 1440# **Base** option > **Decimal**	See the support site and search for article 20720.
SendInventoryOnHUPSignal	Boolean: False	DWORD: 0	When set to **0**, changes the Agent to never send inventory if a Hang Up Signal (HUP) is sent.
SendInventoryOnNetworkChange	Boolean: False	DWORD: 0	When set to **0**, changes the Agent to never send inventory if the Agent changes Active IP.
SendInventoryOnStartup	Boolean: False	DWORD: 0	When set to **0**, prevents the Agent from sending inventory on startup.
SDPerformCheckAfterNetworkChange	Boolean: False	DWORD: 0	When set to **0**, prevents the Agent from sending Software Distribution (SD) check requests if the Agent changes its active IP.

Table 9. Agent preference settings defined globally on the LANrev server (continued)

Global agent			Description
Setting name	**macOS .plist value**	**Windows registry value**	
SDPerformCheckAfterUserLogin	Boolean: False	DWORD: 0	When set to **0**, prevents the Agent from sending SD check requests if the user performs a login/logout of the system. Do not enable this if you are depending on package installation on login event.
SendInventoryOnInterval	Boolean: False	DWORD: 0	Disables automatic inventory based on interval. Set only when you want to manually gather inventory to update information.
SendCustomFieldsWithBasicInventory Only	Boolean: True	DWORD: 1	If basic inventory is enabled and you need dynamic custom fields to populate inventory, enable this option.

Optimizing mobile device management server settings

In most situations, mobile devices send a lighter inventory footprint than desktop devices. However, under certain circumstances – such as in very large implementations – you may need to set server-side preferences that reduce the potential load on the LANrev database, specifically with regard to requests handled by the MDM Server.

You can also configure interval settings for when the Agents update information on managed mobile devices, shown in Table 10.

Table 10. Recommended Server Center interval settings for managed mobile devices

Number of managed mobile devices	Gather inventory device information (hours)	Track device interval (minutes)
default settings are:	24	10
1 – 499	24	10
500 – 1999	24	30
2000 – 4999	24	60
5000 – 9999	36	90
10000 – 19999	48	120

Table 11 provides LANrev server-side optimization settings for MDM implementations.

Table 11. LANrev server-side optimizations for MDM implementations

MDM Agent			Description
Setting name	**Recommended setting value for macOS platforms**	**Recommended setting value for Windows platforms**	
MDMApplistingDelayAfterInstall where MDM devices > 1000	Number: 900	DWORD: 900 # **Base** option > **Decimal**	These two values, in seconds, affect whether the next list of installed applications is requested when certain installation responses are sent during installation. Due to the way MDM is implemented in iOS, you need to issue these commands after you install a managed application.
MDMApplistingDelayAfterInstall2 where MDM devices > 1000	Number: 1200	DWORD: 1200# **Base** option > **Decimal**	The smaller the interval, the faster the installation state is updated to the correct value, but this also produces a larger amount of database operations (resulting in a larger number of records being updated).
			The larger the interval, the less likely it is that multiple **get installed application** commands need to be issued, which decreases the amount of data that gets transferred. However, this larger interval also causes the installation state to be updated less frequently, so the final **Installed** state may not show until after this delay has passed after the installation.
			Large intervals are less responsive than short intervals, therefore, when you decrease large values you increase responsiveness. You can fine-tune the values to find a balance between load and timeliness.
MDMInstallAppProvisioningProfile Timeout	Number: 300	DWORD: 300# **Base** option > **Decimal**	This value (in seconds) determines how long the LANrev Apps app waits when installing the application before downloading the provisioning profile.
MDMSendPushNotificationOnCustomFieldsChange	Boolean: No	DWORD: 0	With this setting in place, custom **Information** field changes on endpoints do not trigger an automated Device Update command. The effect is that custom fields will not get updated immediately, but only when the devices report in on their scheduled contact interval or when the administrator performs a manual **Update Device Information** command.
VPPServiceParallelServerConnectionCount	Number: 5	DWORD: 5	The number of parallel connections to the Apple VPP server that LANrev Server uses for retrieving license information.

