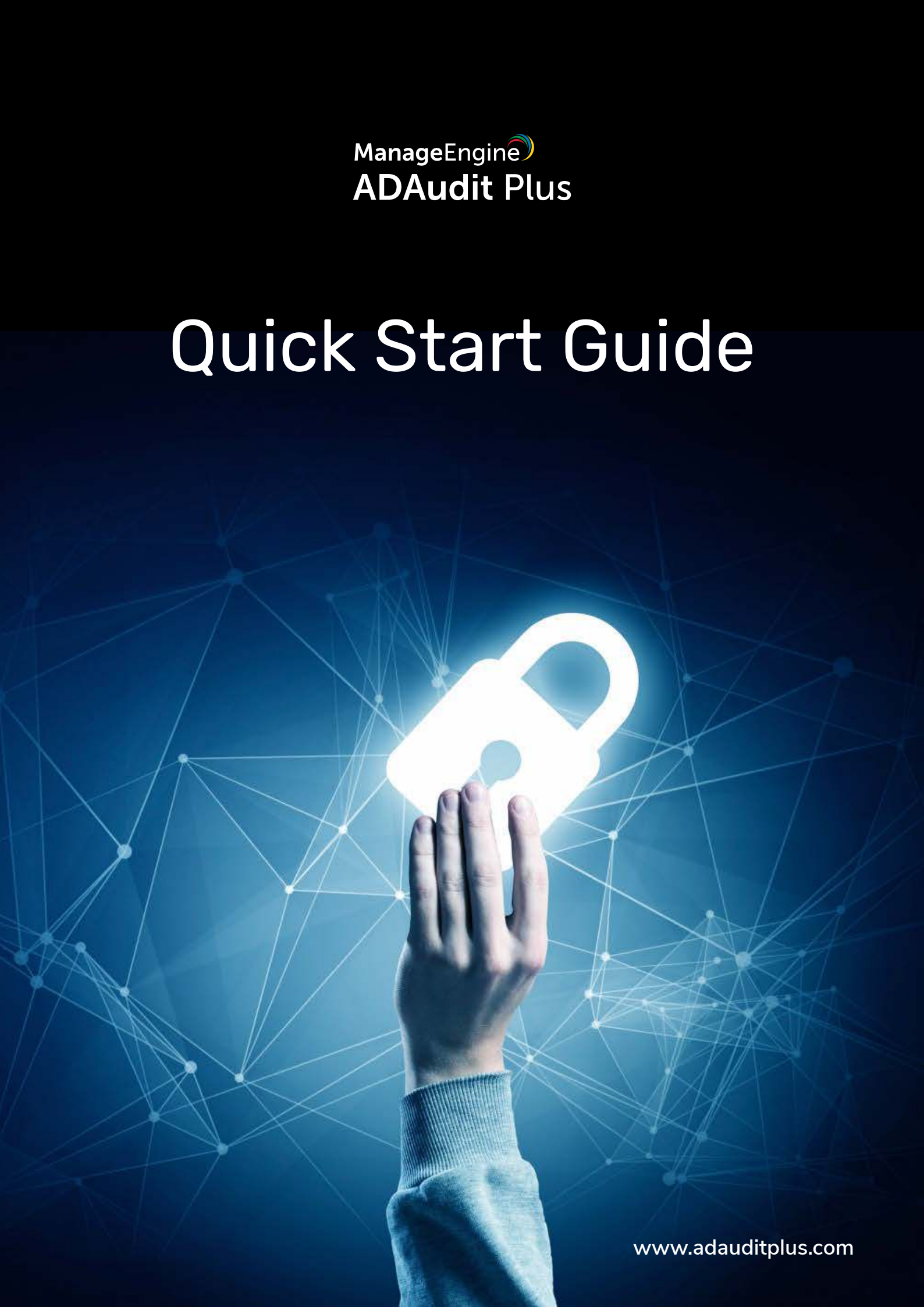
ManageEngine
ADAudit Plus

Quick Start Guide



www.adauditplus.com

Table of Contents

Document summary 1

1. System requirements 1

2. Prerequisites 3

2.1 Configuring audit policy and object level auditing 3

2.1.1 To audit Domain Controllers 3

2.1.2 To audit Windows file servers 3

2.1.3 To audit Windows member servers 3

2.1.4 To audit workstations 3

2.1.5 To audit NetApp Filers 3

2.1.6 To audit NetApp clusters 3

2.1.7 To audit EMC servers 4

2.1.8 To audit EMC Isilon 4

2.1.9 To enable File Integrity Monitoring (FIM) 4

2.1.10 To audit Group Policy Objects (GPOs) 4

2.1.11 To audit removable storage devices 4

2.1.12 To audit Windows PowerShell 4

2.1.13 To audit Active Directory Federation Service (AD FS) 4

2.2 Configuring security log size and retention settings 4

2.3 Ports to be opened 4

2.4 Setting-up a service account 5

3. Deploying ADAudit Plus 5

3.1 Installing ADAudit Plus 5

3.2 Starting ADAudit Plus 6

3.3 Launching ADAudit Plus 7

4. Configuring components in ADAudit Plus 8

4.1 Configuring domain controllers 8

4.2 Configuring file servers 8

4.3 Configuring Windows member servers 8

4.4 Configuring Windows workstations 8

4.5 Configuring cloud directory (Azure AD) 8

Related documentation 8

Document summary

ManageEngine ADAudit Plus is a user behavior analytics-driven change auditor that helps keep your Active Directory, file servers, Windows servers, and workstations secure and compliant.

This guide takes you through the basic configurations required to quickly set up ADAudit Plus for change auditing. To view the entire set of configurations, refer to the online help document.

1. System requirements

ADAudit Plus can be installed on any Windows operating system based-machine in the domain with the following system specifications.

Hardware

Resource	Minimum	Recommended
Processor	2.4 GHz	3 GHz
Core	4	6 or more
RAM	8 GB	16 GB
Disk space	50 GB	100 GB

Note: Based on the number of users and audited events captured, additional disk space might be needed.

Operating systems

ADAudit Plus can be installed and run on the following Microsoft Windows operating system versions:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista

Web browsers

ADAudit Plus requires one of the following browsers to be installed in the system.

- Internet Explorer 8 and above
- Mozilla Firefox 3.6 and above
- Google Chrome
- Microsoft Edge

Recommended screen resolution

1024 x 768 pixels or higher.

Databases

ADAudit Plus comes bundled with a default PostgreSQL database. However, MS SQL can also be used. Mentioned below are the versions supported:

- SQL Server 2019
- SQL Server 2017
- SQL Server 2016
- SQL Server 2014
- SQL Server 2012
- SQL Server 2008 R2 (EOLed by Microsoft)

Note: Follow these steps to migrate from PgSQL to MS SQL database.

Platforms

