ManageEngine
ADAudit Plus

Security specifications of ADAudit Plus to help you meet all your Active Directory reporting and alerting needs.

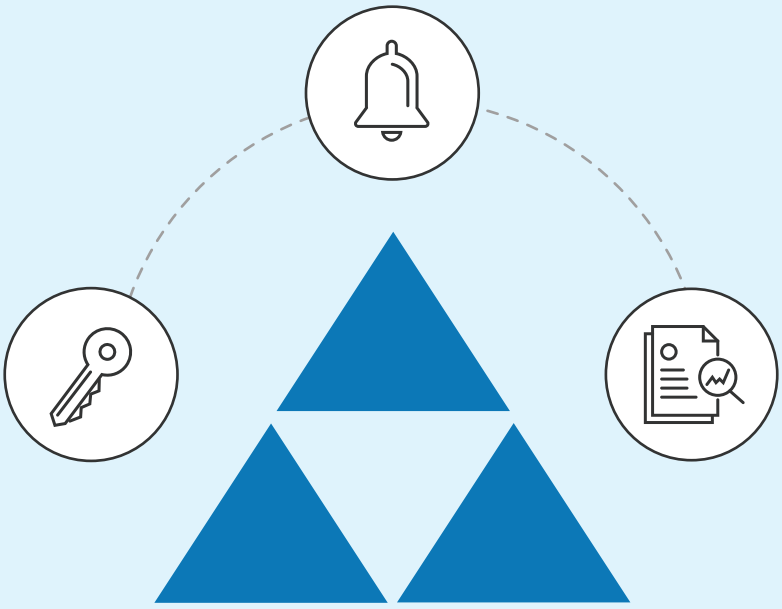

Table of Contents

Abstract

With the rise in stringent laws and reforms on one hand and huge financial losses due to data breaches on the other, security hardening has become a mandate. It is thus inevitable that software companies ensure that the products they make can withstand malicious attacks and comply with IT security standards. ADAudit Plus is designed with this in mind. This document focuses on the various security specifications of ADAudit Plus.

Potential vulnerabilities of web applications

1. Third Party interception:

If the client-server communication is not secure, then anyone in between can intercept the data being exchanged in 'plain text' leading to a "Man in the Middle" (MITM) attack. This can result in confidential data, such as usernames and passwords, being obtained. A person being attacked might not even be aware of such an intrusion. Meanwhile the attacker can save a copy of the data for a later exploit.

2. Port Vulnerability:

While it's necessary for some ports to be open to internet traffic, it's also standard practice to ensure that only the bare minimum ports are exposed. If data is sent using HTTP, your data is vulnerable and can be exploited by stealing passwords, eavesdropping, and attacks of the like. The intrusion of malicious software can open unwanted ports and close the ones that's are essential. This allows an intruder to carry out botnet attacks, denial of service, etc. To counter these attacks, firewalls should be configured accordingly to restrict communication only to the ports in use. It is also advisable to use HTTPS while communicating confidential information over the network, as the attacker would need the secret key to decrypt any information he captures over the network.

3. Password compromise and data breaches due to a poor password policy:

If logon credentials are bypassed then attackers can gain access to virtually everything that the end user does including viewing the whole webpages, stealing cookies such as auto fill form data, browsing history etc, and even hijacking Windows accounts rendering them inactive but for a trade-off. Weak passwords can be easily compromised. Brute force attacks are when an automated application by a hacker makes multiple guesses (by permutations and combinations) to compromise weak passwords.

A strong password, (i.e.) that is long and has a complex combination of alpha, numeric and special characters make it difficult for hackers to hack passwords. If a company's network-attached storage (such as servers) is accessible without a password, or data is accessible between computers on a network without the need for authentication, huge volumes of records could be stolen. If a strong password policy is not in place, it can cause an irreversible loss of corporate data.

4. Malicious code injection by hackers:

Bugs in network related software can be exploited by breachers for injection of malicious codes. This is called cross site scripting. This allows for a backdoor entry for hacking vectors which, once installed, allows remote code execution that can disrupt normal services, steal your credentials and/or cause your system to be part of series of botnet attacks on other computers in the network.

