DIRECTORY PASSWORD V1.2
Quick Start Guide

Directory Password is a self-service password reset / account unlock tool that is an optional add-on for Directory Update v2.5. Directory Update must be installed first.

Using Directory Password involves two steps (as shown in Figure 1). The first step involves the user answering their security questions via the Directory Update interface.
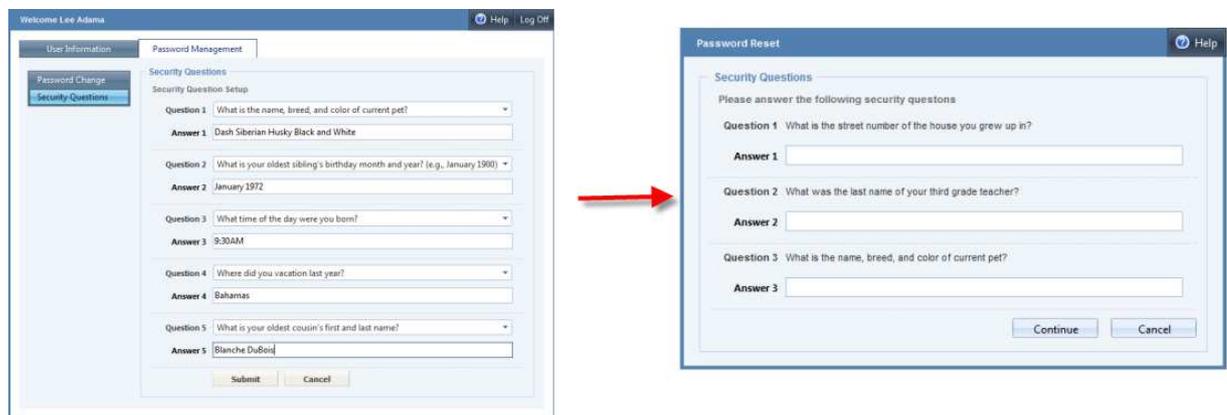

Figure 1: Steps to using Directory Password

The second step requires that the user be able to access a Web browser either from a mobile phone, kiosk or co-worker's computer. From the Directory Password URL (eg. http://servername/DirectoryPassword) the user answers their security questions and then they are able to rest their password.

Directory Password does not include a Windows module that would allow a user to reset their password or unlock their account without logging on to Windows. The user must be able to access a browser to use Directory Password.

Security questions and answers are stored (by default) in the user's **PostalAddress** attribute. Security questions are encrypted and answers are hashed using an irreversible hashing formula. This attribute stores a maximum of 4KB there for the total size of the questions and answers must be less than 4KB.

Ithicos Solutions
http://www.ithicos.com

This document is intended to provide you with a quick reference for getting Directory Password installed.

Tips

Here are some tips and information that will make your work with Directory Password easier and more trouble-free.

- Directory Password v1.2 *requires* Directory Update v2.5 or later be installed.
- Install Directory Update first
- Get a good XML editor; that will make editing the XML files much more painless. We recommend Notepad++; a very good and free text editor. http://notepad-plus.sourceforge.net
- Directory Password has two primary configuration files: *AppSettings.XML* and *PasswordSettings.XML*
- Once Directory Password is installed, Directory Update can use the same PasswordSettings.XML file. See the Directory Update AppSettings.XML file.
- Always make backup copies of your XML files prior to editing them.
- Enable file logging in the auditing section of the AppSettings.XML file

Using Secure Sockets Layer (SSL)

We recommend that you implement Secure Sockets Layer (SSL) for any web site on which end users will enter private/personal data or on which a username / password may be passed over the network. All web-based Ithicos Solutions products will work on SSL-enabled web sites.

There is nothing you need to do to our products to enable SSL. This is done in Internet Information Server (IIS) 6 / IIS 7 / IIS 7.5 / IIS 8 / IIS 8.5. For more information, see:
http://support.microsoft.com/kb/299875
http://learn.iis.net/page.aspx/144/how-to-set-up-ssl-on-iis-7/

We recommend using a certificate authority that will be trusted by the browsers of all users. It is a very bad practice to get users in the habit of ignoring SSL security warnings.

Prerequisites

Directory Password installs only on the x64 flavors of Windows 2008/2012. Both physical and virtual servers are supported.

