Soonr - Active Directory Direct Integration

Direct LDAP Integration

The Soonr "Direct LDAP Integration" is a new, secondary method to integrate Active Directory with your Soonr *Team*. This new mode eliminates the need for one or more machines within the domain running a *Soonr Integration Agent* to authenticate the users. Instead, Soonr leverages the LDAPS protocol to directly query AD.

This release note is supplementary to the Active Directory Integration Guide, which should be read in full prior to preceding with this document. This document highlights the differences to the 'Requirements' and 'Configuration' sections only.

Overview

The new "Direct" connection mode involves connecting directly to the target domain via the LDAPS protocol (LDAP over SSL (TLS)).
While the integration is easier, faster and does not have the hardware requirements of the "OnPrem Agent" AD integration mode, security is not as high as a communication channel needs to be opened on the Domain Controller.

Requirements

- Windows Server 2003 or later
- Open SSL port in the target domain (default 636)
- SSL certificate for the target domain.
  For more information, see: https://support.microsoft.com/en-us/kb/321051
- Firewall configured to accept communication from the Soonr server outgoing IP address range, represented by the appropriate DNS names for your region. To identify your region, login to Soonr Online. Once logged in, use the domain name shown in the browsers address bar to identify the corresponding DNS names that need to be allowed to connect to your AD server(s):
  vip.soonr.com: mgt-sj.soonr.com, lvs.soonr.com
  eu.soonr.com: mgt-dk.soonr.com, lvs-dk.soonr.com
  mp.soonr.com: mgt-mp.soonr.com, lvs-mp.soonr.com
- Account in domain which Soonr authenticates via (makes the connection to domain). These credentials are stored on the server. The account only needs "Read" permissions to the domain, so a standard user account can be used for this purpose.
- Administrator credentials for a Soonr Enterprise *Team*

Configuration

1. Login to *Soonr Online* using the administrator credentials for the *Team*
2. Navigate to '**Configuration**' → '**Active Directory**', and select the '**LDAP Direct**' option
3. Complete the following fields:

   a. **Authentication Domain**
   Enter the domain to be used to authenticate users.
   Note: The domain must be entered in the format "domain_name.local".

   b. **Synchronization at**
   Specify at what hour of the day the synchronising will occur.

   c. **LDAP Search Path**
   Complete the LDAP search path. Multiple paths can be specified by clicking the 'Add path' button.
   The LDAP path must be specified as per the instructions in the **Active Directory Integration Guide**.

   d. **Default phone number prefix**
   This optional field allows for a telephone prefix to be entered, which will automatically be applied to any phone number that does not start with '+'. In AD environments where prefixes have not been entered, this allows for the prefix to automatically be appended upon import into Soonr. Entries into this field must be in the format '+XX', where 'XX' is the desired country code.

   e. **Host Name**
   The IP address or hostname of the domain server.

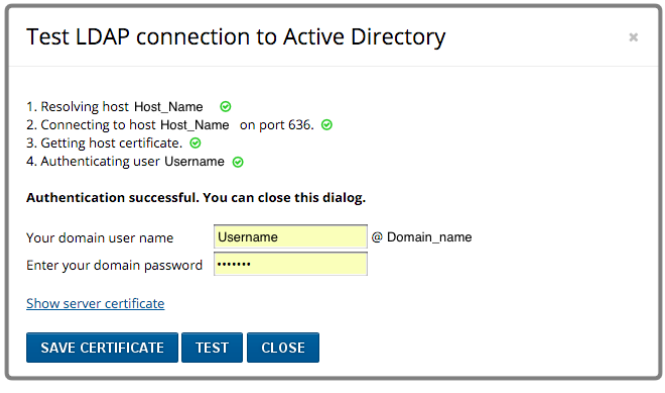
   f. **Port**
   The port number for LDAPS (default is 636).

4. Click on '**Test LDAP Connection to Active Directory**'

   In the window that opens, enter your domain credentials and click '**Test**'.

   This will start a multi-stage test, showing green check marks if successful, or displaying an error message with an explanation if a failure occurs at any stage of the checks.

   If the test fails, close the dialog box, correct the appropriate field and run the test again.
   If the test completes successfully, you may click on "Show server certificate" and verify the information is as expected.



5. Click on '**Save Certificate**'
   The certificate will now be displayed and will show the status as '**Stored**'. Clicking '**Get certificate from host**' will retrieve the current certificate from the host. Clicking '**View more details**' will display detailed information about the certificate.

6. Enter domain username into the '**User Name**' field
7. Click '**Set Password**' and enter the password associated with the username as per set 6

   Be aware this password will be stored securely in the Soonr service.

8. Click on '**Save Settings**'
9. Click on '**Enable Active Directory**'