Implementing best practices for MDM

This section provides information about optimizing various Mobile Device Manager (MDM) settings, which include the following:

- Specifying how many devices a user can enroll
- Controlling how many entries are logged for each device

Specifying how many devices a user can enroll

There is a server-side prefs key that specifies how many devices a user can enroll. In cases where an exception is needed, you can specify a dictionary that contains the numbers of users where the key is the enrollment username.

IMPORTANT The username in the dictionary has to be all lowercase.

When specifying the following settings, keep in mind that they are values set in the registry for Windows servers and that they are keys set in the server plist for macOS servers.

- **Key: MDMMaxDevicesPerUser**

  Type: Number

  Default: 0 (A value of **0** means that there is no limit on the number of devices a single user can enroll. This setting is up to the administrator. If set to **1** there are implications, which are documented in https://community.heatsoftware.com/community/products/heat-unified-endpoint-management in the topic titled "Limiting amount of devices a user can enroll".)

  Description: If the Default value is not **0**, then this is the number of devices a user can enroll.

  NOTE When this setting is changed to **1** and the user enrolls his or her device again, he or she gets an error. The user must use the Admin application to remove the device from the mobile devices window.

- **Key: MDMMaxDevicesUserList**

  Type: Dictionary

  Description: A list of numbers where the key is the username (the one the user authenticates with) and the value is the number of devices the user can enroll. This value supersedes the value set in **MDMMaxDevicesPerUser**.

A new server side **plist** setting controls the following key:

- **Key: MDMWhiteListedDevices**

  Type: Array

  Description: A list of UDIDs (unique device identifiers) that can enroll into the MDM system

Controlling how many entries are logged for each device

You can use the audit log and control how many entries are logged for each device. This feature gives you the ability to manage the volume of log entries, which is useful for organizations that manage many devices. When you have numerous devices, you may also want to control the number of entries that get logged for each device.

To activate the audit log and control how many entries are logged for each device on the macOS platform:

---

1. Stop the LANrev Server service by opening the **Extras** folder and clicking **Stop LANrev Server.command**.

2. Set the following .plist keys in the **/Library/Preferences/com.poleposition-sw.lanrev_server.plist** as follows:

    Key: AuditLogEnabled

    Type: Boolean

    Value: true

3. The following value controls how many Audit Log entries are actually logged for each device if you have numerous devices:

    Key: AuditLogMaxDeviceNames

    Type: integer

    Default: 20

    Description: When an operation is performed against more devices than specified in **AuditLogMaxDeviceNames**, then instead of each individual device name, only the number of devices is shown.

4. Start the LANrev Server service by opening the **Extras** folder and selecting **Start LANrev Server.command**.

To enable the Audit Log feature and control how many entries are logged for each device on Windows platforms:

1. Using the Windows Services applet, stop the LANrev Server service on the server.

2. Run regedit on the server.

3. Navigate to the registry location **\\HKLM\Software\Pole Position Software\LANrev Server**

4. Add the following registry value:

    Value: AuditLogEnabled

    Type: DWORD

    Value: 1

5. If you want to control the number of Audit Log entries that are captured for each device, also add the following registry value:

    Value: AuditLogMaxDeviceNames

    Type: DWORD

    Value: 20 (**Base** option > **Decimal**)

    Description: If an operation is performed against more devices than specified in **AuditLogMaxDeviceNames**, then instead of each individual device name, only the number of devices is shown.

6. Using the Windows Services applet, start the LANrev Server service on the server.

Customizing MDM settings for large systems

The number of managed endpoints in an environment has a direct correlation to server performance: The more endpoints managed, the greater the demand on your LANrev inventory server. If you are managing mobile devices in your environment, you can optimize the system to improve performance under heavy loads:

*   Separate your MDM server from the inventory server role.

In smaller environments, it is perfectly fine to run the MDM server service (the web service) on the same server as the inventory server role (LANrev Server).

We strongly recommend, however, that you separate these two roles onto two physical servers when you manage more than about 2000 endpoints. Doing so can greatly increase performance.