ManageEngine ADAudit Plus supports the following platforms:

- Windows Server 2003 and above
- Azure AD (Check system requirements under 'Via Office365 Cmdlet')
- AD FS 2.0 and above
- Windows workstations XP and above
- Windows File Server 2003 and above
- NetApp Filer - Data ONTAP 7.2 and above
- NetApp Cluster - Data ONTAP 8.2.1 and above
- EMC Storage Systems - Celerra, VNX, VNXe, Unity, and Isilon
- Windows Failover Cluster with SAN
- Synology - DSM 5.0 and above

2. Prerequisites

Ensure that the following settings and components are configured prior to deploying ADAudit Plus.

2.1 Configuring audit policies and object-level auditing

Audit policy settings specify categories of security-related events that you want to audit. Advanced audit policy settings help administrators exercise granular control over which activities get recorded in the logs, helping reduce event noise.
Object-level auditing settings (referred to as system access control list [SACL] in this document), log attempts to access a secured object.

Audit policies or advanced audit policies (recommended for computers running Windows 7, Windows Server 2008, and later) must be configured for computers, while object-level auditing must be configured for secured objects to ensure that security-related events get logged whenever any relevant activity occurs.

Note: The required audit policy and object-level auditing settings can be configured automatically via the ADAudit Plus console, by following the steps found under the Automatic configuration section in each of the links found below.

2.1.1 To audit Active Directory:

1. Configure the Default Domain Controller policy.
2. Configure object-level auditing.

2.1.2 To audit Windows file servers:

1. Configure audit policies for the Windows file servers that need to be audited.
2. Configure object-level auditing for the shares that need to be audited.

2.1.3 To audit Windows member servers:

1. Configure audit policies for the Windows servers that need to be audited.

2.1.4 To audit Windows workstations:

1. Configure audit policies for the Windows workstations that need to be audited.

2.1.5 To audit NetApp Filers:

1. Configure audit policies and SACLs for the NetApp Filers that need to be audited.

2.1.6 To audit NetApp clusters:

1. Configure audit policies and SACLs for the NetApp clusters that need to be audited.

2.1.7 To audit EMC servers:

1. Configure audit policies and SACLs for the EMC servers that need to be audited.

2.1.8 To audit EMC Isilon:

1. Configure audit policies and SACLs for the EMC Isilon nodes that need to be audited.

2.1.9 To enable File Integrity Monitoring (FIM):

1. Configure audit policies for the domain controllers, Windows servers, and Windows workstations on which file integrity needs to be monitored.
2. Configure object-level auditing for the shares that need to be audited.

