DIRECTORY UPDATE V3.0
Quick Start Guide

Directory Update is an easy-to-use, customizable, Web-based self-service utility that allows an end-user to update their own information in the Active Directory and thus to the Exchange or Office 365 Global Address List. This guide is intended for use with Directory Update v3.0 and later.

This document is intended to provide you with a quick reference for getting started with Directory Update.

Tips

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

- Get yourself 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-plus.org/
- Directory Update is solely designed as a "self service" tool; user are not allowed to other user's information.
- The end user accesses the site using a Web browser and a URL similar to http://ServerName/DirectoryUpdate
- All updates to the Active Directory are done using a service / proxy account, not via the currently logged on user's credentials.
  - Create a service/proxy account that has the permissions necessary to update all users.
  - The service/proxy account's password should not expire.
  - Members of Account Operators cannot update other operator or administrative users. This is a Windows security feature.
- The administrator controls which fields are visible an editable via the DirectorySettings.XML file.
- Most all customization and configuration is performed in one of these XML files found in the `c:\inetpub\wwwroot\DirectoryUpdate\Settings`
  - `DirectorySettings.XML` contains the field/attribute configuration such as which fields show up on the Edit interface, which fields are hidden, drop-down list values, etc…
  - `AppSettings.XML` allows you to customize the search options, window labels, error/help messages, and narrow the scope of a search to a single OU.
  - `AddressSettings.XML` allows you to specify an attribute such as Office name that, when selected, will automatically read the

    office address (street, city, state, postal/zip code, and country) and populate that for the user.
    - `Subsettings.XML` allows you to specify a "parent" attribute and a child attribute. If a specific parent attribute value is selected, the child drop-down list is populated with values dependent on the parent.
    - `PasswordSettings.XML` allows you to define password strength/complexity rules if the users are allowed to change their passwords via Directory Update as well as setting security questions. This file is also used by Directory Password.
- Always make backup copies of your XML files.
- XML tags must have an "open" tag and a "close" tag. *(Hint: Open up an XML file in Internet Explorer to find potential problems.)*
- Photo support requires that the NETWORK SERVICE be given "Modify" permissions to the `c:\inetpub\wwwroot\DirectoryUpdate\photos` folder. This folder is a temporary holding location for photos before they are uploaded to Active Directory.
- You can install the evaluation version and later run the Configuration wizard to add a license key so that it no longer expires. The installer should do this automatically but it does not hurt to check.
- Browsers supported are Internet Explorer 11, Edge, as well as newer versions of Firefox and Google Chrome.
- Changes / customizations to the ASPX and web.config files may not be supported so tread lightly and *make backups* of your original files.

Prerequisites

Make sure that your server meets all of the prerequisites and your installation will go much more smoothly.

- Operating Systems Compatibility
    - Windows Server 2008 R2
    - Windows Server 2012 or R2
    - Windows Server 2016
    - Apply all Microsoft critical and recommended updates
    - Full server installation – Server Core is not supported
- Web Services Requirements
    - Internet Information Server (IIS) web services and management console must be installed / enabled
    - ASP.NET enabled and .NET Application support enabled
    - .NET Framework 4.0 installed / enabled
    - ASP.NET enabled and .NET Application support enabled
    - Basic and Windows Authentication services must be enabled
- Create a service/proxy account that has permissions to update user accounts.

- Have a domain user account that is also a member of the IIS Server's local Administrators group to do the installation
- If User Access Control (UAC) is enabled, you may need to run the installer from the command prompt (Run As Administrator), such as this:

  ```
  msiexec.exe  /i  c:\directoryupdate.msi
  ```
- Download the latest version of the Directory Update software from our Web site.

> We strongly recommend that perform a full update on the server prior to installing Directory Update to ensure that all updates and fixes available from Microsoft have installed. Including any updates related to the .NET Framework.

Installing Prerequisites

The easiest way to ensure that all prerequisites are installed is to use the PowerShell.

