DeviceLock® DLP Quick Install Guide

Contents:

- [General information](#)
- [Choosing the right management console](#)
- [Deploying DeviceLock Service for Windows](#)
- [Deploying DeviceLock Service for Mac](#)
- [Installing DeviceLock Enterprise Server](#)
- [Installing DeviceLock Content Security Server](#)

General information

DeviceLock DLP Suite consists of three parts: the agent (DeviceLock Service), the server (DeviceLock Enterprise Server and DeviceLock Content Security Server) and the management console (DeviceLock Management Console, DeviceLock Group Policy Manager, DeviceLock WebConsole and DeviceLock Enterprise Manager).

1. DeviceLock Service is the core of DeviceLock. DeviceLock Service is installed on each client system, runs automatically, and provides device and network protection on the client machine while remaining invisible to that computer's local users.

2. DeviceLock Enterprise Server is the optional component for centralized collection and storage of the shadow data and audit logs. DeviceLock Enterprise Server uses MS SQL Server to store its data. You can install several DeviceLock Enterprise Servers to uniformly spread the network loading.

   DeviceLock Content Security Server is also the optional component which includes:

   - DeviceLock Search Server for instant search of text across shadowed files and other logs stored on DeviceLock Enterprise Server.
   - DeviceLock Discovery Server for locating certain types of content stored within and outside the limits of the corporate network.

3. The management console is the control interface that systems administrators use to remotely manage each system that has DeviceLock Service. DeviceLock ships with four different management consoles: DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager, DeviceLock WebConsole, and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor). DeviceLock Management Console and DeviceLock WebConsole are also using to manage DeviceLock Enterprise Server and DeviceLock Content Security Server. You can choose the console that best fits your needs.

Below you can find the system requirements for each part of DeviceLock DLP Suite.

The computer on which you install DeviceLock Service must meet the following system requirements:

Operating System for DeviceLock Service for Windows	Microsoft Windows NT 4.0 SP6/2000/XP/Vista/7/8/8.1/10 and Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016. Installation is supported on both the 32-bit and the 64-bit editions of the operating system. **Note:** Windows Internet Explorer version 4.0 or later must be installed on computers running Windows NT 4.0 SP 6.
Operating System for DeviceLock Service for Mac	Apple OS X 10.6.8 (Snow Leopard), 10.7 (Lion), 10.8 (Mountain Lion), 10.9 (Mavericks), 10.10 (Yosemite), 10.11 (El Capitan). Installation is supported on both the 32-bit and the 64-bit editions of the operating system.
RAM	Minimum: 512 MB.
Hard Disk Space	Minimum: 400 MB.
Processor Type	Minimum: Intel Pentium 4.
Supported Virtualization Products	Microsoft Remote Desktop Services (RDS), Citrix XenDesktop/XenApp, Citrix XenServer, VMware Horizon View, VMware Workstation, VMware Player, Oracle VM VirtualBox, Windows Virtual PC.

The computer on which you install DeviceLock management consoles must meet the following system requirements:

Operating System	Microsoft Windows 2000/XP/Vista/7/8/8.1/10 and Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016. Installation is supported on both the 32-bit and the 64-bit editions of the operating system.
RAM	Minimum: 512 MB.
Hard Disk Space	Minimum: 1 GB.
Processor Type	Minimum: Intel Pentium 4.

The computer on which you install DeviceLock Enterprise Server and DeviceLock Content Security Server must meet the following system requirements:

Operating System	Microsoft Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016. Installation is supported on both the 32-bit and the 64-bit editions of the operating system.
RAM	Minimum: 1 GB. Recommended: 8 GB.
Hard Disk Space	Minimum:1 GB. Recommended: 800 GB (if an SQL database is used).
Processor Type	Minimum: Intel Pentium 4. Recommended: 2x Intel Xeon Quad Core 2.33 GHz.
Relational Database Management Systems	Microsoft SQL Server Express 2005 or later, SQL Server 2005 or later.

To install DeviceLock, you MUST have administrative privileges.

DeviceLock uses *Remote Procedure Call* (RPC) technology for communication between the agent and the management console. By default, DeviceLock Service, DeviceLock Enterprise Server and DeviceLock Content Security Server are set to use specific TCP ports for RPC communication: 9132, 9133 and 9134 thereafter. If these ports are unavailable on the local computer, then other ports will be allocated dynamically. You can instruct DeviceLock Service to

use any other TCP port. To do so, please refer to the [Frequently Asked Questions](#) section of our website. Please note that DeviceLock doesn't rely on its own RPC communication when you are using DeviceLock Group Policy Manager. In this case, all communications are handled by Active Directory.

Choosing the right management console

- ▪ **DeviceLock Management Console** is a snap-in for Microsoft Management Console (MMC). Using DeviceLock Management Console, you can view and change the policy, install and update DeviceLock Service as well as view audit records for individual computers. Also, DeviceLock Management Console is used for viewing logs stored on DeviceLock Enterprise Server and for managing this server and work with DeviceLock Content Security Server.

- ▪ **DeviceLock Group Policy Manager** integrates into the standard Windows Group Policy Editor that comes with Windows 2000 and later. With DeviceLock Group Policy Manager, you can change the DeviceLock's policy across the entire Active Directory forest. The advantages are:

    - Ability to control DeviceLock Service on a large number of computers simultaneously via Group Policy.
    - No need to install our application-specific console for centralized management and deployment.
    - Ability to deploy DeviceLock Service's settings to new computers that are just connecting into the domain.
    - Clear and standard interface provided by Microsoft Management Console.