Note that you should use separate DNS names for the inventory server and MDM roles in any case, even if one physical servers performs both. In particular, this avoids having to re-enroll all managed devices when you later need to split the roles.

- Add additional MDM servers, if you have a very large system.

In very large systems, simply splitting the inventory and web server roles may not be sufficient for optimal performance. If there are more than 5,000 to 10,000 managed devices, you may want to consider splitting the MDM (web server) roles onto multiple front-end servers in a round-robin DNS configuration.

The details of this configuration are described in the knowledge base article 20823.

As a rule of thumb, one front-end MDM server should be set up per each 5,000 to 10,000 managed devices.

Chapter 4   *Backing up your LANrev system*

Backing up your data is significant to optimizing your LANrev system, specifically from the stand point of implementing your disaster recovery plan without loss of data. The tasks provided in this chapter provide instructions for backing up your specific data and settings to prepare you for either migrating to new LANrev releases as they become available or recovering from a catastrophic failure of your equipment.

This chapter provides the following tasks to help you maximize the built-in provisions for database maintenance and backups included with LANrev:

- Backing up the server
- Backing up server settings and dynamic custom fields
- Backing up the LANrev Server databases
- Backing up the LANrev Server certificates folder
- Backing up the MDM server certificates
- Backing up the admin application
- Backing up the iOS payloads
- Backing up a master distribution point
- Manually backing up the software distribution packages

IMPORTANT   Before you can restore, migrate, or move the LANrev server and your entire system, you need to ensure that you have exported a customized version of your LANrev Agent in the Agent Deployment Center, which is configured with the correct server addresses and server certificates for your LANrev installation. For more information, see the *LANrev User Guide*, "Installing or updating LANrev Agent".

Backing up the server

When you back up your old server in readiness to migrate it, you need to ensure that you have backed up the components shown in Table 12.

Table 12. LANrev components to back up and move when migrating to a new server

LANrev component	Action to take	Description
Agent	Export	Ensure that you export a customized version of your LANrev Agent in the Agent Deployment Center, configured with the correct Server address (DNS) and server certificates for your LANrev installation.
Server settings	Export	You can export the Server Settings from the command line.
	Copy	These settings are found in the Server Center's **Server Settings** area.
Dynamic custom fields	Export	Open the **Server Center** and from the **Custom Fields** area, export the dynamic custom fields.
Custom field attachments	Copy	This information includes the scripts and executables associated with dynamic custom fields.

Table 12. LANrev components to back up and move when migrating to a new server (continued)

LANrev component	Action to take	Description
iOS payloads	Copy	This information includes the payload items for mobile apps and media, configuration profiles, and provisioning profiles.
Active server databases	Copy	These databases include the current inventory, software distribution, and license monitoring data.
Backup server databases	Copy	These databases include the previous database backup sets.
Server certificates	Copy	This information includes the SSL certificate that is unique to this server and possibly Apple push certificates, if applicable.
Server logs	Copy	This information is the historical data for the past database maintenance and backups.

Backing up server settings and dynamic custom fields

All client information is stored in the LANrev databases, however the LANrev Server settings are stored externally in a macOS **plist** file or Windows **registry settings**.

To migrate LANrev Server installation from one computer to another, most of the data, such as the database tables, can be transferred easily by copying the relevant files from the LANrev Server folder. By default, this folder is found at **/Library/ Application Support/LANrev Server** on macOS systems and **ProgramData\Pole Position Software\LANrev Server** on Windows systems.

This section provides the following tasks:

- Backing up custom executables or script files
- Saving server settings and custom field definitions to an XML file on the macOS platform
- Saving server settings and custom field definitions to an XML file on windows platforms
- Exporting the dynamic custom fields

Backing up custom executables or script files

If you defined any dynamic custom information items based on executable or script files, you also need to back up the **CustomFieldScriptFiles** folder at the following locations:

- For Mac: **/Library/Application Support/LANrev Server/CustomFieldScriptFiles**
- For Windows: **%programdata%\Pole Position Software\LANrev Server\CustomFieldScriptFiles**

Saving server settings and custom field definitions to an XML file on the macOS platform

There is a command line option that lets you save the server settings and custom field definitions as an XML file, and import that file into any other server instance. The file is compatible with both the macOS and Windows versions of the server.