1) Open a PowerShell prompt (Run As Administrator)
2) Load the Server Manager module

   ```
   Import-Module ServerManager
   ```
3) Depending on the operating system, add the appropriate Windows Features:

Windows Server 2008 R2

```
Add-WindowsFeature Web-Server, Web-Basic-Auth, Web-Windows-Auth, Web-ASP-NET, Web-Net-Ext, AS-Web-Support
```

Windows Server 2012 / 2012 R2

```
Add-WindowsFeature Web-Server, Web-Mgmt-Console, Web-Scripting-Tools, Web-Basic-Auth, Web-Windows-Auth, NET-FRAMEWORK-45-Core, NET-FRAMEWORK-45-ASPNET, Web-HTTP-Logging, Web-NET-Ext45, Web-ASP-Net45
```

Windows Server 2016

```
Add-WindowsFeature Web-Server, Web-Mgmt-Console, Web-Scripting-Tools, Web-Basic-Auth, Web-Windows-Auth, NET-FRAMEWORK-45-Core, NET-FRAMEWORK-45-ASPNET, Web-HTTP-Logging, Web-NET-Ext45, Web-ASP-Net45
```

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. Use 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.

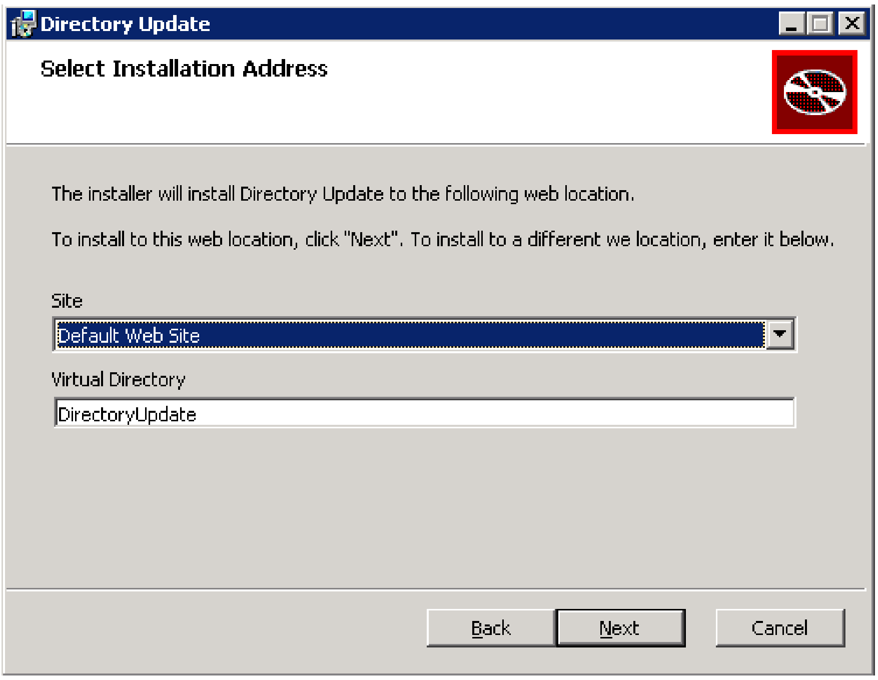
All web-based Ithicos Solutions products will work on SSL-enabled web sites. There is nothing you need to do to our products to enable SSL. This is done in Internet Information Server (IIS).

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. Run the **DirectoryUpdate.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\DirectoryUpdate.msi

2. On the welcome screen click "Next" and then on the License Agreement screen, agree to the license and click "Next"
3. On the Select Installation Address, You can take most of the defaults for the installer including the default virtual directory name (**/DirectoryUpdate**) and putting the site on to the Default Web Site.



Directory Update

Select Installation Address

The installer will install Directory Update to the following web location.

To install to this web location, click "Next". To install to a different we location, enter it below.

