ManageEngine
ADAudit Plus

Security hardening for ADAudit Plus

www.adauditplus.com

Table of Contents

Abstract

With the increasing amount of attention on information security, it is essential for all IT administrators to strengthen security within their existing infrastructure to avoid possible breaches. This document focuses on the best ways to configure ADAudit Plus to ensure that your information stays secure.

Security hardening for ADAudit Plus

1. Following the principle of least privilege

An Active Directory (AD) user account is generally associated with ADAudit Plus for the collection of logged data. If a domain administrator account is used, ADAudit Plus instantly starts auditing changes within your AD environment. But, in general, a domain administrator account has several elevated rights and privileges not required by ADAudit Plus. This is why we recommend creating dedicated user accounts that only have the privileges and permissions needed for ADAudit Plus to perform its job. This way, even if a dedicated user account is compromised, the impact of the breach is innately contained. Here are the required privileges and permissions for ADAudit Plus.

2. Securing the built-in admin account

ADAudit Plus comes with a built-in admin account with ultimate privileges. By default, this account's password is the same for every customer of ADAudit Plus, which means you need to change this password in order to properly secure it. If this step is overlooked, you will leave your system vulnerable.

3. Enabling HTTPS for secure communication

We recommend that you use HTTPS over HTTP to ensure secure transportation of information over your network. You can do this from within the user interface under the Admin tab. Navigate to the settings found under General Settings > Connection.

These settings can be further optimized from within the following XML file:

- conf\server.xml > connector (find the HTTPS connector corresponding to your configured port number).

If you choose to allow only a particular version of Transport Layer Security (TLS), namely TLSv1, TLSv1.1, or TLSv1.2, you can disable the other versions by modifying the following parameter, keeping only the required TLS versions:

- sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"

If you want to disable or restrict ciphers, you can do so by modifying the following parameter to only contain the required ciphers:

- ciphers = "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256,
  TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_RSA_WITH_AES_256_CBC_SHA"

With these changes, you can secure all communication through ADAudit Plus and strengthen security.

4. Restricting logon access to the ADAudit Plus server

To further strengthen ADAudit Plus' security, we recommend that you restrict logon access to the ADAudit Plus server, thereby preventing unwarranted access. You can define the local policy settings in the User Rights Assignment tab within the Group Policy Management Editor to Allow log on locally or Allow log on through Remote Desktop Services, only to a specific set of users. This way, you reduce the attack surface of your infrastructure.

5. Restricting access to the ADAudit Plus installation folder

Administrators can restrict access to the ADAudit Plus installation folder by modifying folder permissions. This ensures that no one except permitted users have access to ADAudit Plus' files.

6. Auditing for changes to ADAudit Plus' installation folder

ADAudit Plus enables change logging of its installation folder by configuring the System Access Control List (SACL). Any changes made in this folder are then presented as reports to ensure file integrity. This way, you can be sure that no one has tampered with the information.

7. Securing your database with additional password protection

ADAudit Plus comes with a built-in, password-protected PostgreSQL database, allowing only authorized personnel access. By default, the PostgreSQL service creates a user account with unrestricted privileges—similar to a domain administrator account in AD—to perform various administrative actions. ADAudit Plus changes the default password of this account and creates another user account with limited privileges. This new account has restricted permission, is used to connect to the database, and is encrypted to ensure security.

8. Delegating and auditing technicians

Technician roles can be configured to limit access to certain reports. These roles can also restrict technicians from performing administrative functions such as adding or removing servers for auditing, modifying configuration settings, etc. In addition, ADAudit Plus provides a detailed user-based audit trail of all actions performed.

9. Securing data transfer over the network

For collecting event logs, ADAudit Plus lets you choose between the following event fetch modes:

- Real-time mode
- Native mode
- EvtQuery mode
- WMI mode

By default, Real-time and EvtQuery modes encrypt data transferred over the network. The WMI and the Native modes, by default, do not encrypt transferred data, but encryption can be enabled on the WMI mode for enhanced security. We recommend that administrators use the Real-time mode to ensure secure data transfer and to get instant updates on all AD changes.

10. Restricting database access from within the UI

ADAudit Plus, by default, disables database access from within its user interface and permits only the default administrator account to enable this option. The administrator can also choose which accounts have this privilege. This prevents other technician accounts from modifying or deleting information from the database.

11. Securing archived data

In order to reduce storage space consumption within the database, historical data can be compressed and stored separately. These files can then be restored at a later point in time. These archived files are password protected by ADAudit Plus to ensure security. For an additional layer of security, we recommend that you restrict access to the folders containing these files.

12. Protecting exported and scheduled reports

When a user exports a report in a particular format (PDF, CSV, etc.), or when a user schedules a particular report to be saved locally, the files are password protected by ADAudit Plus. It's also recommended that you modify the folder permissions for the folder that contains these files to prevent unwarranted access.

13. Using LDAP over SSL

ADAudit Plus allows administrators to enable Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL) to ensure that all communication of Active Directory data is encrypted. This can be performed from within ADAudit Plus' user interface under Connection settings.

Need help?

If you have trouble configuring any of the above mentioned settings, please contact us at support@adauditplus.com. You can also schedule a free personalized demo to receive expert guidance on tightening up your IT infrastructure's security.

The full scope and capabilities of ADAudit Plus

ADAudit Plus is a web-based, real-time Active Directory (AD) change auditing tool that helps you:

- Track all changes to Windows AD objects including users, groups, computers, GPOs, and OUs.
- Monitor every user's logon and logoff activity, including every successful and failed logon attempt across network workstations.
- Audit Windows file servers, failover clusters, NetApp, and EMC storage to document changes to files and folders.
- Monitor system configurations, program files, and folder changes to ensure file integrity.
- Track changes across Windows servers, printers, and USB devices with a summary of events.

To learn more about how ADAudit Plus can help you with all your Active Directory auditing needs, please visit: manageengine.com/products/active-directory-audit.