To create an XML file for saved server settings and custom field definitions from a server installed on macOS:

1. On the computer on which the server is installed, start **Terminal**.

2. On the **Terminal** window, type (or paste) the following command:

   sudo /Library/Application\ Support/LANrev\ Server/LANrev\ Server.app/Contents/ MacOS/LANrev\ Server --ExportPreferences /LANrevServerSettings.plist

   where **LANrevServerSettings.plist** is the path and name of the settings file you want to create.

   Press **Enter**.

3. When prompted, enter the **password** to run the command with **superuser privileges**.

   The settings file is created with the specified name at the specified location.

Saving server settings and custom field definitions to an XML file on windows platforms

To create an XML file for saved server settings and custom field definitions from a server installed on Windows:

1. On the computer on which the server is installed, start **cmd.exe** with **administrator** privileges.

2. On the Terminal window, browse to the **Program Files\Pole Position Software\LANrev Server** directory.

3. Enter the following command:

   LANrev Server.exe --ExportPreferences C:\LANrevServerSettings.plist

   where **LANrevServerSettings.plist** is the path and name of the settings file you want to create.

   Press **Enter**.

   The settings file is created with the specified name at the specified location.

Exporting the dynamic custom fields

To export the dynamic custom fields:

1. Open the Server Center and in the **Custom Fields** area, select all of your dynamic custom fields that do not use attachments.

2. Right-click and on the options menu, click **Custom Information Fields > Export Selected Fields** to export their definitions.

3. If you have any dynamic custom fields that use scripts stored as text instead of a file attachment, copy the script's text for these into a single text file.

Backing up the LANrev Server databases

All client information is stored in the LANrev databases, therefore backing up these databases regularly is essential.

Backing up your databases on LANrev Server is set when you initially install the system and occur according to the default backup settings or the edited settings you provide. (See the *LANrev User Guide*, "Configuring database backup and maintenance".)

It's also important to know that you must back up live and stored backup databases to separate locations. Therefore, we recommend that you change the **DatabaseBackupDirectory** path to

another location on another physical or network drive that is backed up on a regular basis to provide some extra redundancy. The point is to store your backed up databases on a different drive than the one that hosts your live databases. Otherwise, if that hard disk fails for any reason, all of your database backups are fine.

Database backups include the following files:

- ServerCommandDatabase.db
- ServerDatabase.db
- AgentRequestCache.db
- SoftwareLicenseControl.db
- MobileDevices.db
- ClassroomDatabase.db

The following tasks are included in this section:

- Enabling the LANrev database maintenance checks and backups
- Changing the database backup location

Enabling the LANrev database maintenance checks and backups

LANrev database maintenance checks look for possible corruption, which is repaired when found if possible. These database maintenance checks also compact the databases.

To enable database maintenance checks:

1. In the **Server Settings** area of the Server Center, click the **General** tab.

2. Enable the **Run database maintenance** and **Backup database** options.

3. Make sure that the database maintenance is scheduled approximately **60 minutes** before the backup is scheduled. This precaution ensures that the database is compacted to the smallest size possible before it's backed up.

4. Also consider adjusting the database backup settings to an interval of three days and keeping up to seven backups. This setting extends the time window back to **21 days** from which you can recover data.

   The database maintenance fixes minor integrity problems whenever it can. However, moderate corruption that is too extensive to completely repair – and which may not have triggered an error message – may exist.

   Extending the time window back to 21 days increases the chances of being able to revert back to a database set before the corruption started.

   NOTE   If you have more free hard drive space, you may consider keeping even more backups. For example, 14 x 3 = 42 days from which you can back up.

5. In the case of database corruption without a power outage event, we highly recommend that you run a disk scanning utility to verify the integrity of the physical disk hosting the LANrev databases, particularly if there are repeated instances of database corruption.

