**Overview:**

The LDAP provisioning tool allows an organization to keep their VersionOne active user list synchronized with users that belong to an LDAP group. The tool assumes that the list of users in the LDAP group is the master list, making updates in VersionOne accordingly. It is built as a standalone exe that can be run as a scheduled task. It polls a configured LDAP directory (active directory and Sun One LDAP have been tested) for users belonging to a configured group, and polls a configured VersionOne instance for a list of users. It compares the users it finds in the LDAP group to the users found in VersionOne and takes appropriate action, according to the chart below. If the Version One instance that is being used is utilizing Version One’s internal security, every user that is created or reactivated is emailed a randomly generated password (which is not stored anywhere else other than VersionOne), and instructions on logging in and changing their password. If the instance is using integrated windows authentication, the users will be emailed a notification with instructions where to log in, using their windows system account. Each time the provisioning tool runs, a summary of accounts that were created, reactivated, and deactivated is emailed to the configured administrator address, along with instructions for assigning project access for new users.

|  |  |  |
| --- | --- | --- |
| **Username found in LDAP** | **Username found in VersionOne** | **Action Taken in VersionOne Instance** |
| Yes | No | User created in VersionOne |
| Yes | Yes (active) | None |
| Yes | Yes (inactive) | User reactivated in VersionOne |
| No | Yes (active) | User deactivated in VersionOne |
| No | Yes (inactive) | None |

**System Requirements:**

* VersionOne:
  + 9.3 or higher,
* LDAP
  + Currently tested with Active Directory and SunOne LDAP,
* Windows
  + Windows XP or higher
  + .Net Framework 3.5 or higher
* Access to an SMTP server.

**Download:**

The latest version is available on the community integration downloads site.

**Configuration:**

This tool utilizes LDAP/Active Directory, Version One, and SMTP. Due to the complexity of integrating these three components, there are several configuration parameters that are required. These settings will be found in the file named “VersionOne.Provisioning.Console.exe.config”.

|  |  |  |
| --- | --- | --- |
| Key | Description | Sample/possible values |
| Version One Settings | | |
| V1Instance | Location of VersionOne instance | http://localhost/versiononeauth |
| V1InstanceUsername | User name of a V1 Admin. If using windows integrated authentication, leave this value blank | corp\bob; admin |
| V1InstancePassword | V1 Admin password. | \*\*\*\*\* |
| V1UserDefaultRole | Default role for added team members | 4 is the User role |
| IntegratedAuth | Does version one use windows integrated authentication? | True/false |
| proxyServerUri | Location of proxy server, if one is being used | http://proxy.server.com/ |
| proxyUsername | User name for accessing proxy server | Corp\bob |
| proxyPassword | Password for accessing proxy server | \*\*\*\*\* |
| proxyDomain | Domain for proxy server | corp |
| LDAP Settings | | |
| ldapGroupMemberAttribute | Attribute that points to the LDAP group member | member |
| ldapServerPath | Network location of ldap server | 192.168.36.4 |
| ldapGroupDN | Top level LDAP domain names | CN=TestV1Users,CN=Users,DC=corp,DC=versionone,DC=net |
| ldapUsername | Username to access LDAP, if not using default credentials | Can be empty if using default credentials |
| ldapPassword | Password to be provided to LDAP, , if not using default credentials | Can be empty if using default credentials |
| mapToV1Username | LDAP user atttribute that holds username to be mapped to the V1 username | sAMAccountName |
| mapToV1Fullname | LDAP user atttribute that holds users full name to be mapped to the V1 Full Name | displayName |
| mapToV1Email | LDAP user atttribute that holds email address to be mapped to the V1 email address | userPrincipalName |
| mapToV1Nickname | LDAP user atttribute that holds a nickname to be mapped to the V1 nickname attribute | sAMAccountName |
| useDefaultLDAPCredentials | Whether to use the system level credentials of the logged in user when accessing LDAP | True |
| Email Properties | | |
| smtpEnableSSL | Whether smtp requires ssl | false |
| userNotificationEmailSubject | Subject line for all user notification emails | You Have Been Added as VersionOne User |
| userNotificationEmailBodyFilename | File name of html file that contains the body of the user notification emails. | userNotificationEmail.html;  userNotificationEmailIntegratedAuth.html |
| adminFullName | Full name of admin for a user to contact if necessary | VersionOne Administrator |
| adminEmail | Email address of said admin | admin@versionone.com |
| adminNotificationEmailSubject | Subject line for notifications sent to administrators | Notification of VersionOne User Changes |
| adminNotificationEmailBodyTemplateFilename | File name of html file that contains the body of the admin notification emails | adminNotificationEmailTemplate.html |
| adminNotificationEmailBodyNewUsersFilename | File name of html file that contains specific text for admin notification of new users added | adminNotificationEmailNewUsers.html |
| adminNotificationEmailBodyDeactivatedUsersFilename | File name of html file that contains specific text for admin notification of users deactivated | adminNotificationEmailDeactivatedUsers.html |
| adminNotificationEmailBodyReactivatedUsersFilename | File name of html file that contains specific text for admin notification of users reactivated. | adminNotificationEmailReactivatedUsers.htm |

In addition, there are SMTP specific keys to be set in the system.net section:

<system.net>

<mailSettings>

<smtp deliveryMethod="Network">

<!-- use this network declaration to include a specific username and password

<network host="mail.mydomain.com" password="xxxxxx" port="25" userName="someaddress@mydomain.com" defaultCredentials="false"/>

-->

<!-- use this network declaration to use the credentials of the process running the provisioning tool -->

<network host="beryllium" port="25" defaultCredentials="true"/>

</smtp>

</mailSettings>

</system.net>

**Running the Application:**

Once the settings have been confirmed, simply navigate to the directory where the application resides and type:

VersionOne.Provisioning.Console.exe

The tool will perform a check of most of the parameters for validity, and report any errors, if there are any. Errors will be displayed on the console and also stored in the file “log.txt”.

The tool will provide a brief summary after running, describing the actions taken, then exit.

Sample output:

13:52:11|Info||Checking VersionOne Settings

13:52:11|Info||Attaching to version one at: http://localhost/versiononeauth/

13:52:11|Info||13 users successfully retrieved from VersionOne.

13:52:13|Info||4 directory members retrieved.

13:52:13|Debug||Member retrieved from directory: corp\Maggie2

13:52:13|Debug||Member retrieved from directory: corp\Maggie1

13:52:13|Debug||Member retrieved from directory: corp\maggie

13:52:13|Debug||Member retrieved from directory: corp\LCunningham

13:52:13|Info||2 Directory users have been marked for creation in VersionOne.

13:52:13|Info||1 VersionOne users have been marked for deactivation.

13:52:13|Info||0 VersionOne users have been marked for reactivation.

13:52:13|Info||Member with username 'corp\Maggie2' has been CREATED in the VersionOne system.