2.1.10 To audit Group Policy Objects (GPOs):

1. Configure the Default Domain Controller policy.
2. Configure object-level auditing.

2.1.11 To audit removable storage devices:

1. Configure audit policies for the domain controllers, Windows servers, and Windows workstations on which removable storage activity needs to be audited.

2.1.12 To audit Windows PowerShell:

1. Configure audit policies for the domain controllers, Windows servers, and Windows workstations on which PowerShell activity needs to be audited.

2.1.13 To audit Active Directory Federation Service (AD FS):

1. Configure audit policies for the domain controllers and Windows servers on which AD FS activity needs to be audited.

2.2 Configuring security log size and retention settings

Security log size and retention settings must be configured to prevent loss of audit data due to overwriting of events.
Follow these recommendations to configure appropriate security log settings.

2.3 Ports to be opened

Ports must be opened to allow exchange of data between computers.
Here is the list of default ports used by ADAudit Plus and the ports that should be opened on the destination computers.

2.4 Setting-up a service account

After the Domain Admin credentials are entered, ADAudit Plus starts to audit activities.
If you do not want to provide Domain Admin credentials, follow these steps to set up the service account to have only the least privileges required for auditing your environment.

3. Deploying ADAudit Plus

ADAudit Plus is distributed in the EXE format. It is available in 32-bit (ADAudit Plus.exe) and 64-bit (ADAudit Plus_x64.exe) versions for download.

3.1 Installing ADAudit Plus

ADAudit Plus can be installed on any Windows operating system based-machine in the domain with the specified system requirements.

When you install the product, the Professional Edition is loaded, and will work for 30 days. After 30 days, it will automatically revert to the Free Edition, unless the Standard or Professional Edition license is purchased. Check out the various editions of ADAudit Plus.

ADAudit Plus can be installed as an application, or as a Windows service.

3.1.1 Installing ADAudit Plus as an application

By default, ADAudit Plus gets installed as an application. Once you've downloaded and launched the .exe file, follows these steps to install ADAudit Plus:

1. In the InstallShield Wizard that opens, click **Next.**
2. Read the License Agreement, and click **Yes.**
3. Choose the destination folder for installation files, and click **Next.** By default, ADAudit Plus is saved in C:\Program Files (x86)\ManageEngine\ADAudit Plus.
4. Enter the port number that you wish to use for ADAudit Plus, and click **Next.** By default, ADAudit Plus uses port number 8081.
5. Sign up for technical support by providing your business email ID, and click **Next.** You can choose to skip this step.
6. Click Next again, to begin installation. This process will take a few minutes. Once installation is complete, click **Finish.**

Note: When ADAudit Plus is installed as an application, it runs with the privileges of the user who is logged on to the system.

3.1.2 Installing ADAudit Plus as a Windows service (Recommended)

Installing ADAudit Plus as a Windows service is recommended to ensure that event collection does not stop even after a user logs out.

To install ADAudit Plus as a service from the Command Prompt:

After the product is installed, go to <Installation directory>\bin, open an elevated Command Prompt (right-click Command Prompt and select **Run as administrator**), and execute **InstallNTService.bat**

To install ADAudit Plus as a service from the Start menu:

After the product is installed, go to **Start menu > Programs > ADAudit Plus > NT Service > Install ADAudit Plus Service.**

Note: When ADAudit Plus is installed as a Windows service, ADAudit Plus runs with the privileges of the service account provided in the Domain Settings tab, within the product console. Follow these steps to set-up the service account with only the least privileges required for auditing your environment.

3.2 Starting ADAudit Plus

ADAudit Plus can be started as an application or as a Windows service.