Changing the database backup location

The database backup makes a copy of the current databases and adds a **.dbbackup.n** extension, where **n** denotes the numerical age of the backup. Newer backups have a lower **n** number with the exception of the most current backup set, which has no **n** number.

By default, the LANrev server backs up the databases to the same folder as the live databases at the following default locations:

- For macOS: **/Library/Application Support/LANrev Server**

- For Windows: **%programdata%\Pole Position Software\LANrev Server**

NOTE We recommend that you back up live and stored backup databases to separate locations.

Therefore, we recommend that you change the DatabaseBackupDirectory path to another location on another physical or network drive that is backed up on a regular basis to provide some extra redundancy. The point is to store your backed up databases on a different drive than the one that hosts your live databases. Otherwise, if that hard disk fails for any reason, all of your database backups are fine.

To change the database backup path:

1. Stop the LANrev Server services on the server as follows:
   - For macOS, open the **Extras** folder and select **Stop LANrev Server.command**.
   - For Windows, use the Windows Services applet and select the **LANrev Server** to **stop**.

2. Move all **.dbbackup<n>** files to the new database backup location.

3. Edit the **DatabaseBackupDirectory** key or value at the following settings locations in the registry to define the new backup location.
   - For macOS: **/Library/Preferences/com.poleposition-sw.lanrev_server.plist**
   - For Windows: **HKLM\Software\Pole Position Software\LANrev Server**

4. Restart the LANrev Server services on the server as follows:
   - For macOS, open the **Extras** folder and select **Start LANrev Server.command**.
   - For Windows, use the Windows Services applet and select the **LANrev Server** to **start**.

Backing up the LANrev Server certificates folder

Server certificates are unique to your LANrev server.

Each time the LANrev server is installed, it generates a unique SSL server certificate that is used to secure traffic between all LANrev components. Reinstalling the server, even on the same physical device, results in a different server certificate. For your new server to accept traffic from existing Agents, you must migrate the server certificate from the old server certificate backups to the new server.

The following tasks are included in this section:

- Backing up server certificates on macOS
- Backing up server certificates on Windows

Backing up server certificates on macOS

To back up the SSL server certificates folder for macOS platforms:

1. In the **Finder**, go to **/Library/Application Support/LANrev Server**.

2. Edit the folder permissions for the **Certificates** folder to add your current user account and grant it **Read only access**.

3. Add the **Certificates** folder to a zip file by right-clicking it and picking **Compress "Certificates"**. Save the zip file to a network drive or a removable storage device such as a USB stick.

Backing up server certificates on Windows

To back up the SSL server certificates folder for Windows platforms:

1. Go into **C:\ProgramData\Pole Position Software\LANrev Server** and take ownership of the **Certificates** folder, assigning it to the local Administrators group.

2. Make sure to enable the checkbox **Replace owner on subcontainers and objects**.

3. Zip up the contents of the **Certificates** folder and save them to a network drive or a removable storage device such as a USB stick.

Backing up the MDM server certificates

When you install your MDM Server, you define and upload the LANrev Server SSL certificate on that server as well as the Organizational SSL certificate for the MDM Server. We recommended that both of these certificates, in addition to any Intermediate SSL certificates, get stored in a safe place in the event that the MDM server needs to be installed again.

For more information, see the *LANrev User Guide*, "Installing MDM support".

To obtain and export the LANrev Server's SSL certificate:

1. Using the LANrev Admin application, open the **Server Center** > **Server Settings** > **General** tab.

2. Export this certificate by clicking **Save Certificate**.

3. On the File System Browser dialog, archive the certificate (that is, **server '<my server name>' certificate.pem**) to the file system.

To obtain the Organizational SSL certificate:

1. Contact your SSL certificate vendor and purchase this certificate.

2. **Save this certificate and the private key**. If you don't retain the private key, the identify of the recovered server is not the same as the original identity of the certificate.

   As a result, if the private key is unknown, all mobile devices will need to be enrolled into the service again.

   In a macOS environment, the certificate and private key exist in the Keychain application, and should be exported as a **.p12** file.

   In a Windows environment, the certificate and private key are in the **PKCS#7** format and are saved as a **.pfx** file.

