IDENTITY SYNCRONIZER

Getting Started

Autotask® Integration

Identity Syncronizer™
Autotask® MMC Getting Started Guide

Table of Contents

Identity Syncronizer – Getting Started Guide

Launching the Autotask® Active Directory tab
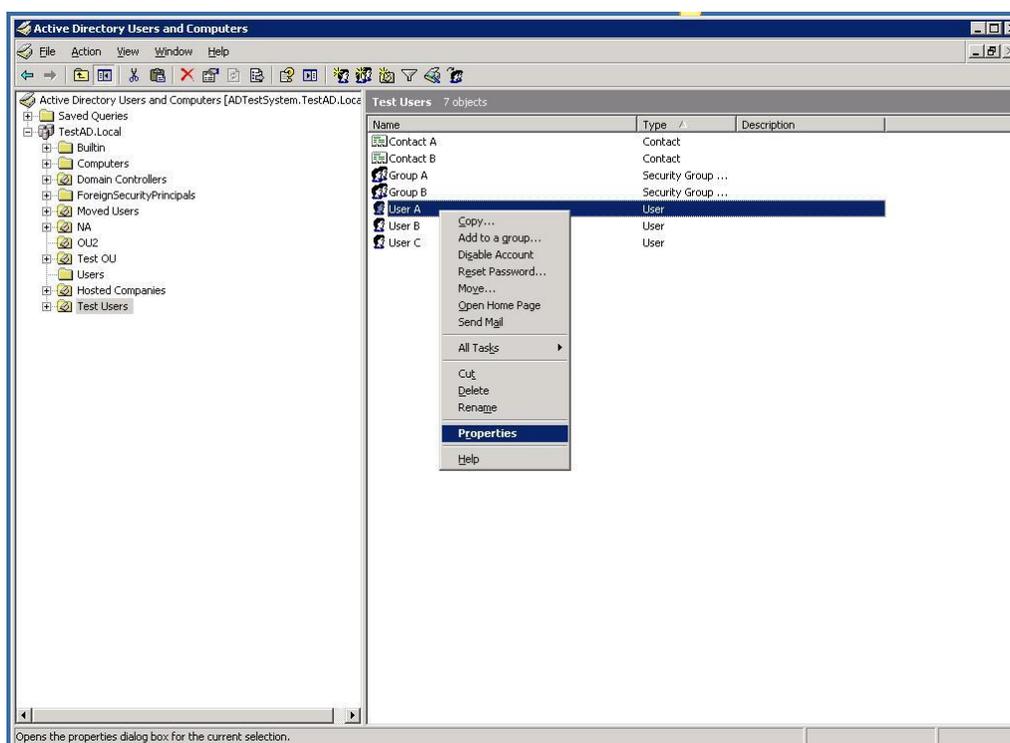
To launch the Identity Sycnronizer Autotask™ tab you should start the "Active Directory Users and Computers" (ADUC) tool as you would normally. This can be found in on any domain controller under Administrative Tools on the start menu or by typing "dsa.msc" into Start->Run.

Once ADUC has opened, navigate to the user you wish to administer or right click on the domain and select "Find" to search for the user. Access the properties for the user by either double clicking the user or you my right click the user and select properties from the context menu as shown in the image above.

After selecting the properties option, the Properties window for that use will be displayed. You will notice many tabs displayed along the top of this property window. Each tab represents a different configuration item for that user. Look for the tab titled "Autotask" and select that tab by left clicking it.