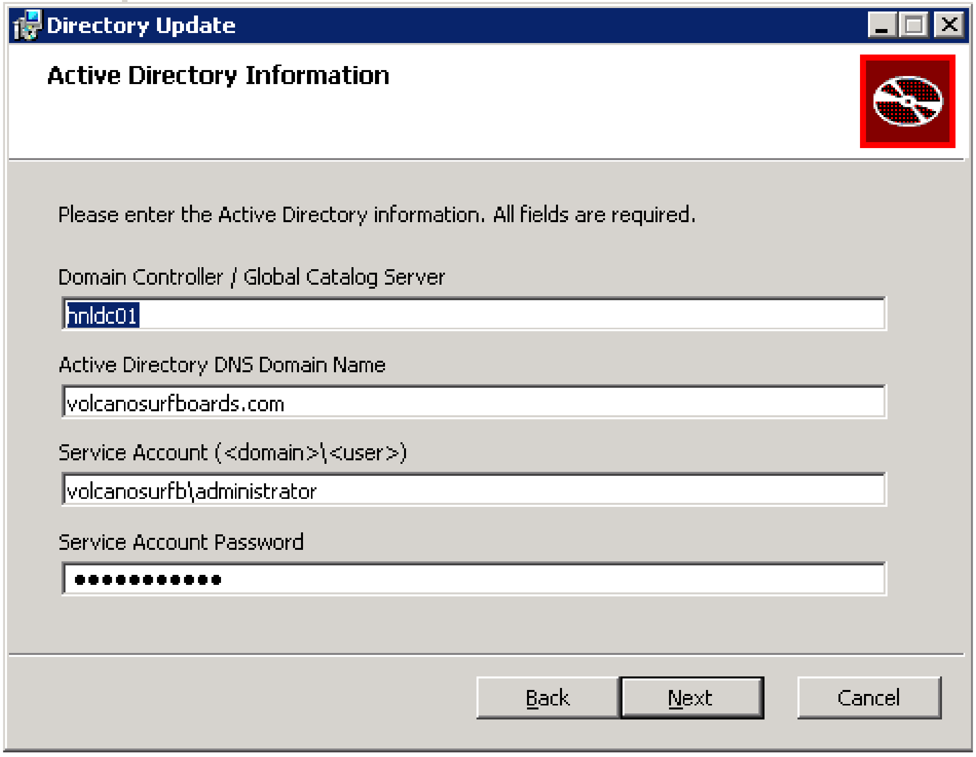
Site: Default Web Site

Virtual Directory: DirectoryUpdate

4. 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\DirectoryUpdate which works for most installations.

5. 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.



Active Directory Information

Please enter the Active Directory information. All fields are required.

Domain Controller / Global Catalog Server: hnldc01

Active Directory DNS Domain Name: volcanosurfboards.com

Service Account (<domain>\<user>)

volcanosurfb\administrator

Service Account Password: ●●●●●●●●●●●

6. Enter the organization name and the license key (or check evaluation version.) You can always add the license key later. Click Next.
7. On the Ready To Install Directory Update screen, click Install.
8. The installer will run for 20 to 30 seconds. When the installer completes, click Finish.
9. 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/DirectoryUpdate
10. Now that the install is completely, customize the XML files to suit your organization. Always make a good backup of your XML files before customizing.

Customization Quick Reference

Customizing the Directory Update interface for your specific requirements is reasonably simple once you have taken a look at the XML files that store the configuration and if you get yourself a good XML editor. The XML files are all found in the following folder:
`C:\inetpub\wwwroot\DirectoryUpdate\Settings`

There are five primary configuration files available to you for Directory Update:

DirectorySettings.XML – Controls the user interface, which fields are visible, which fields are editable, field labels, validation rules, dropdown lists, etc…
AddressSettings.XML – Allows a user to populate multiple values, such as street address, city, state, country, postal code, by selecting a single value such as an office name.
Subsettings.XML – Allows the creation of a parent-child relationship between two fields, such as division to department. If a user selects a certain division name, then only the departments associated with that particular division are selected.
AppSettings.XML – Controls settings in the user interface such as button labels, search fields, export fields, and which fields are visible in the search results columns.
Password.XML – Allows you to define complexity rules for the Change Password functionality.