3.2.1 Starting ADAudit Plus as an application

After installing ADAudit Plus as an application, go to **Windows > ADAudit Plus > Start ADAudit Plus server.**

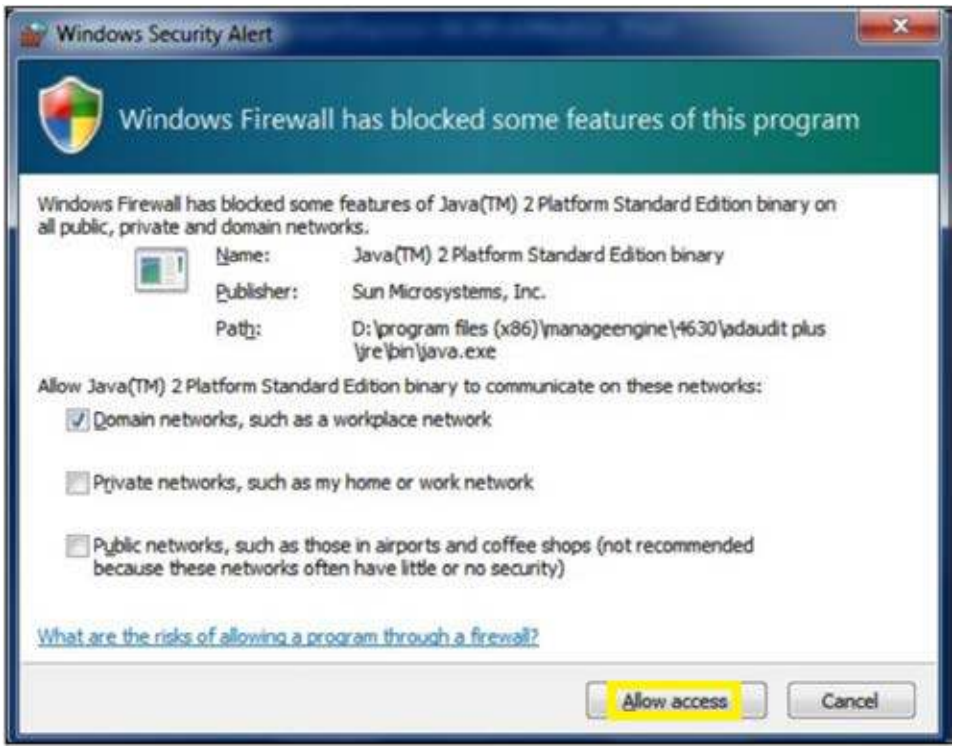
3.2.2 Starting ADAudit Plus as a Windows service

After installing ADAudit Plus as a service, go to **Windows > Services** > Right-click on **ManageEngine ADAudit Plus > Start.**

Note: When ADAudit Plus is started in Windows 8/7/Vista/XP/Windows 2012/2008 R2/2008/2003 machines with firewall enabled, Windows may display a security alert, asking whether to allow access to the following programs:

- Database Server
- Java(TM) 2 Platform Standard Edition binary

Click on **Allow access** to start ADAudit Plus.



3.3 Launching ADAudit Plus

1. Open a web browser and type **http://<hostname>:<port number>** in the address bar.
   The hostname is the DNS name of the machine where ADAudit Plus has been installed, and the port number is the web server port number that was specified during the installation of ADAudit Plus. The default port used by ADAudit Plus is 8081.

2. Specify the user name and password as **admin** (for first time users) in the respective fields and click **Login.**

Note: After launching, ADAudit Plus automatically discovers the local domain and the domain controllers running in it. Login to ADAudit Plus web console > **Domain Settings** > **Configure** > Provide Domain Admin credentials, to start auditing. You can select the necessary domain controllers by clicking on the respective check boxes.
If you do not want to provide Domain Admin credentials, follow these steps to set-up the service account with only the least privileges required for auditing your environment.

In case automatic discovery fails, follow these steps to manually add the required domain and domain controllers.

4. Configuring components in ADAudit Plus

4.1 Configuring domain controllers.

4.2 Configuring file servers.

4.3 Configuring Windows member servers.

4.4 Configuring Windows workstations.

4.5 Configuring cloud directory (Azure AD).

Related documentation

- ADAudit Plus help document details the entire set of configurations related to ADAudit Plus.
- ADAudit Plus architecture details how ADAudit Plus works.
- Database migration guide covers the steps to:
    - Move DB and/or data from PostgreSQL/MySQL to MS SQL.
    - Move DB and/or data between two different versions of MS SQL.
    - Move DB and/or data from MySQL/MS SQL to PostgreSQL.
    - Move ADAudit Plus from one server/drive to another.
    - Move ADAudit Plus from 32-bit to 64-bit architecture.
- Agent installation guide covers the steps to install agents on target computers to enable agent based log collection.
- SSL configuration guide covers the steps to enable SSL in ADAudit Plus to secure communication between the users' web browsers and ADAudit Plus.
- Security hardening guide details the recommended ways to configure ADAudit Plus to ensure that your data stays secure.
- ADAudit Plus pricing covers information about pricing and editions available.