Active Directory FAQ

Active Directory FAQ

Q). Are there any changes required to the AD schema or extensions?

A). No

Q). Can you change a username within AD and how will Swivel treat the user?

A). If you change the username, it will be treated as a new user. You can move the account within AD, and you change other attributes, but the username cannot be changed.

Q). Can PINsafe read users from Active Directory groups?

A). Yes. Groups are used in Active Directory to specify only the users that are required for PINsafe authentication, thus licenses are only required for the number of users to be used rather than the total number of Active Directory users.

Q). Can PINsafe read multiple AD servers and Multiple AD groups?

A). Yes, as well as multiple LDAP and SQL data sources.

Q). With Active Directory is there any User configuration in PINsafe?

A). No, most information is imported from AD. Users are added and removed in Active Directory.

Q). Can A User sign on with their Active Directory Password?

A). PINsafe integrates to read Active Directory Usernames but will define its own PIN number and password (if a password is required). PINsafe can check the password entered against the repository (AD) server, but the AD password is not stored in PINsafe.

Q). Is there any software to install on the AD server?

A). No

Q). Can we move PINsafe or the AD server without new PIN numbers being issued?

A). Yes. Users will not receive new PIN numbers provided that:

Their username is the same

The PINsafe option Ignore FQ Name is set to Yes

There is no synchronisation during the AD group re-configuration

Q). Can PINsafe read the Global Catalogue

A). Yes. If the AD server is configured with Global Catalogue, then PINsafe can read this to access multiple AD domains, instead of connecting to each AD domain individually.

Q). Can we create more than 3 user groups?

A). Yes, creating a new group adds another empty configuration below so you can add additional groups.

Q). What would happen if the user mobile phone number is added later to the user in Active Directory?

A). This would be detected by PINsafe on the next synchronisation and the user would be sent a security string, if they were configured as a dual channel user.

Q). How long does the AD synchronisation take place?

A). There are a lot of contributing factors that can impact this, such as AD server load, the number of AD users being synchronised, the information required, Global catalog etc. However a typical synchronisation of 2500 users would in practice take around 30 seconds.

Q). How often does PINsafe synchronise with AD?

A). This is configurable, the usual time that is used for synchronisation is every hour.

Q). How many AD Domains can PINsafe synchronise with?

A). There is no upper limit in PINsafe, although managing large numbers of AD domains could present a challenge.

Q). Does PINsafe support nested AD groups, and if so how many levels?

A). Yes PINsafe supports nested groups without any limit on levels, but only within the confines of the domain. To use multiple domains the PINsafe server can use Global catalog.

Q). Are there any restrictions on the type of groups / group membership supported?

A). Users must be a member of the same domain as the group. Links to users in trusted domains are not supported. Use Global Catalog to get around this problem. Additionally, PINsafe cannot import users from a group if that group is configured as the user's primary group. Active Directory implements trusted domains and primary groups in non-standard ways, which standard LDAP queries cannot discover.

Q). Can a user be a member of more than one AD group that is read by PINsafe or will it create a new user.

A). Yes a user can be a member of more than one group, new users will not be created of the same name. Be aware that a user cannot have more than one transport for their alerts, and more than one transport for their security strings.

Q). If we create a group static group in AD that are read by PINsafe, and also create new dynamic AD groups read by PINsafe and move users across, will we have to resend out new Pin codes or will existing ID's be used?

A). The existing user information will be used as long as the Ignore FQDN option is used and the transports are the same or the option (3.8) onwards to not resend out PIN numbers when the transport changes, is used.

Q). Does PINsafe support Active Directory on 2008 Server

A). Yes

Q). Can I upgrade from 2003 Active Directory to 2008 Active Directory

A). Yes, ensure that the BaseDN remains the same. or you will encounter issues when attempting to sync. Specifically, it would be trying to look for the old FQDN and then abort. If you intend to change the BaseDN then you can avoid this issue by upgrading to the latest version of PINsafe before migrating to AD 2008. The latest version would attempt to find the user elsewhere in the directory when performing a user sync if the BaseDN had changed, thus avoiding the abort issue.

Q). Why are Active Directory errors is stored in the Swivel logs?

A). When the Swivel appliance connects to the domain controller via LDAP, either to perform a user sync or to authenticate the AD password, it may receive errors. These errors are stored in the Swivel logs as sent by AD. In most cases, the messages are checked and illegal characters are filtered, but there are one or two cases in which the message is not checked. In particular, checking the AD password.