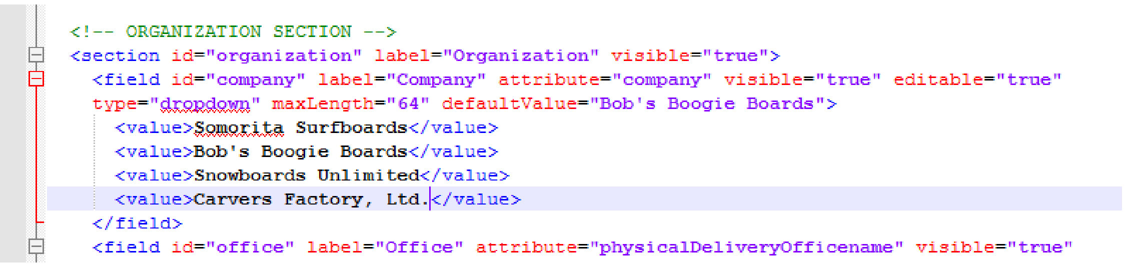
Each attribute / field on the user interface has some of the same basic options. Here is an example of the “tag” for the Office name.

```
<field id="office" label="Office" attribute="physicalDeliveryOfficename"
visible="true" editable="true" type="dropdown" maxLength="128"></field>
```

- Each field has a unique identifier that is used within our software.
    - id=”office”
- Each field contains the LDAP attribute name to which it is mapped in Active Directory.
    - attribute="physicalDeliveryOfficename"
- Each field contains the maximum field size. In most cases, this is the maximum data size Active Directory will accept. Do not increase this.
    - maxLength="128"
- Each field label can be changed

  - Label="Office"
- Each field type can be text, dropdown, or combo
  - type="dropdown" type="text"   or type="combo"
- Each field can be hidden / unhidden
  - visible="true" or visible="false"
- Each field can be made read only or editable
  - editable="true" or editable="false"
- Each field can have a default value
  - defaultValue="My Office Name"
- Each field can have a validation format assigned to it
  - validationFormat="US-Phone"
- Each field can have example text
  - example="Type your official title"
- Each field can be required
  - required="true"

Below is an example of the Organization section and two fields (company and office.) This will give you an idea of some of the types of customization that can be done.



```
<!-- ORGANIZATION SECTION -->
<section id="organization" label="Organization" visible="true">
  <field id="company" label="Company" attribute="company" visible="true" editable="true"
  type="dropdown" maxLength="64" defaultValue="Bob's Boogie Boards">
    <value>Somorita Surfboards</value>
    <value>Bob's Boogie Boards</value>
    <value>Snowboards Unlimited</value>
    <value>Carvers Factory, Ltd.</value>
  </field>
  <field id="office" label="Office" attribute="physicalDeliveryOfficename" visible="true"
```

> The DirectorySettings.XML and AddressSettings.XML files CAN be interchanged with **Directory Update**. The AppSettings.XML file cannot be used with our other programs.