Ithicos Solutions
http://www.ithicos.com

Make sure that your server does meet all of the prerequisites and your installation will go much more smoothly:

- Windows Server 2003 requirements – **Manual installation required.**
  - Windows Server 2003 with SP1 or later
  - IIS Web service installed
  - Microsoft .NET Framework v4.0 installed
  - Server must be a member of the domain/forest
  - In IIS Manager under Web Service Extensions, make sure that ASP.NET v4. is visible and Allowed
  - Apply all Microsoft critical and recommended updates
- Windows Server 2008 requirements
  - Windows Server 2008 / Windows Server 2008 R2
  - IIS 7 / IIS 7.5 web service enabled
  - IIS 6 compatibility components of IIS 7 enabled
  - ASP.NET enabled and .NET Application support enabled
  - .NET Framework 4.0 installed
  - Apply all Microsoft critical and recommended updates
  - Basic and Windows Authentication services must be enabled
- Windows Server 2012 requirements
  - Windows Server 2012/ Windows Server 2012 R2
  - IIS 8 / IIS 8.5 web service enabled
  - IIS 6 compatibility components of IIS 8 enabled
  - ASP.NET enabled and .NET Application support enabled
  - .NET Framework 4.0 components enabled
  - Basic and Windows Authentication services must be enabled
- Create a service/proxy account that has permissions to update user accounts; this service/proxy account must be able to change a user's password.
- The installation must be performed by a domain user account that is also a member of the IIS Server's local Administrators group
- Download the latest version of the Directory Update and Directory Password software from our Web site.

> We strongly recommend that you run Microsoft Update on the server prior to installing Directory Update to ensure that all updates and fixes available from Microsoft have installed.

Ithicos Solutions

http://www.ithicos.com

Installation

Installation is usually simple and quick though the software will be installed with the default XML templates and you will need to customize these for your organization.

1. Install the current version of Directory Update v2.5 first
2. Run the **DirectoryPassword.MSI** installer
   a. Alternately, copy the installer to a folder, such as C:\temp
   b. Open a command prompt using "Run As Administrator"
   c. Run   **msiexec.exe /i c:\temp\DirectoryPassword.msi**
3. On the welcome screen click "Next" and then on the License Agreement screen, agree to the license and click "Next"
4. On the Select Installation Address, You can take most of the defaults for the installer including the default virtual directory name (**/DirectoryPassword**) and putting the site on to the Default Web Site.
5. On the Destination Folder screen, click Next if you want the default path or specify a new path for the software. The default is c:\inetpub\wwwroot\DirectoryPassword which works for most installations.
6. On the Active Directory Information screen, enter the domain controller name, the domain name, the service account information, and the service account password. Make sure you use the host (or short name) of the domain controller. Click Next when finished.
7. Enter the organization name and the license key (or check evaluation version.)   You can always add the license key later. Click Next.
8. On the Ready To Install Directory Password screen, click Install.
9. The installer will run for 20 to 30 seconds. When the installer completes, click Finish.
10. After the installation completes, immediately test the installation with the default settings. From the server's console, you can open up the web browser and type http://localhost/DirectoryPassword. You should

Ithicos Solutions

see the first screen of the Directory Password interface.

11. Using the **Directory Update** AppSettings.XML file, enable the Password Management tab so that the Security questions are available to the user.
12. In the Directory Password AppSettings.XML file, locate the <Auditing tag and make sure that auditingLogFile is set to enabled="yes". This ensures all use of Directory Password is audited.
13. Customize the XML files to suit your organization including password policies and local links or language options.

Ithicos Solutions

http://www.ithicos.com

Customization Quick Reference

Customizing the Directory Password interface for your specific requirements is reasonably simple once you have taken a look at the XML files that store the configuration. The XML files are all found in the following folder:

`C:\inetpub\wwwroot\DirectoryPassword\Settings`

PasswordSettings.XML

There are two configuration files that you will need to customize. The first file is the PasswordSettings.XML file. The first part of the PasswordSettings.XML file allows you to define password complexity; this is sown in Figure 2. Note that the PasswordSettings.XML file must be *at least* as complex as your Active Directory password policies. In this version, we cannot enforce password uniqueness.

```xml
<passwordSettings>
  <passwordPolicies text="Password policies:">
    <!-- In the "Help" text, you can use the text {0} and the application will fill in the value specified in the tag. -->
    <minimumPasswordLength    value="7" text="Password must be at least {0} characters long." />
    <minimumLowercaseLetters  value="1" text="Password must contain at least {0} lowercase characters." />
    <minimumUppercaseLetters  value="0" text="Password must contain at least {0} uppercase characters." />
    <minimumNumericCharactors value="1" text="Password must contain at least {0} numbers." />
    <minimumSpecialCharacters value="1" text="Password must contain at least {0} special characters." />
  </passwordPolicies>
```
Figure 2: Defining password complexity

The each password complexity rule has a value that allows you to set a specific password complexity and then the display text that the user sees when they set their password.