- ▪ **DeviceLock Enterprise Manager** can be used to control many computers simultaneously. With DeviceLock Enterprise Manager, you can view and change the policy; install, update and uninstall DeviceLock Service; and view audit records for all the computers in a large network. We recommend using DeviceLock Enterprise Manager if you have a large network without Active Directory. The advantages are:

    - Ability to control and deploy DeviceLock Service on a large number of computers simultaneously;
    - Multi Document Interface (MDI), allowing you to keep each task in its own window.

- ▪ **DeviceLock WebConsole** provides a simple and intuitive Web interface for DeviceLock Management Console and DeviceLock Service Settings Editor. With DeviceLock WebConsole, you are not limited to managing DeviceLock Service, DeviceLock Enterprise Server and DeviceLock Content Security Server from a particular machine where DeviceLock Management Console and DeviceLock Service Settings Editor have been installed. Instead, you can access and use DeviceLock WebConsole from any supported Web browser.

To get more information about management consoles, please read *[DeviceLock Manual.pdf](#)*, a documentation file that installs with DeviceLock and is also available in different languages at our website.

Deploying DeviceLock Service for Windows

There are multiple ways to deploy the agent (DeviceLock Service) to client Windows systems:

- ▪ The first and easiest way is to run *setup.exe* and select DeviceLock Service for installation. You must run *setup.exe* on each computer that is to be controlled with DeviceLock.

To install DeviceLock Service without user intervention (silent mode), you can use a special configuration file (*devicelock.ini*) to define some settings and permissions for unattended setup.

Moreover, the unattended setup allows you to deploy the agent using Microsoft System Center Configuration Manager (formerly Microsoft Systems Management Server). Use the package definition files (*DevLock.pdf* for SMS version 1.x and *DevLock.sms* for SMS version 2.0 and later) supplied with DeviceLock, located in the *sms.zip* file.

▪ Another simple way to deploy the agent is to use the remote installation function of DeviceLock Management Console. The remote installation function allows you to install or update DeviceLock Service on remote machines without ever having to physically go to them. When you're trying to connect to a computer where DeviceLock Service is not installed or is outdated, the management console suggests that you install or update it. You just need to select the directory that contains all of the files needed for installation (such as *DeviceLock Service.msi*, *DeviceLock Service x64.msi*, *DLRemoteInstaller.exe*, and *InstMsiW.exe*) and the management console deploys DeviceLock Service automatically. These files are located in the DeviceLock installation directory. By default, the DeviceLock installation directory is *%ProgramFiles%\DeviceLock*.

▪ A third way to install the agent is to use the *Install service* plug-in in DeviceLock Enterprise Manager. When you select the directory that contains all of the files needed for installation (such as *DeviceLock Service.msi*, *DeviceLock Service x64.msi*, *DLRemoteInstaller.exe*, and *InstMsiW.exe*), DeviceLock Enterprise Manager will deploy DeviceLock Service automatically on all the selected computers in your network.

▪ The fourth and the most powerful way to deploy the agent is only possible in Active Directory domains. DeviceLock Service can be deployed via Group Policy using the Microsoft Software Installer (MSI) package (*DeviceLock Service.msi* and *DeviceLock Service x64.msi*). This method will also deploy DeviceLock Service to new computers that are just connecting into the domain.

For more information regarding deploying DeviceLock Service for Windows, please read *DeviceLock Manual.pdf*.

Deploying DeviceLock Service for Mac

First of all, mount *DeviceLock Service.dmg*. There are multiple ways to install the agent (DeviceLock Service) to client Mac OS systems:

▪ The first and easiest way is to launch *DeviceLock Service.pkg* and follow the instructions that appear on the screen. You must run *DeviceLock Service.pkg* on each computer that is to be controlled with DeviceLock.

▪ A second way to install the agent is to use a command-line utility (located at */Library/DeviceLockAgent/Utilities/install* and in *Utilities* folder of *DeviceLock Service.dmg*) and install DeviceLock Service without user intervention (silent mode). Unattended installation is launched when running the installation utility with the *--silent* parameter in the command line. If the *--settings* parameter is specified in the command line, you can use a special configuration file (*devicelock.ini*) to define some settings and permissions for unattended setup.

▪ A third way is to use a command-line utility (located at */Library/DeviceLockAgent/Utilities/install* and in *Utilities* folder of *DeviceLock Service.dmg*) in the interactive mode. Interactive installation is launched when running the installation utility without the *--silent* parameter in the command line. If the *--settings* parameter is specified in

the command line, you can use a special configuration file (*devicelock.ini*) to load some settings and permissions automatically immediately after the installation.

For more information regarding installing DeviceLock Service for Mac, please read *DeviceLock Manual.pdf*.

Please note that to allow remote management via DeviceLock management consoles using local user credentials, the *Share File and Folders using SMB (Windows)* system option must be enabled for these local users on the computer where DeviceLock Service for Mac is installed.

Installing DeviceLock Enterprise Server

DeviceLock Enterprise Server uses MS SQL Server to store its data. Hence, it is necessary to have MS SQL Server installed and started in your network before installing DeviceLock Enterprise Server. If you don't have MS SQL Server, you can install the free edition called SQL Server Express Edition available for free download at the Microsoft's website.

It is not necessary to run MS SQL Server and DeviceLock Enterprise Server on the same machine. Moreover, for performance and reliability reasons, it is better to install DeviceLock Enterprise Server on a separate computer.

As soon as you prepared MS SQL Server, run *setup.exe* and select DeviceLock Enterprise Server for installation.

For more information about installing DeviceLock Enterprise Server, please read *DeviceLock Manual.pdf*.

Installing DeviceLock Content Security Server

Run *setup_dlcss.exe* and follow the instructions to install DeviceLock Content Security Server.

For more information about installing DeviceLock Content Security Server, please read *DeviceLock Manual.pdf*.