3. If your certificate vendor is classified as a non-CA root, intermediate certificates will likely be required.

   On the Windows platforms, import the intermediate certificates to the **Certificates MMC** snap-in. You can download intermediate certificates from your SSL vendor at any time.

Backing up the admin application

Backing up the Admin application is relative to your organization's particular installation and, of course, the platform on which your system is installed.

The following tasks are included in this section:

- Backing up the admin application on macOS
- Backing up the admin application on Windows

Backing up the admin application on macOS

To back up the Admin application for your new LANrev system, on a macOS platform:

1. Go to **~/Library/Application Support/LANrev Admin**.

2. Zip all folders and files – except for the **Certificates** and **Database** folders – in that location.

3. If you have implemented a custom **DatabaseTableSyncDelays.plist** file, back that file up too.
   This file is placed in one of the following locations:

   - **~/Library/Preferences/com.poleposition-sw.lanrev_admin_DatabaseTableSyncDelays.plist**
   - Inside of the LANrev Admin application package as **Contents > DataTableSyncDelays.plist**

4. Copy the **~/Library/Preferences/com.poleposition-sw.lanrev-admin.plist** file into to a shared location from which you want to back it up on a network drive, an external drive, or a USB drive.

Backing up the admin application on Windows

To back up the admin application for your new LANrev system, on a Windows platform:

1. Go to **%appdata%\Roaming\Pole Position Software\LANrev Admin**.

2. Zip up all files and folders except for the **Database** folder in the location shown in step 1.

3. If you have implemented a custom **DatabaseTableSyncDelays.plist** file, back that file up too.
   This file is placed in one of the following locations:

   - **%ProgramFiles%\Pole Position Software\LANrevAdmin\LANrev Admin.resources\DatabaseTableSyncDelays.plist**
   - **%ProgramFiles(x86)%\Pole Position Software\LANrev Admin\LANrev Admin.resources\DataTableSyncDelays.plist**

4. Export the **HKCU\Software\Pole Position Software\LANrevAdmin** key as a **.reg** file to a shared location from which you want to back it up on a network drive, an external drive, or a USB drive.

Backing up the iOS payloads

The iOS payloads and related items are stored in a folder on the LANrev Server computer.

Backing them up is described below by platform:

- [Backing up server certificates on macOS](#)
- [Backing up server certificates on Windows](#)

Backing up iOS payloads on macOS

To back up the SSL server certificates folder for macOS platforms:

1. In the **Finder**, open **/Library/Application Support/LANrev Server**.

2. Edit the folder permissions for the **iOSPayloads** folder to add your current user account and grant it **Read only access**.

3. Add the **iOSPayloads** folder to a zip file by right-clicking it and picking **Compress "Certificates".** Save the zip file to a network drive or a removable storage device such as a USB stick.

Backing up iOS payloads on Windows

To back up the SSL server certificates folder for Windows platforms:

1. Open **C:\ProgramData\Pole Position Software\LANrev Server** and take ownership of the **iOSPayloads** folder, assigning it to the local Administrators group.

2. Make sure to enable the checkbox **Replace owner on subcontainers and objects**.

3. Zip up the contents of the **iOSPayloads** folder and save them to a network drive or a removable storage device such as a USB stick.

Backing up a master distribution point

If a distribution point fails, you need to have a backup of both the compressed binary files and the package definitions.

To set up a redundant, mirrored distribution point:

1. Install the LANrev Administration application on the new system and log into the old server as an **Administrator**.

2. Open the Agent Deployment Center window and export a customized copy of the Agent that corresponds to the distribution point's particular platform.

3. Install the customized Agent you just exported in the previous step onto the new system.

4. Add this Agent as a secondary distribution point in the Server Center window and save your changes.

At this point, you have created a redundant distribution point that mirrors the master distribution point. If the master distribution point fails, you can promote the secondary distribution point to master, and demote the old master distribution point to secondary.

Manually backing up the software distribution packages

To manually back up the software distribution packages, which includes the compressed binary files and appropriate information, you want:

1. Open the **Server Center**.

2. In the **Software Distribution** folder, select the packages you want to export.

3. Right-click the packages and select **Export Packages**.

4. **Save** as the name of your choice.