Autotask® User Properties

Once the Autotask® tab is selected you will a window similar to the one below:
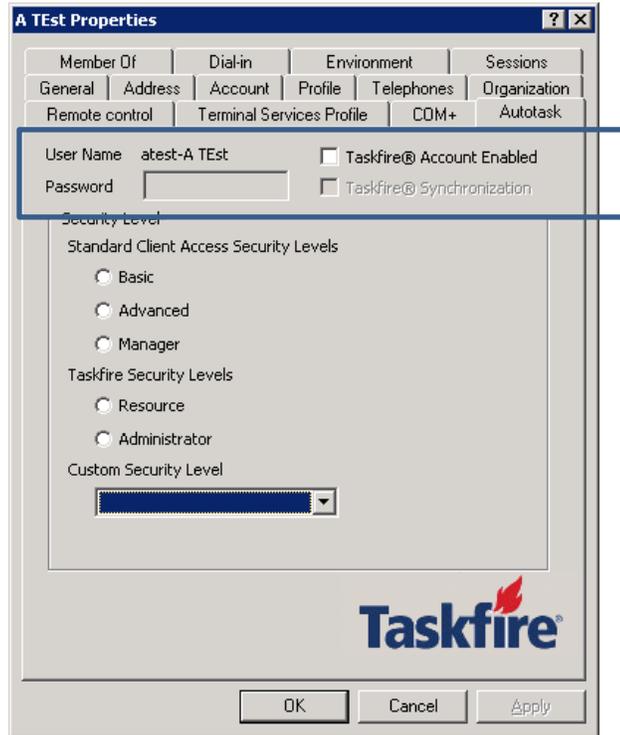
1. **User Name**: This displays the User Name for the currently selected user. This is also known as the SAMAccountName.

2. **Password**: If enabled, this field specifies the current password for the user. This password field is only enabled if the "Syncronization" check box is unchecked. Passwords entered here will not be displayed but will show asterisk (*) characters.

3. **Disable Account**: When checked, this user will be disabled for Autotask®. If unchecked then this user is currently enabled for Autotask. Please note: The user will not be disabled within Active Directory by checking this box, only for Autotask® functionality.

4. **Syncronization**: When checked, the value entered in the password field will be locked to the value stored in the Identity Syncronizer database. When unchecked the password field will be unlocked and can be edited. This password will be sent to Autotask® when the transaction is submitted. This will not change the password for Windows and Active Directory.

Enabling Client Portal

Once a user has been enabled for Autotask®, that user will automatically be added to your Autotask® account as a contact record. Once enabled, you may also select to enable Client Portal access, or Task fire access by selecting from the Security Level options displayed.
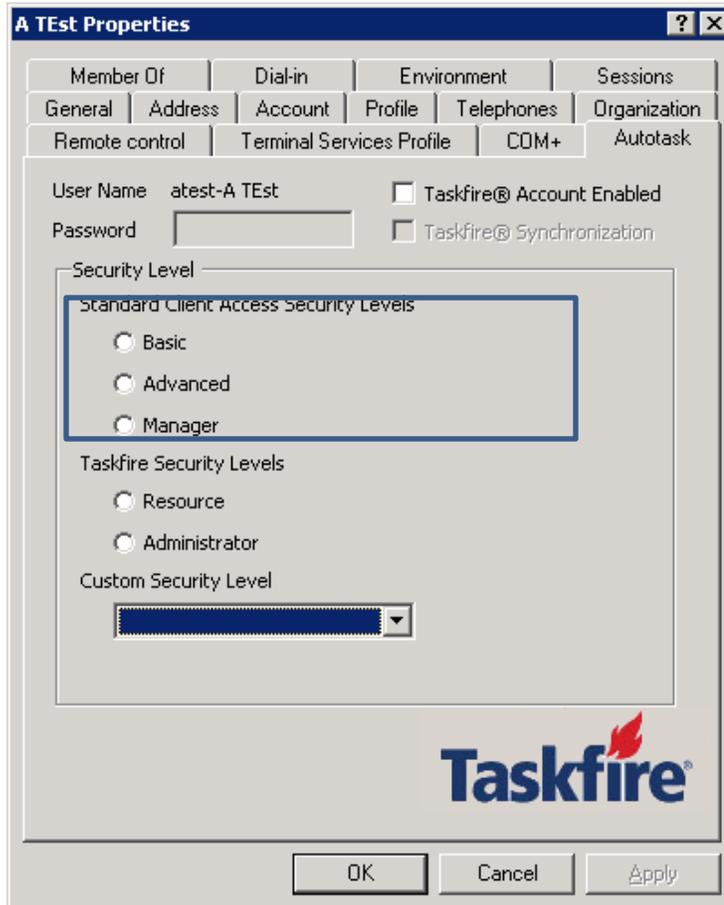
5. Standard Client Access Security Levels – These options enable the Client Access portal feature for this user.

   a. Basic – This use can only see their tickets and has basic access to create new requests and add notes and attachments.

   b. Advanced – This user can see all tickets (including on Child Accounts) for their organization, and can fully create new requests, notes, attachments, and can also e-mail their support team.

   c. Manager – Has all of the access of the Advanced level but can also see costs, hours, and invoice and contract reports.