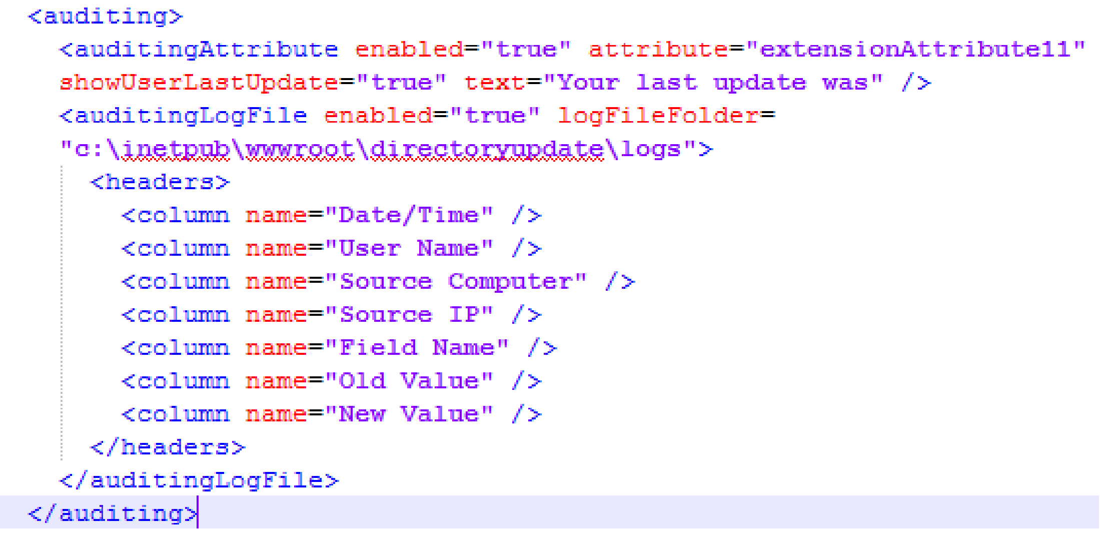
Drop Down Lists

Drop down lists are a popular feature. Drop down lists require the end user to select one of a pre-approved list of values. Here is the company name tag that has been configured as a drop down list type. You have to insert <value></value> tags between the "field" tags. In this example, there are 4 valid company names from which the user can select.

```
    <field id="company" label="Company" attribute="company" visible="true"
editable="true" type="dropdown" maxLength="64" defaultValue="Bob's Boogie
Boards">
      <value>Somorita Surfboards</value>
      <value>Bob's Boogie Boards</value>
      <value>Snowboards Unlimited</value>
      <value>Carvers Factory, Ltd.</value>
    </field>
```

Logging and Auditing

Directory Update 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 1.



```
  <auditing>
    <auditingAttribute enabled="true" attribute="extensionAttribute11"
    showUserLastUpdate="true" text="Your last update was" />
    <auditingLogFile enabled="true" logFileFolder=
    "c:\inetpub\wwwroot\directoryupdate\logs">
      <headers>
        <column name="Date/Time" />
        <column name="User Name" />
        <column name="Source Computer" />
        <column name="Source IP" />
        <column name="Field Name" />
        <column name="Old Value" />
        <column name="New Value" />
      </headers>
    </auditingLogFile>
  </auditing>
```

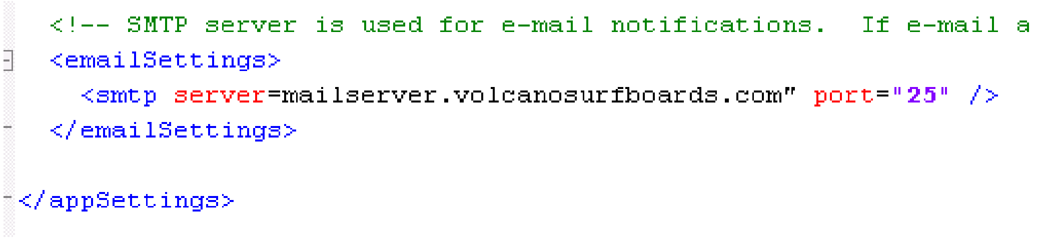
Figure 1: Auditing section of AppSettings.XML file

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

E-mail Notifications

Directory Update v2.0 introduces e-mail notifications as a new feature. All e-mail notification settings are configured in the AppSettings.XML file. The first thing that must be configured is the e-mail server; we recommend you use the fully qualified domain name of an e-mail server that will accept mail anonymously.

The e-mail server settings are found in the <emailSettings…> tag near the bottom of the AppSettings.XML file. An example is shown in Figure 2.



```
  <!-- SMTP server is used for e-mail notifications.  If e-mail a
  <emailSettings>
    <smtp server=mailserver.volcanosurfboards.com" port="25" />
  </emailSettings>

</appSettings>
```