Glossary

The glossary defines the various terms used in the LANrev application and specifically those terms that show in this guide.

Term	Description
ADC	Agent Deployment Center.
agent	A software application that is installed on each managed computer and mobile device. Agents receive commands from LANrev and carry them out on the local computer, sending back information as required. There is a minimal local interface to specify some information.
central server	Acts as the hub of the system. When this server receives instructions, it sends out commands to the Agents, collects the information they send back, and stores the information in its database. There is usually one server per managed network, although multiple servers are possible. Servers have no user interface of their own – they are managed by the Admin application. LANrev effortlessly handles hierarchies of servers and specialized servers; for example, for software distribution.
desktop device	Refers to traditional desktop and laptop computers.
device	A piece of electronic communication hardware on which you can install the Agent, such as Windows or macOS computers.
distribution point	Computers that are designated to hold software installers for the Software Distribution Center and distribute them to the Agents.
DMZ	Demilitarized Zone. Refers to computers, for example, that are directly connected online, instead of being connected to the corporate network.
DNS	Domain Name Service. We recommend that you assign a DNS name to the LANrev servers and distribution points to minimize the time and effort it takes to recover from a catastrophic failure in the event that either of these components fail.
endpoint	The total number of both desktop devices and mobile devices that are hosted on the LANrev servers. For example, in Table 1 on page 11 endpoints refer to determining the thresholds reached for optimizing LANrev functionality.
GUID	Globally Unique IDentifier.
HUP	Hang Up signal.
inventory monitoring	Each Agent on managed computers and devices is assigned to a single server (including the central server) or multiple servers using an IP address or DNS names. An Agent can be assigned to any number of inventory servers, all of which have the same level of access. Only these servers can send commands to and receive information from their assigned Agents.
IP	Internet Protocol.
IT	Information Technology.
LANrev Admin	The command center for the LANrev system. You use LANrev Admin both to control the server (and through the server, to control the Agents), and to show required information. You can install the LANrev Admin application on multiple computers, as needed.

Term	Description
load-balancing	Distributing workloads across computers or other resources for optimal use and overload avoidance. Used to increases reliability through redundancy.
master distribution point	One master distribution point must exist at all times in the software distribution system. For recommended best practice regarding distribution points, see also secondary distribution point. The master distribution point serves as the source of software installers for the other (mirror) distribution points. There must always be exactly one master distribution point.
managed computers and devices	Those desktop devices and mobile devices on which an Agent resides.
MDM	Mobile device management.
MDM server	This optional server handles the management of mobile devices. This server is tightly coupled to the main LANrev Server and is controlled from the same admin application.
multiple servers	An installation where the server roles are dispersed across more than one server.
payload	Files or folders that are installed on the client computers. Payloads are stored on distribution point and referenced in installation packages.
.pem file	Private encryption key file
redundancy	Provides additional or duplicate systems, equipment, and so forth that function when a system or the hardware fails.
secondary distribution point	As a best practice we recommend that you configure at least two distribution points – one master distribution point and one secondary mirror distribution point. This method ensures that there is always a backup copy of your software payloads, which lets you continue distributing software even when one of the distribution points is lost.
server role	Applications have specific network requirements and prerequisites. Server roles include Inventory database, software distribution database, and license monitoring database. One instance of each role is required.
service framework	A root website that hosts web services already shared between all applications in a LANrev data center.
single server deployment	An installation where all three server roles are installed on one server.
software distribution	Automatically distribute and install a specific range of software applications on new and existing managed computers. For mobile devices, you can distribute software applications through an app store.
SSL certificate	For security reasons, LANrev components, such as servers, admin consoles, and agents, require SSL certificates to identify all components, and to validate and secure traffic from the agents.
UDID	Unique device identifier. Found in iTunes, this is a sequence of 40 numbers and letters specific to an iOS mobile device.
user role	LANrev supports users and two types of administrators: standard administrators and superadministrators.
WAN	Wide Area Network.

Index