Enabling Taskfire®
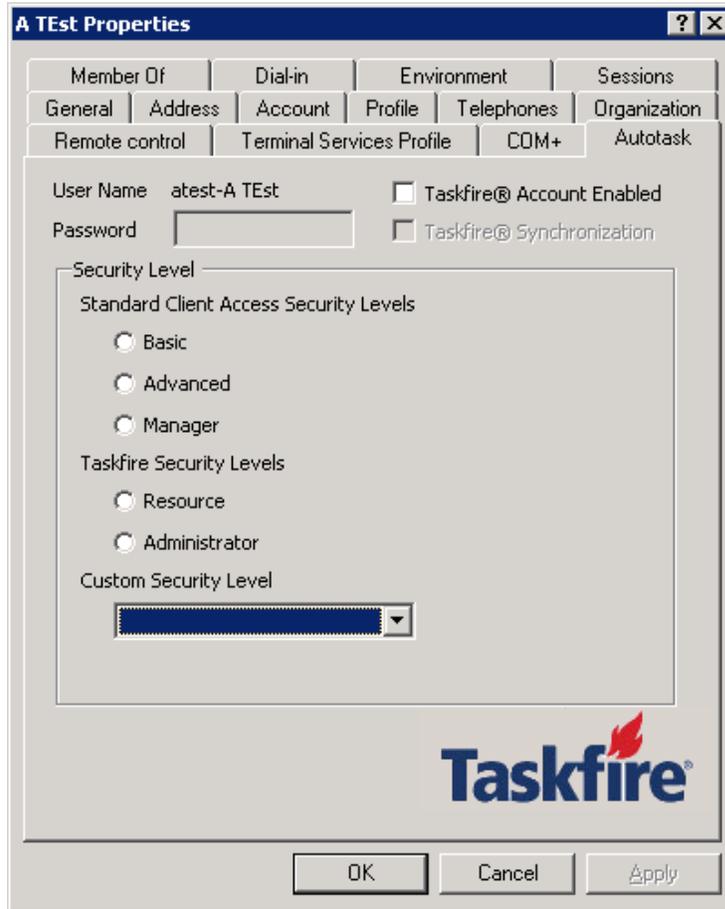
6. Taskfire Security Levels – By selecting one of these options, the user will be enabled for Taskfire.

    a. Resource – Can access all tickets and projects for the Account, Create new Reqeusts, and View/Add notes, attachments, issues, costs, and schedule.

    b. Administrator – Has all the access of the Resource level but can also manage Queues, Request Types, Vendors, Configuration Items, Invoices, and other cost reports.

    c. Custom Security Level - If the none of the standard security levels meet your requirements, you can create a custom security level for the Client Access Portal within Autotask. See the appropriate Autotask® user guide for more information.

Creating a New User

When creating a new user in Active Directory, you can create a new Autotask® portal user as part of this process using Microsoft's standard ADUC tools. To begin, create a new Active Directory user as you would normally. The steps have been outlined below:

Within Active Directory User and Computers, right-click in the appropriate Organizational Unit (OU) and select the option for New > User from the context menu:
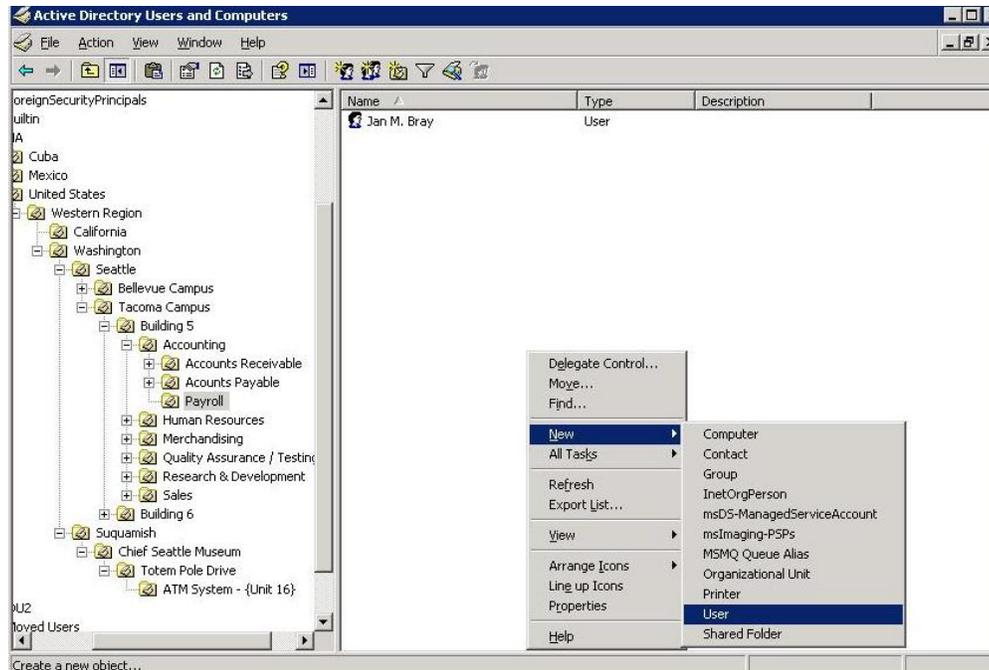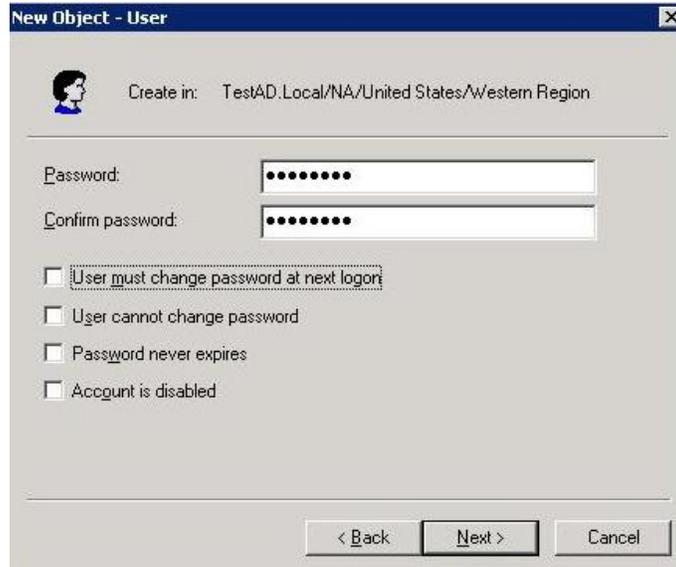

