Secure LDAP mandatory for Active Directory connections (Microsoft Security Advisory ADV190023)

Applies from Application Suite 201x (any version)
to version Application Suite 201x (any version)

Description

As of March 2020, Microsoft is updating security requirements for LDAP connections to Active Directory.
After this update, Secure LDAP (LDAPS) will become mandatory for all LDAP connections to Active Directory.
LDAP connections to Active Directory will not work unless Secure LDAP is configured.
By March, all LDAP configurations must be configured to use secure LDAP for LDAP connections to Active Directory.
In addition, the Active Directory server must be updated with the new security updates that Microsoft requires.
If you do not make these updates, LDAP connections to Active Directory will not work.

Cause

The existing default settings have a vulnerability that may expose Active Directory domain controllers to an elevation of privileges, and man-in-the-middle attacks.
The Secure LDAP updates harden the connection to Active Directory's existing LDAP channel binding and LDAP signing mechanisms, making the system more secure.
For more detailed information, refer to the Microsoft Security Advisory ADV190023:

Solution

1. Configure the users sync with external sources (LDAPS/AD) following our guide:
   Active Directory Secure Connection
2. Configure LDAP/AD users authentication to use LDAP/AD SSL protocol
   How to authenticate LDAP users logging in the Imagicle Application Suite web interface using LDAP SSL protocol

Secure LDAP mandatory for Active Directory connections (Microsoft Security Advisory ADV190023)