ManageEngine
EventLog Analyzer

Enabling Active Directory authentication in EventLog Analyzer for PCI DSS compliance

Requirement 8 of the PCI DSS deals with identifying and authenticating access to system components. For example, requirement 8.1.4 requires inactive user accounts to be disabled within 90 days. These identity and access management requirements listed under clause 8 can be met in EventLog Analyzer by enabling Active Directory (AD) authentication for logging into the application. By doing so, you'll be extending all the password policies and configuration of AD to EventLog Analyzer's access.

EventLog Analyzer technicians

For a user to access and manage EventLog Analyzer, they must be added as a technician to EventLog Analyzer and assigned a role, which defines their privileges. EventLog Analyzer has three predefined roles for its technicians—Admin, Operator, and Guest. The technicians may be created either locally or imported from Active Directory.

Active Directory based authentication

In addition to local authentication for technicians (users created within the product's console), EventLog Analyzer also supports Active Directory based authentication. Active Directory authentication can be enabled for technicians imported from Active Directory to allow them to log into the EventLog Analyzer console using their domain credentials. EventLog Analyzer automatically discovers and displays Active Directory users from the selected domain. Users can be searched and added based on their groups and OUs.

For prospects or customers who use EventLog Analyzer to meet and prove their PCI DSS compliance, we recommend disabling local authentication and enabling Active Directory based authentication so that the identity and access management policies and configurations set in Active Directory is extended to EventLog Analyzer's authentication.

Steps to enable AD authentication

For a user to access and manage EventLog Analyzer, they must be added as a technician to EventLog Analyzer and assigned a role, which defines their privileges. EventLog Analyzer has three predefined roles for its technicians—Admin, Operator, and Guest. The technicians may be created either locally or imported from Active Directory.

- Login to the EventLog Analyzer web console as an administrator. First time users can login using 'admin' as both the username and password.
- Navigate to Settings tab > **Admin Settings.**
- Active Directory based authentication can be enabled by clicking on the **External authentication** icon in the **Technicians and Roles** section.

Note: EventLog Analyzer also supports Remote Authentication Dial-in User Service (RADIUS) server authentication. This will allow technicians to logon to EventLog Analyzer by authenticating with the configured RADIUS server.

Disabling the local technician account

We recommend using only AD based authentication for EventLog Analyzer in order to implement identity management related requirements such as password policy, account lockout policy, and the removal of inactive users.

After importing a user from AD and enabling AD authentication, you can delegate the 'admin' role to that technician in the **Technican and Roles** page. Then, in the same page, the default local admin account can be selected and disabled.

Contact support for more details

For further details, please contact support: support@eventloganalyzer.com