LDAP/AD Product FAQ

From the release of version 9.3 in October 2020, the GateManager includes support for LDAP user validation. This is our first implementation of LDAP that addresses the mandatory requirements of all implementations of LDAP validation of GateManager users.

However, the expectations for the ideal LDAP and AD functionality highly depend on the IT infrastructure and strategy of each specific company. Accommodating all such potential strategies and desires would be a huge development effort, which conflicts with our Agile principles of building the essential functionality necessary to provide value fast.

This document addresses the most common questions related to LDAP/AD integration with Secomea.

Contents

Revision 1.2 – 2020-09-11

1. What’s the difference between LDAP and AD?

Directory Services means a database system that provides authentication, directory, policy, and other services in an IT environment.

LDAP (Lightweight Directory Access Protocol) is an application protocol for querying and modifying items in directory service providers, which supports a form of LDAP.

Third party LDAP directory servers do exist (such as IBM Tivoli), but Microsoft Active Directory is by far the most used directory service, which supports LDAP.

Short answer: AD is a directory services database of Microsoft, and LDAP is one of the protocols you can use to talk to it.

2. How is the current GateManager implementation best described?

The LDAP integration in GateManager allows you to select external validation for accounts or account roles. This selection can be for individual accounts, or server wide for specific account roles. The process is as follows:

1. If “external validation” is selected for an account, the GateManager will start a script based on the username of the account and the credentials entered by a user. (If the account is combined with Certificate or SMS, then the GateManager will validate that as part of the authentication process)
2. The script will communicate via LDAP to an Active Directory to have the username and password validated.
3. If the user exists in the AD and the password is correct, the script will return a positive acknowledgement to the GateManager.
4. The GateManager will then consider the user properly authenticated and log the user in.

The script is an integral part of the GateManager 9.3 release, but it must be customized to communicate with the specific LDAP or AD server instance. In the first version this must be done with the assistance of our presales department.

3. Do we support LDAP on our shared cloud servers?

No. The implementation is for GateManager Own only, as the script is general for the entire server and toward a single LDAP/AD server. Most Secomea customers requiring external user validation also prefer their own GateManager.

4. Does the GateManager server require a special license for activating LDAP?

No. Any activated GateManager Own will in principle support LDAP, but we will only provide customized instructions and additional support for customers entering a service level agreement (SLA). These customers will then also have the full benefit of future enhancements of the LDAP implementation.

5. Can we combine LDAP validated users and non-LDAP validated users?

Yes, you can specify individual accounts to be externally validated, or you can set a server wide policy per account role, i.e. Server admins, Domains admins, LinkManager and LinkManager Mobile. E.g. if the LinkManager role is specified server wide for external validation only, then a LinkManager account cannot be created for local validation.

We have until now seen two use-cases for combinations of external and internal validation:

A. The Server admins that maintain the GateManager are internal employees that should be AD controlled, so that you can revoke access centrally if they leave the company. The Domain admins and LinkManager users, however, are external users (consultants) that should not be controlled by the corporate AD. This scenario is typical for shared cloud servers or for a server of an OEM providing access to end customers.

B. The Server admins have special authority that should not rely on the AD, while all regular users, such as LinkManager users, should be controlled by the AD. This scenario is seen for factory sites where access is primarily for the factory's own employees.

6. Do we have support for MS Azure based AD?

Yes, but you need to enable LDAP on the Azure AD domain services instance. This is not enabled by default. By default, Azure AD assumes you are running a clean MS based infrastructure.

Note that Microsoft claims that LDAP (or Secure LDAP) is not supported in Azure AD, but it is possible to achieve LDAP connectivity by enabling Azure AD Domain Services (Azure AD DS), and then configuring network security groups through Azure Networking.

7. Why don't we validate directly toward an AD without LDAP?

LDAP is the way for a non-MS based platform to validate against AD, so there are really no other viable options. Unless using RADIUS (Remote Authentication Dial-In User Service), which in some cases can be an alternative to LDAP.

8. Why would a customer request AD validation, but without using LDAP?

It may be because some customers expect a clean MS environment, or that enabling LDAP requires more work, especially for advanced functionality such as Single Sign On (SSO) and authorization control from the AD.

9. Some customers mention Single Sign On (SSO). Do we support that?

No, it would require the GateManager login portal to be an integral part of the AD sign on process (The SSO topic is mentioned later).