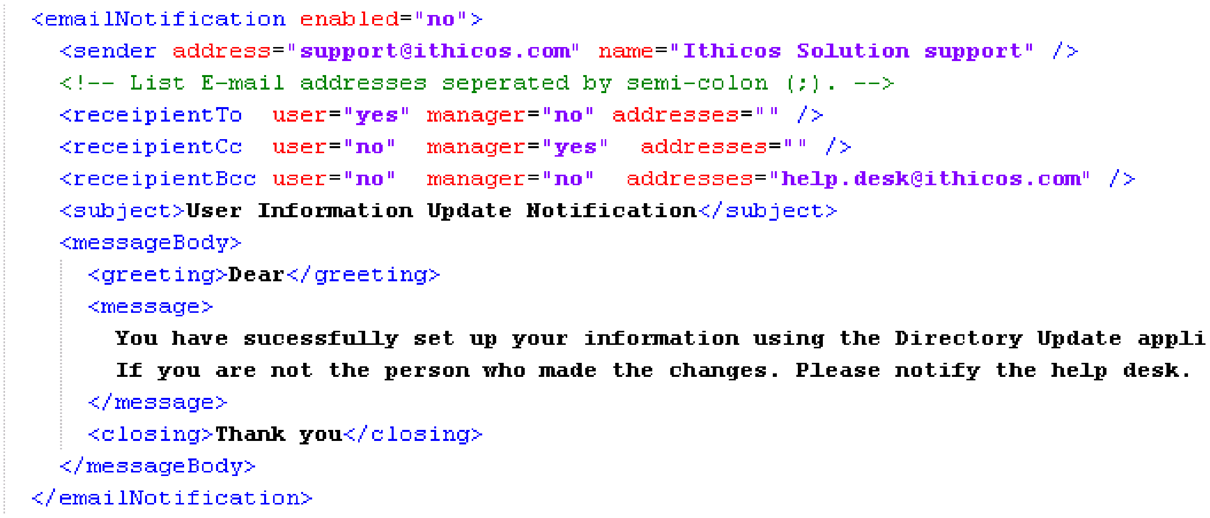
Figure 2: Configuring the SMTP e-mail server

The SMTP e-mail server that you specify must accept mail from the Directory Update server. If you are sending to e-mail addresses outside of your organization, then that server must allow relay for the recipients to which you are sending.

There are three types of events for which you can send e-mail notifications. These are:

- Directory information updates (such as phone, address, title, etc…)
- End user changes their own password
- User updates/changes their security questions (if Directory Password is installed.)

Figure 3 shows the e-mail notification settings that are used if a user changes their own personal information in the Active Directory. You can also configure separate notifications for password changes and setting up security questions.



```
<emailNotification enabled="no">
  <sender address="support@ithicos.com" name="Ithicos Solution support" />
  <!-- List E-mail addresses seperated by semi-colon (;). -->
  <receeipientTo  user="yes" manager="no" addresses="" />
  <receeipientCc  user="no"  manager="yes"  addresses="" />
  <receeipientBcc user="no"  manager="no"  addresses="help.desk@ithicos.com" />
  <subject>User Information Update Notification</subject>
  <messageBody>
    <greeting>Dear</greeting>
    <message>
      You have sucessfully set up your information using the Directory Update appli
      If you are not the person who made the changes. Please notify the help desk.
    </message>
    <closing>Thank you</closing>
  </messageBody>
</emailNotification>
```

Figure 3: E-mail notification settings

You must customize the sender's SMTP address and display name since the default/example values will not be valid for your company. You can send the notification to the user, the user's manager, or a predefined SMTP address (such as the help desk's SMTP address.