Directory Password's password complexity requirements allow you to **exceed** Windows password complexity requirements if you wish. However, that may confuse users.

The second part of the PasswordSettings.XML file is where you define the security questions, lockout duration, and question options; this section is shown in Figure 3.

```xml
<securityQuestions questionsAndAnswersAttribute="postalAddress" lockoutDurationAttribute="homePostalAddress" invalidResetAttempts="5" lockoutDuration="15">
  <!-- When picking security questions, do not choose something that is easy to guess or that co-workers might readily know about the user. -->
  <!-- If you change the security questions AFTER you deploy the software, existing questions/answers that users have already answered do not change. -->
  <questions questionsToSetUp="5" optionsPerQuestion="5" questionsToVerify="3" defaultValue="Please select a security question">
    <question>What was your childhood nickname?</question>
    <question>In what city did you meet your spouse/significant other?</question>
    <question>What is the name of your favorite childhood friend?</question>
    <question>What street did you live on in third grade?</question>
    <question>What is your oldest sibling's birthday month and year? (e.g., January 1900)</question>
    <question>What is the middle name of your youngest child?</question>
    <question>What is your oldest sibling's middle name?</question>
```
Figure 3: Defining security questions and options

Ithicos Solutions
http://www.ithicos.com

Directory Password relies entirely on the Active Directory for storing question, answer, and reset information. We do not require any other database interfaces. By default, a user's security questions and answers are stored in the Active Directory attribute **postalAddress**. The **postalAddress** attribute holds up to 4KB of textual or binary data and is not commonly used by Active Directory applications. We use the **homePostalAddress** attribute to store the incorrect logon count. Both of these attributes can be changed but make sure the attribute that is used to store the questions and answers allows for at least 4KB of data.

When a user initially answers their security questions, they are presented with a list of security question options; if a user does not feel that one question is applicable to them they can select a different question from the list. The "questions" tag allows you to define the number of questions that a user must answer (the **questionsToSetUp** option) the number of possible questions in the drop-down list (the **optionsPerQuestion** option), and the number of questions the user must answer in order to reset their password (the **questionsToVerify** option.)

The rest of the PasswordSettings.XML file consists of the security questions. If you are going to require 7 questions to set up and 5 options per question, then you must have at least 35 questions available. We recommend more questions as that provides more possible options for the end user.

Logging and Auditing

Directory Password offers two forms of logging. The first is to log the last date/time of each update to an attribute in Active Directory. The second is to log each individual change to a tab-separated value (TSV) file. These are enabled in the auditing section of the AppSettings.XML file in the section shown here in Figure 3.

Ithicos Solutions
http://www.ithicos.com

```
<!-- Auditing - Directory Update will log the date in yyyy-mm-ddThh:mm:ss format format, username, and IP address each time
<!-- For attribute audit, you can specify extensionAttribute1 through extensionAttribute15. In order to use the extensionAt
<!-- your Active Directory must have been prepped for Exchange 2000/2003/2007. -->
<!-- For log file audit, the default log folder is the "Logs" folder in the DirectoryUpdate folder.  You can change this to
<!-- Ensure that the "Application Pool" account (usually NETWORK SERVICE) has "Modify" permissions to the Logs folder. -->
<auditing>
  <auditingAttribute enabled="no" attribute="extensionAttribute11" showUserLastUpdate="yes" text="Your last update was" />
  <auditingLogFile   enabled="no" logFileFolder="c:\inetpub\wwwroot\directoryupdate\logs\">
    <headers>
      <dateTime  text="Date/Time" />
      <userName  text="User Name" />
      <sourceIp  text="Source IP" />
      <fieldName text="Field Name" />
      <oldValue  text="Old Value" />
      <newValue  text="New Value" />
    </headers>
  </auditingLogFile>
</auditing>
```

Figure 4: Auditing section of AppSettings.XML file

Note that the default log file folder is c:\inetpub\wwwroot\directorypassword\logs. The user account under which the application pool is running (usually NETWORK SERVICE) must have Modify permissions to this folder.

Ithicos Solutions

http://www.ithicos.com