The New User dialog will be displayed and should be filled out as you normally would for any user.   The first page is general user information including Name, Logon, etc. Click Next to continue.
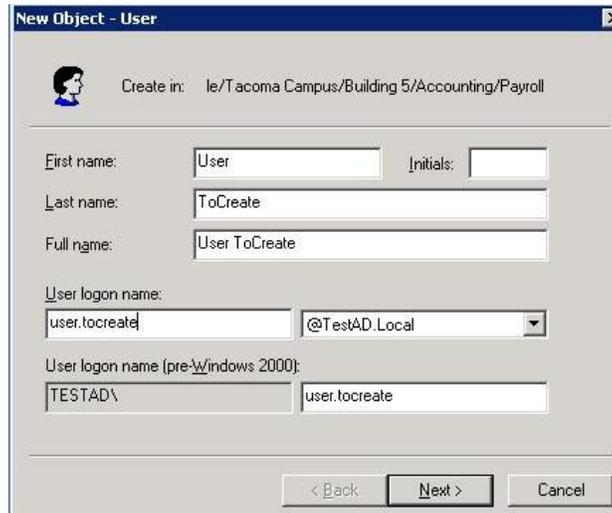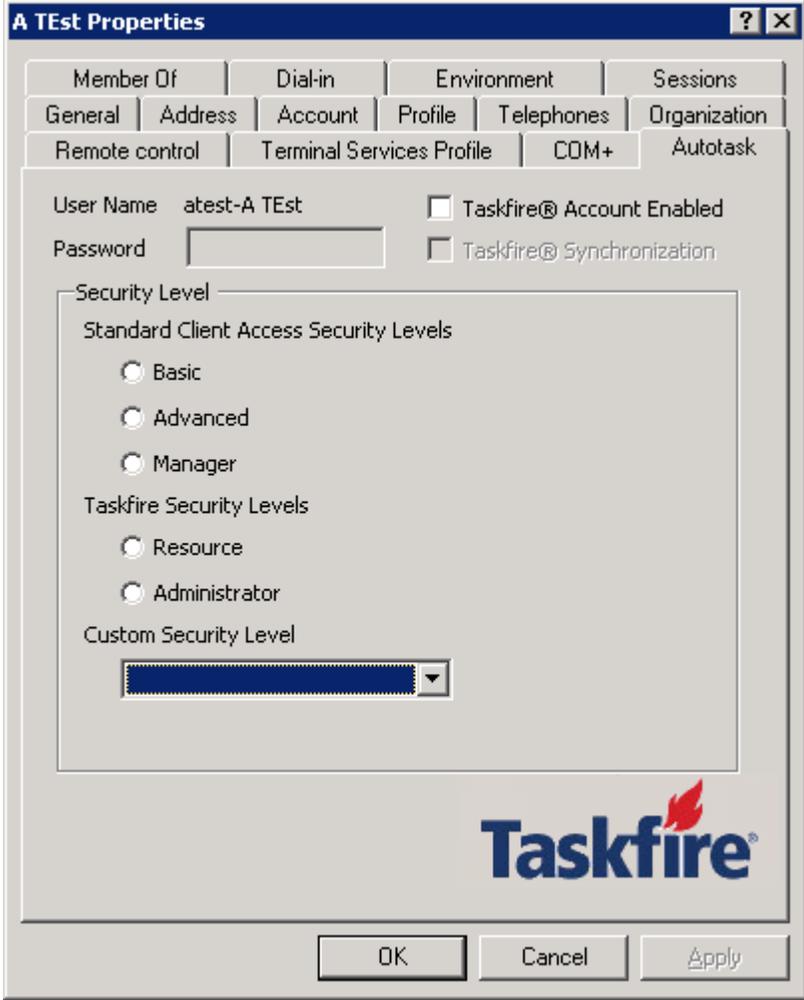
The next page of the dialog will allow you to specify the user's password and other standard options. These should be filled out as normal. Click Next to continue.

The last page of the dialog will provide you with a summary of the user being created. normal. Click Finish to create the user.
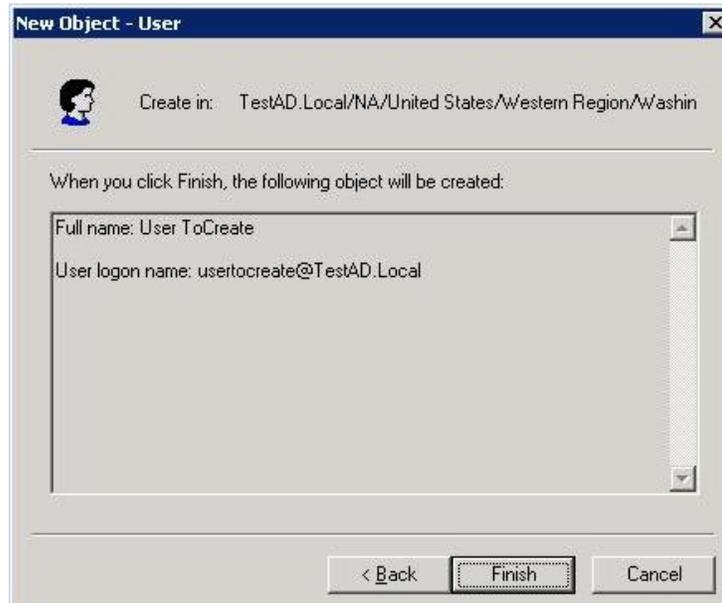
Once the user has been created, right click on the new user and select "Properties" from the context menu to display the property sheet for that user. Select the Autotask® property sheet. The user should not contain any data and should be disabled as shown in the image below:

Configuring New User Settings

To create a user in Autotask®, check the box that says "Account Enabled". By selecting this box only and clicking OK the user will be created in Autotask® as a contact record. If no other options are selected, the user will not have any Client Portal or Taskfire rights.

A user configured in this way will be setup in Autotask as a contact for Tickets, Projects, and other items but will not themselves have access to the system.
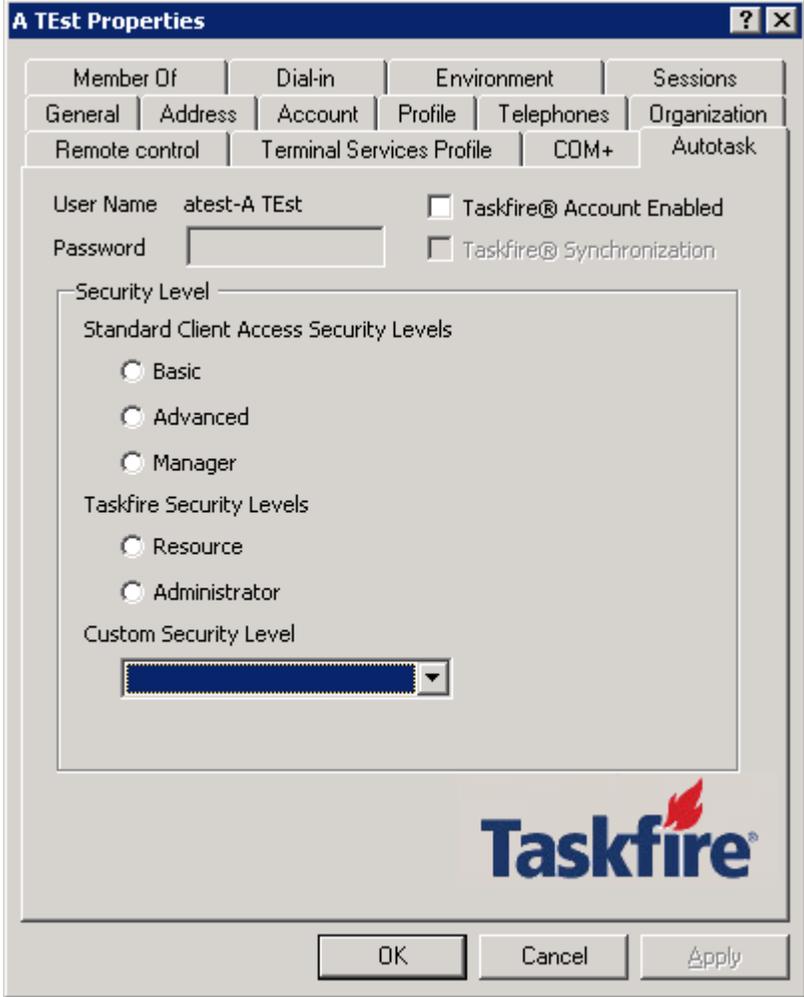
Unprocessed Transactions

When displaying a User's property page you may occasionally notice that the property sheet may appear locked with a status message at the bottom of the screen indicating that there are unprocessed transactions for this user.

