

DeviceLock® Quick Install Guide



Contents:

- [General information](#)
- [Choosing the right management console](#)
- [Deploying DeviceLock Service](#)
- [Installing DeviceLock Enterprise Server](#)

General information

DeviceLock works on any computer using Windows NT 4.0/2000/XP/Vista or Windows Server 2003/2008. It supports 32-bit and 64-bit platforms. To install and control DeviceLock, you MUST have administrative privileges.

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

1. DeviceLock Service is the core of DeviceLock. DeviceLock Service is installed on each client system, runs automatically, and provides device 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.
3. The management console is the control interface that systems administrators use to remotely manage each system that has DeviceLock Service. DeviceLock ships with three different management consoles: DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor). DeviceLock Management Console is also using to manage DeviceLock Enterprise Server. You can [choose the console](#) that best fits your needs.

DeviceLock uses *Remote Procedure Call (RPC)* technology for communication between the agent and the management console. By default, DeviceLock Service and DeviceLock Enterprise Server are set to use specific TCP ports for RPC communication: 9132 and 9133 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 permissions and audit rules, 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.

- **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 DeviceLock's settings, permissions and audit rules 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 permissions and audit rules; 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.

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

There are multiple ways to deploy the agent (DeviceLock Service) to client 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 Systems Management Server (SMS). 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 service executable file (*dlservice.exe* or *dlservice_x64.exe*) and the management console deploys DeviceLock Service automatically.

- A third way to install the agent is to use the *Install Service* plug-in in DeviceLock Enterprise Manager. When you select the service executable file (*dlservice.exe* or *dlservice_x64.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, please read *DeviceLock Manual.pdf*.

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*.