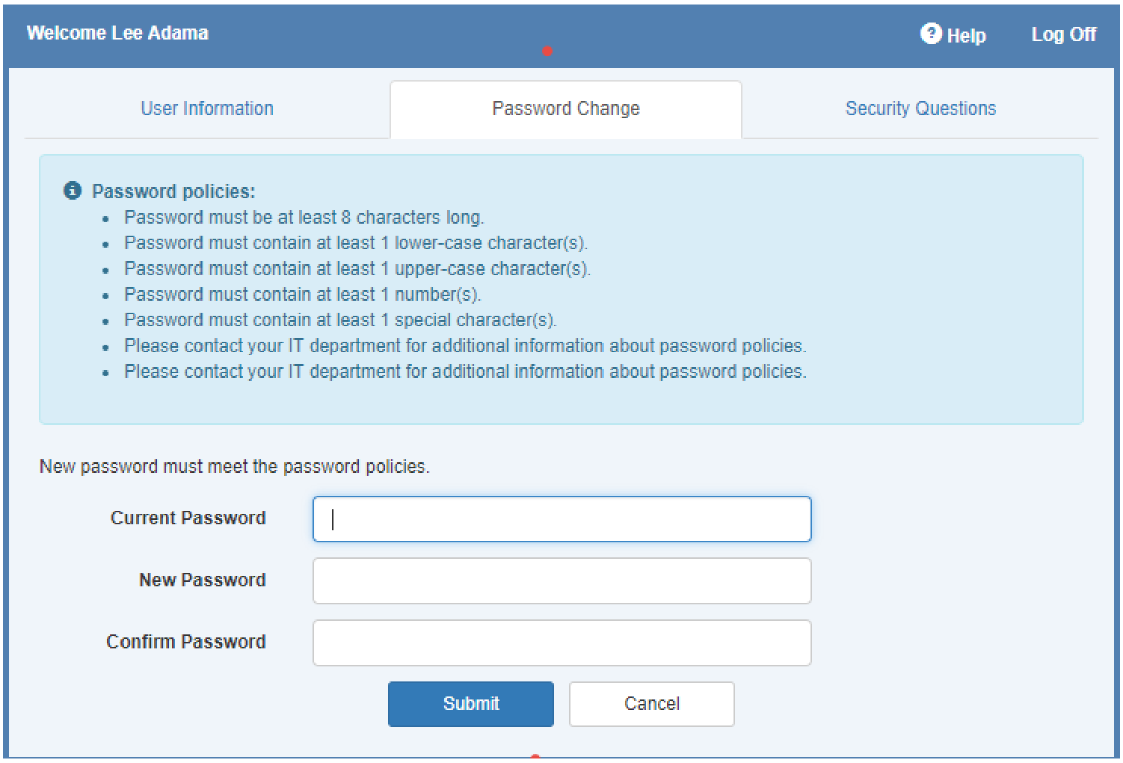
Note that if you select the option to send the notification to the person's manager, the person's Manager field must be filled out and the manager must have an e-mail address.

Password Options

Directory Update v2.0 and later offers the ability to allow end users to change their own password. This option is enabled in the <passwordChange…> section of the AppSettings.XML file.

```
  <passwordChangeTab visible="true" title="Password Change"…
```

The Password Management tab is shown in Figure 4. Password Management is disabled by default.



Password policies:

- Password must be at least 8 characters long.
- Password must contain at least 1 lower-case character(s).
- Password must contain at least 1 upper-case character(s).
- Password must contain at least 1 number(s).
- Password must contain at least 1 special character(s).
- Please contact your IT department for additional information about password policies.
- Please contact your IT department for additional information about password policies.

New password must meet the password policies.

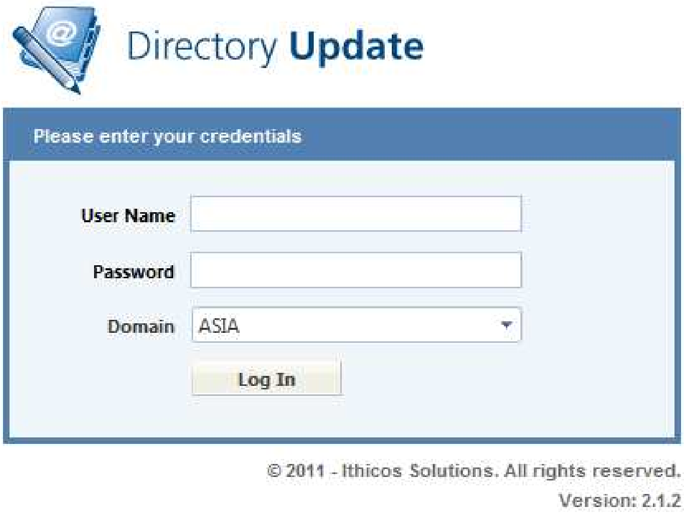
Figure 4: Change password feature of Directory Update

If you are going to use this feature, you should tune the PasswordSettings.XML file to match your organization's password policy.