There is 1 unprocessed transaction for this user out of 1 total

| OK | Cancel | Apply |
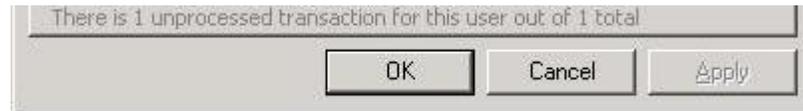
This is indicating that there are uncommitted changes that have not yet been completed. This message will not be displayed once the pending change has been completed.

The property sheet will automatically attempt to refresh the screen every 30 seconds. Once the transaction processes you will be able to manage the user's settings.

Resetting Passwords

Password changes made by the user at their workstation using standard Windows procedures will automatically be synchronized to Autotask® immediately upon the user's request. Should it become necessary to reset the User's password, you may do so by using the "Reset Password" function within Active Directory.

Right click on the user and select "Reset Password" from the context menu that is displayed. You will be promped for the new password and this will be automatically synchronized to Autotask®.
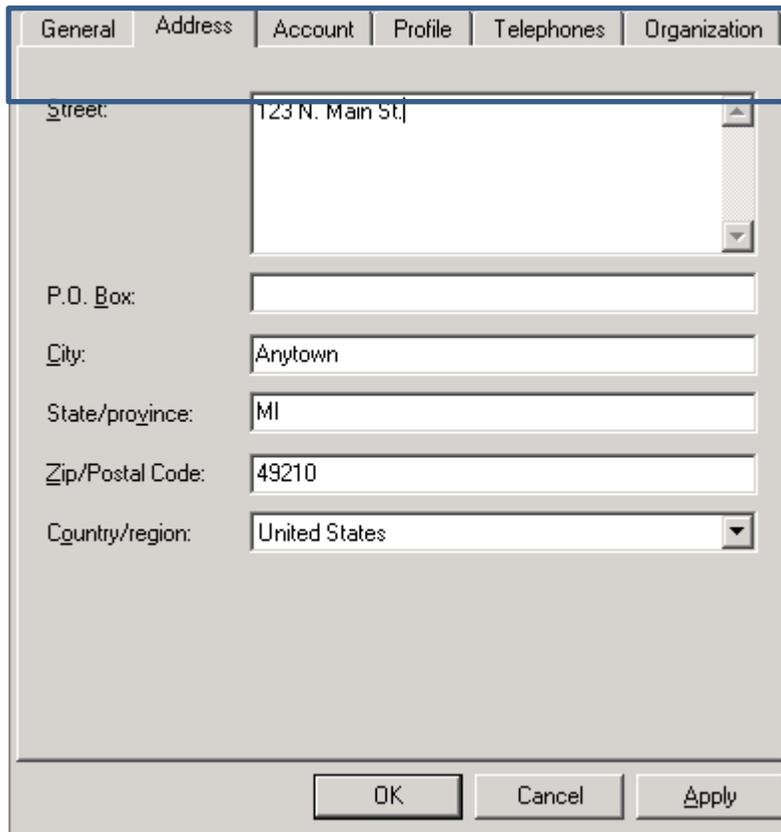
User Changes – Enable, Disable, Delete

Identity Syncronizer™ will automatically keep Autotask™ updated when changes are made to users that are configured for access. When a user is enabled or disabled within Active Directory (even if they are disabled for entering a password incorrectly) – this change in status will be automatically replicated to Autotask®. These changes are replicated whether they are system generated, user generator, or are automatically generated by Windows.

If a user is deleted from Active Directory, that user will be automatically removed (if possible) from Autotask®. If Identity Syncronizer attempts to remove a user from Autotask® but is unable to do so (due to tickets, or projects attached to that user), it will simply disable the user instead.

User Data Syncronization

Identity Syncronizer™ automatically keeps Autotask® updated with changes in user information stored in Active Directory.   This includes all of their address, telephone, and organizational information stored on the tabs within the Users' Property sheet.

The General, Address, Telephones, and Organization tabs are all synchronized to Autotask®

When a change to this information is made within Active Directory, Identity Syncronizer™ will automatically send these change to Autotask® to keep that information fully up-to-date with changes that are occurring.   The information that is synchronized can be restricted by configuring the Autotask integration (see the Installation Guide) to remove certain data elements that you do not wish to have maintained.