Active Directory PLugin capabilities overview

**ISO Version 3.0**



# Document Control

## Version History

| **Version** | **Date** | **Author** | **Description** |
| --- | --- | --- | --- |
| 0.1 | April-29-2015 | Shawn Meginley | Initial documentation for Active Directory Plugin |
| 0.2 | May-10-2015 | Rhoda Goodrham | Updated formatting. |
| 0.3 | May-19-2015 | Rhoda Goodrham | Updated content and formatting to revamp for a marketing slant. |
| 0.4 | July-22-2015 | Rhoda Goodrham | Test for Git |

## Approval/Authorization

| **Name** | **Role** | **Signature** | **Date** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Introduction
   1. Workflow icon
   2. Plug-in Overview
      1. Generic term of plug-in – how are they used in ISO?
   3. Purpose

This plugin supports connecting to Active Directory via LDAP or LDAPS to make changes to a user and pull the details of a given user. This document will indicate what the requirements are to support this plugin, including Active Directory account access and libraries that will need to be installed. It will also define the Plugin parameters and the input and output parameters for the supported commands.

* 1. What is Active Directory

Active Directory is a special-purpose database — it is not a registry replacement. The directory is designed to handle a large number of read and search operations and a significantly smaller number of changes and updates. Active Directory data is hierarchical, replicated, and extensible. Because it is replicated, you do not want to store dynamic data, such as corporate stock prices or CPU performance. If your data is machine-specific, store the data in the registry. Typical examples of data stored in the directory include printer queue data, user contact data, and network/computer configuration data. The Active Directory database consists of objects and attributes. Objects and attribute definitions are stored in the Active Directory schema.

Link: <https://msdn.microsoft.com/en-us/library/aa746492(v=vs.85).aspx>

* 1. How does ISO use Active Directory?

ISO allows users of ISO to grant and remove accesses and pull additional detail for a given user via LDAP or LDAPS connections.

* 1. Pre-Install Requirements and Dependencies

This plugin requires Python 2.7 to run. The following libraries must be installed:

python-ldap 🡪 <http://www.python-ldap.org/doc/html/installing.html>

The page doesn’t indicate it, but the package can be installed via pip.

Active Directory will need to be configured to accept LDAP or LDAPS (whichever is chosen) connections for the provided username (and password). The username will need to be granted full Domain Administrator privileges (assuming ISO needs to make changes to users).

The plugin is currently only tested against Windows 2008 Server.

* 1. Related Technologies

Include families (i.e. other FireEye products).

1. Command Descriptions

| **Command** | **Description** |
| --- | --- |
| disableUser | This command verifies the user is in the Active Directory and if so then adds them to the specified (Disabled) group and sets the ‘userAccountControl’ to disabled. |
| addUserToGroup | This command verifies the user is in the Active Directory and if so then adds the user to the specified group. |
| removeUserFromGroup | This command verifies the user is in the Active Directory and if so then removes the user from the specified group. |
| replaceUserAttribute | This command verifies the user is in the Active Directory and if so then changes the specified attribute to the specified value. |
| lookupUserBySamName | This command looks up the details for the given SAM USER.  This command returns all of the fields returned by Active Directory (which are only those that are populated). For a full list of those fields, visit:  <https://msdn.microsoft.com/en-us/library/ms675094(v=vs.85).aspx> |
| lookupUserByEmailAddress | This command looks up the details for the given user with the provided Email Address.  This command returns all of the fields returned by Active Directory (which are only those that are populated). For a full list of those fields, visit:  <https://msdn.microsoft.com/en-us/library/ms675094(v=vs.85).aspx> |

What goes in the CPR?

1. Indexing for tags and categories, keywords.