Integrated Windows Authentication / Single Sign On

Internet Information Server (IIS), Windows, and Internet Explorer support a feature called Integrated Windows Authentication. Essentially this means that when a user connects to a web site that supports this feature (and if the Web browser supports it), then the user will automatically be signed on.

The default logon interface for Directory Update is the logon form also known as Forms Based Authentication. Forms Based Authentication (FBA) should work with any browser, from any Windows, Unix, or Apple desktop computer and for users that are not on a computer that is a member of a domain.

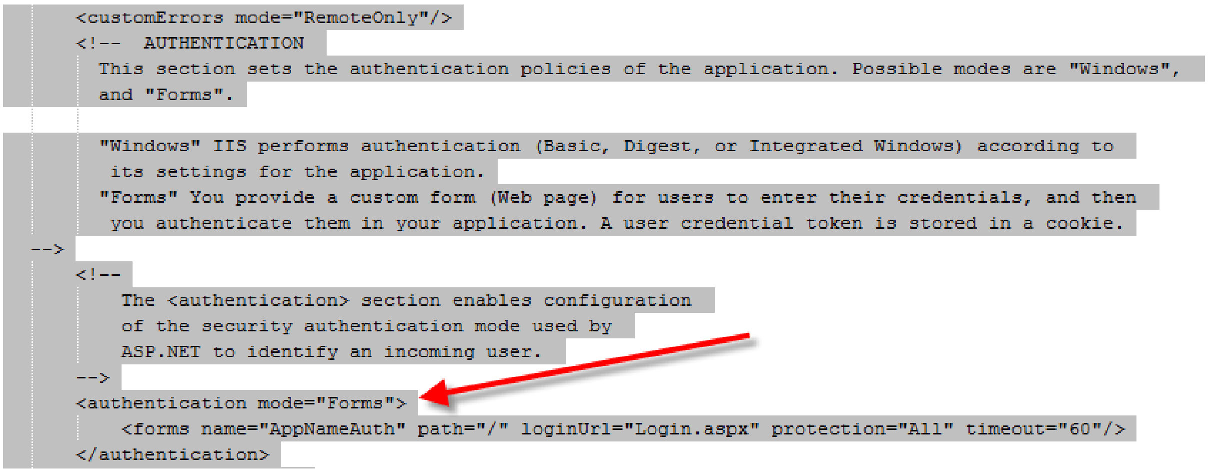


Domain: ASIA

© 2011 - Ithicos Solutions. All rights reserved.
Version: 2.1.2

You can use Integrated Windows Authentication (IWA) with Directory Update to eliminate the logon for the user. All the user needs to do is to visit the URL for Directory Update and they are automatically logged on. Note that there is no such thing as a "log off" when using IWA since the user did not really logon.

To enable IWA for Directory Update, edit the **web.config** file (found in **c:\inetpub\wwwroot\directoryupdate** by default). Locate the authentication section and change *mode="Forms"* to *mode="Windows"*



```
    <customErrors mode="RemoteOnly"/>
    <!--  AUTHENTICATION
      This section sets the authentication policies of the application. Possible modes are "Windows",
      and "Forms".

      "Windows" IIS performs authentication (Basic, Digest, or Integrated Windows) according to
       its settings for the application.
      "Forms" You provide a custom form (Web page) for users to enter their credentials, and then
       you authenticate them in your application. A user credential token is stored in a cookie.
  -->
    <!--
        The <authentication> section enables configuration
        of the security authentication mode used by
        ASP.NET to identify an incoming user.
    -->
    <authentication mode="Forms">
        <forms name="AppNameAuth" path="/" loginUrl="Login.aspx" protection="All" timeout="60"/>
    </authentication>
```

Integrated Windows Authentication works provided the following is true:

- The user is using a browser that supports IWA such as Internet Explorer
- The computer on which the user is logged in is a member of the Active Directory forest in which the Directory Update IIS Server is located
- The user logs on to that computer with a domain account
- There are no security settings that prevent IWA
- The browser's local security zone permits IWA (such as Internet Explorer's "Local Intranet" zone.

If you are interested in learning more about IWA, see this link: http://en.wikipedia.org/wiki/Integrated_Windows_Authentication