



Planning is key to "packaged" deployments of Password Reset with Active Directory

Whether you are considering VoiceRite's Password Reset or a different solution, here are some helpful tips on how to prepare and configure your Microsoft Active Directory so that the integration will go smoothly.

Key Points:

- A SSL connection is required between the application server hosting the third party application (VoiceRite's Password Reset) and the Microsoft Active Directory Server.
- To support the SSL connection, an administrative certificate (or at least a user with password reset privileges) must be installed on the third party application (VoiceRite's Password Reset) and the Microsoft Active Directory Server.
- Many of these applications require browser based access to the server running the application.
- If administrators or users plan on accessing the applications via the Internet, a method of secure access (VPN or firewall tunnel) will be required.
- The most effective (cost and otherwise) vendor support is remote, so plan to provide VPN or some type of remote access.

Recommendation 1: Make sure your Active Directory server SSL feature is enabled. Most third party applications that perform administrative types of functions (like password reset) on your Active Directory will require a SSL or other secure connection to the Active Directory server.

Recommendation 2: Install the Active Directory server certificate on the application server that hosts the third party application (such as Password reset). This may require coordination with active directory administrator to get the certificate file.

Recommendation 3: To support two-way SSL certifications, you must retrieve the Active Directory administrator certificate from the Microsoft Certificate Services by logging in to certsrv as administrator or a user with reset password privilege.

This will involve requesting a User certification for the Microsoft Base Cryptographic Provider with Key Usage for both, a key size of 512, and the created key set must be marked as exportable. This certificate should be installed (in IE), and exported from IE as a private key (PKCS #12) with strong protection. The password for this certificate should be the same one used for the SSL Key Store password.

Recommendation 4: Before you start your integration, you might want to consult with the Active Directory administrator on the values of parameters:

1. Base Distinguish Name (DN)
2. Security Principal
3. Security Credentials
4. SSL Trust Store
5. SSL Trust Store Password
6. SSL Key Store
7. SSL Key Store Password
8. SSK Key Store Type

For More Information

Please call VoiceRite at 954-653-2600 or email us at sales@voicerite.com