ManageEngine's ADAudit Plus takes utmost care to ensure that it is secure from potential vulnerabilities. Following are the specifications of ADAudit Plus which hardens security against various attacks to prevent data breaches.

Security specifications of ADAudit Plus

1 Secured communication over HTTPS

ADAudit Plus helps in a secured gateway communication, allowing servers to communicate using HTTPS protocol. Since corporations deal with confidential data, it is essential that the HTTPS protocol is in place. When you choose secured communication, ADAudit Plus chooses HTTPS ports over insecure ports. The appropriate changes need to be made to the firewall to only allow HTTPS port and disable the other ports. The ADAudit Plus console thoroughly validates all inputs in the GUI. Usage of special characters and HTML code are filtered, and the application is guarded against common attacks like SQL injections, cross-site scripting, Cross site request forgery (CSRF), buffer overflows and other attacks. A secure HTTPS connection and the SSL certificates help in preventing MITM attacks by placing an overcoat of encryption to the data exchanged. This secure connection can be used to forward logs to your SIEM solution to prevent possible exploits. Also, ADAudit Plus allows users to use secure connections(SSL/TLS) while configuring SMS/mail servers, NetApp and EMC storage.

2 Secured Socket Layer (SSL) Certificates

For an added layer of security over HTTPS, ADAudit Plus provides for a certificate based encryption between machines in the network. Users can import third party SSL certificates in ADAudit Plus which encrypts all data transferred between clients and servers. This rules out the possibility of an intercepting attack. Even if an attacker gains intermediate access, he wouldn't be able to make much of the information without the key to decrypt it. However, communication might not be secure post expiry of certificates.

3 Securing the ports used for Communication

As ADAudit Plus is a complete agentless solution and does not use any proprietary technique, although standard Windows ports need to be opened for event log collection. This includes the standard RPC, WMI, SMB ports and a few dynamic ports used for communication. All other ports can be disallowed thereby strengthening security.

4 Secure Authentication: Password policy

ADAudit Plus supports two methods of authentication – Active Directory authentication and ADAudit Plus authentication. Users can log on using their AD credentials or credentials created via ADAudit Plus. ADAudit Plus provides a lockout policy to protect ADAudit Plus users against brute force attacks. For AD authentication, the pre-defined AD policies become applicable.

5 Encrypted password storage

ADAudit Plus uses the AES 256-bit algorithm for encrypting passwords when storing them in the PostgreSQL database. This ensures that password information always stays secure.

6 Windows Active Directory Authentication

With the increase in software applications, each with their own authentication and password complexity levels, it becomes very difficult to remember all passwords. Active Directory's authentication and capabilities can be extended to ADAudit Plus letting users log on with their AD credentials. The database constantly synchronizes with the directory, and is automatically updated whenever users are added or removed in AD. This will greatly minimize the risk of unauthorized users accessing ADAudit Plus' web interface. The scope of authorization for users is dealt with in "Role Based administration"

7 Role based Administration

In mid-size and larger networks, it is unlikely for a single person to manage the entire systems administration. ADAudit Plus helps overcome this concern using its 'Role Based Administration' module. This 'Role Based Control' feature not only helps the administrator share his work but also adds an additional layer of network security by restricting system access only to authorized personnel. Tailor-made roles such as Guest, Technician, Auditor, etc. can be created and given customized access permissions (read, write, no access, full control) based on your requirement.

8 Secure reading of event logs

ADAudit Plus needs access to Windows Event Viewer to read and collect logged data in order to process logs into graphs and reports. ADAudit Plus collects logs only if the account associated with it is authorized to do so. This data is then encrypted and communicated securely. Additionally, ADAudit Plus supports LDAP over SSL (LDAPS) certificates for secure communication of Active Directory data.

9 Demilitarized Network Security

Certain networks are kept totally disconnected from the internet to be capsuled from hacks. ADAudit Plus supports auditing of servers residing in DMZs provided the RPC secure ports are kept open. This ensures that all events in your network are collected and reported on, including servers in DMZs.

10 Securing notification endpoints

ADAudit Plus uses TLS/SSL to provide secure communication on the internet for email notifications. Its also employs the HTTPS protocol for SMS notifications. This way the information cannot be intercepted by hackers and stands to enhance overall network security.