10. Does the LDAP implementation support 2FA?

Yes. But how "officially" it is supported depends on whose 2FA implementation we are talking about.

A. If using the **GateManager SMS 2FA authentication**, then by default yes. If the account is specified to use SMS and has a valid mobile number, the GateManager will generate and send the SMS code to that mobile number *after* the validation of the username and password has been validated via LDAP.
An experimental feature in GateManager 9.3 is that if the LDAP script returns a mobile number (or email address) in the "2FA_ADDR" field along with the positive validation, then GateManager will generate and send an SMS code to that number or email (instead of what may be specified in GateManager itself) – and do so even if the login method used by the account does not specify SMS validation.

B. If using the **Microsoft two factor SMS validation**, then officially no. There is, however another experimental implementation in GateManager 9.3: if the LDAP script returns a PIN in form of a "N" digit number in the "2FA_PIN" field, the GM will prompt the user to enter an SMS code and check that the code entered by the user, matches the PIN received from the AD.

C. If using **Microsoft two factor APP authentication**, then in principle yes. As it will be completely invisible to the GateManager and the LDAP script that the AD is authenticating the user via the APP. The assumption is that when the script delivers the username and password to the AD, the AD will in turn initiate an APP validation. Not until the user has successfully authenticated via the APP, the AD will return a successful validation acknowledgement to the script.

11. Can the GateManager certificate-based login be combined with LDAP authentication?

Yes. Currently accounts must be created in the GM manually, and if the account is created with Certificate/Password, then the GM will validate the certificate and use it to look up the username. This with then be fed, together with the password, to the LDAP script.

12. What topics or features are Secomea considering for the future?

Note that the following are still subject for research and does not reflect a roadmap.

A. **Single Sign On (SSO) authentication.**
It would be more realistic to look at integrating remote access into a native UI platform of an enterprise, similar to what we are planning for DCC in 2021; i.e. to embed web or VNC access capabilities into a custom dashboard using the LinkManager Mobile API. In principle this could be extended to LinkManager access also, although it would be a separate project.

B. **MS 2FA authentication.**
See topic "Does the LDAP implementation support 2FA?" above. Note that some of above defined 2FA functionality scenarios are still experimental and may have to be further refined and tested to assure reliability and fault tolerance.

C. **Users created/deleted in AD to be automatically created/deleted in GateManager.**
This requires some sort of bidirectional synchronization.
NOTE: The GateManager CRM API supports this, so it would be possible to write a middleware application to manage this as a supplement to the LDAP feature.

D. **GateManager to authorize user without live connection to the AD**
Currently the GateManager needs real-time access to the AD. If this connection breaks, no externally authenticated users can login. Other LDAP enabled applications handle this by holding a replica of the user database. In principle, it would be possible to build logic for the LDAP script to at least cache user credentials from previous successful logins (e.g. by mapping username and account role to hashed password), and verify logins against that in case it cannot connect to the LDAP server. The concern is that if a user is revoked from the AD while offline, the user will still be able to login to the application until next synchronization with the AD.

E. **AD group association reflecting the Account role (LinkManager, Domain admin etc.)**
The idea is that a user must be authorized by its association to a specific AD Security Group (e.g. named "LinkManager"), for the AD to return a positive response on a LDAP validation

request. It might be a manageable project to apply this (at least experimentally), as the LDAP script retrieves the account role (e.g. "LMU" for a LinkManager User) from GateManager. So, the script could map this to an AD security group and send it along with the user credentials, the AD would reject the request if the user is not member of the security group with that name. Alternatively, the AD would return the user group name to the GateManager to have the LDAP script check against the account role. However, we need a closer dialogue with customers to understand the exact expected outcome.

F. **AD User Group association reflecting access to specific GateManager Domains**
Although some of the principles explained above could be used, this is more complex as a GateManager user can be associated with (joined to) several domains. If every domain should correspond to a specific AD Security Group, it may be complex to maintain (at least on the AD side). So, we are in the process of assessing the use cases and expected outcome.

13. Do other options exist that supplement the LDAP features?

As indicated above the GateManager CRM API can administer users, like:

A. Create user
B. Delete user
C. Change role of user
D. Move a user to another domain
E. Join a user to other domains

In addition to this, the CRM API can:

A. Create domains
B. Delete domains
C. Assign license to SM-E
D. Move a SiteManager to another domain

So, a lot of possibilities exist for applying added authorization features and external control, by writing a suitable middleware application.