

## INSTALLATION & USER GUIDE

# ShoreTel Active Directory Import Application

ShoreTel Professional Services

## Introduction

The **ShoreTel Active Directory Import Application** allows customers to centralize and streamline management of the communication related data that they store in their Active Directory (AD) database. By automating both the initial creation of new ShoreTel records and the ongoing synchronization of data between the Microsoft AD and ShoreTel systems, IT groups can increase efficiency, accuracy, and service levels. The application is highly configurable, designed to easily accommodate customers' specific AD organizations and data structures. Customers will benefit greatly from deploying this solution as a central component of their ongoing data management processes.

When a new user is added to the AD, the application can be configured to either create a new ShoreTel AD user or to create a ShoreTel System Directory entry so that ShoreTel users can easily dial this non-ShoreTel user from Communicator.

The application is installed on the ShoreTel Director (HQ) server and is run manually by a System Administrator or configured to run periodically by the Windows Task Scheduler.

### Benefits/Features:

- Automates the creation of ShoreTel users when users are added to the Active Directory.
- Enables migration from legacy systems (e.g., Microsoft OCS) to ShoreTel by creating ShoreTel System Directory entries for non-ShoreTel users so a complete corporate directory is available in Communicator.
- Keeps the ShoreTel System current with the Active Directory information.
- Option to specify an LDAP path to support multiple AD Forests.
- Optional LDAP filter to select which AD users are synchronized with the ShoreTel system.
- Options to change (or disable) mappings between LDAP properties and the System Directory fields.
- Options to save users DID and extension numbers in the AD.
- Provides a "test" mode option to view changes which would be made to the ShoreTel system based on the current application configuration. This is useful for debugging LDAP filters and LDAP property mappings before changes are made to the ShoreTel database.
- Creates a Windows Event Log entry listing ShoreTel AD users which were not found by the LDAP search.
- Creates a Windows Event Log entry summarizing the results of the import.

### Requirements:

- ShoreTel Release 10.X and later.
- The ShoreTel system must be configured for Active Directory Integration.
- The application should run when the system is not busy, ideally, during off-hours

- The domain account running the application must have administrator rights on the ShoreTel server as well as Active Directory read access. AD write access is required if DID or extension numbers are saved in the AD.
- Phone numbers in Active Directory must begin with an optional '+' (plus) followed by the country code in order for the ShoreTel system to correctly dial the number.
- Knowledge of Active Directory and LDAP queries.

## Table of Contents

Introduction .....	1
Table of Contents .....	3
ShoreTel AD User Creation .....	4
Overview .....	4
User Creation Details .....	4
Active Directory Import Overview .....	5
Installation Prerequisites .....	5
Licensing .....	5
Installation .....	6
Configuration .....	7
Default User Parameters .....	7
Send Email When ShoreTel Users are Created .....	7
Application Command Line Options .....	8
Running the Application .....	12
Best Practices .....	12
Deployment Scenarios .....	12
Synchronize Existing ShoreTel AD Users .....	12
Migration from Legacy PBX .....	12
Creation of ShoreTel Users .....	13
Creation of ShoreTel Users from Multiple AD Forests .....	13
Restrictions .....	13
Event Log .....	14
Log Files .....	16
Application Log File .....	16
DB Import Log Files .....	17
Application Data File .....	18
Appendix A – System Directory LDAP Property Mapping Options .....	18
Appendix B – Application Command Line Options .....	19

## ShoreTel AD User Creation

This section describes the process for creating ShoreTel users from the Active Directory.

### Overview

Creating ShoreTel users is complex and requires more than 50 configuration parameters. Due to the large number of parameters, user configuration data will come from the following sources:

- User specific data from the Active Directory (see Appendix A) and the user login name contained in the “samAccountName” LDAP property.
- Default configuration values which apply to all created users.
- Manual configuration within ShoreTel Director for the following few parameters which cannot be automated:
  - DID Number
  - Caller ID
  - Non ShoreTel IM
  - Phone assignment

Listed below is the work flow for newly created users:

- Users are added to the Active Directory.
- The AD Import application creates the ShoreTel AD users and generates a Windows event log entry containing the created users.
- The ShoreTel System is configured to forward the event log entry to a ShoreTel Administrator to configure the remaining parameters for each user.

### User Creation Details

The application will run the ShoreTel DBImport utility to create ShoreTel AD users. A DBImport Template (“DBImportTemplate.csv”) file in the installation directory is used to specify the default configuration parameters.

The software creates a CSV file containing a line for each new user, executes the DB Import application, and then creates the Window Event Log entry listing the added users.

DB Import output and errors will be saved in the application log file.

## Active Directory Import Overview

The application is a Microsoft Windows console application which may be configured to run daily by the Windows Task Scheduler.

The application works as follows:

- Reads the “Active Directory Integration” system parameters from the ShoreTel database.
- Process the command-line parameters:
  - Determines the LDAP Path.
  - Determines if a LDAP filter is specified.
  - Determines which LDAP properties to retrieve.
- Performs the LDAP search and processes each record as follows
- Determine if this record should be excluded for the following reasons:
  - Is not an AD user record
  - There is no “First Name” LDAP property or if there is no “Last Name” LDAP property when creating ShoreTel AD users.
  - The record does not contain a phone number or IM address

Note: the above conditions may be caused by command line options which change the LDAP filter or change the returned LDAP properties.
- Excludes this record if the AD User matches a ShoreTel non-AD user.
- If this AD User is a ShoreTel AD User:
  - Update the System Directory information for this user (if needed)
  - If AD Import created a System Directory entry for this user, delete the entry (use case: non-ShoreTel AD user becomes a ShoreTel AD user)
- If a System Directory entry exists for this AD User, update the System Directory entry (if needed)
- Else either create a new ShoreTel user or create a System Directory entry for this new AD User.
- After processing all the AD Users, delete System Directory entries for AD Users which no longer exists (removed from AD or LDAP filter changed).
- If changes were made to the System Directory, notify the ShoreTel service of the changes.
- Create a Windows Event Log entry containing the summary of the import.

## Installation Prerequisites

### Licensing

The application is licensed per system. License errors (e.g., trial or temporary license expirations) will terminate the application after an error is written to the Windows Event Log.

The Application Licensing Server must be installed on the ShoreTel Headquarters (Director) server in order to install the Active Directory Import license key. The Application Licensing Server may be downloaded from the ShoreTel support website: <http://support.shoretel.com/products/applications/>

**NOTE:** The trial license will only import the first 5 (valid) AD users returned from the LDAP search into the ShoreTel System Directory. However, the application may be run in “test” mode (using the

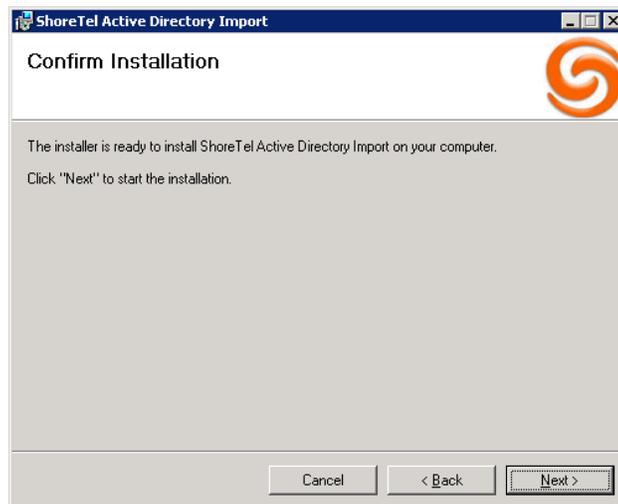
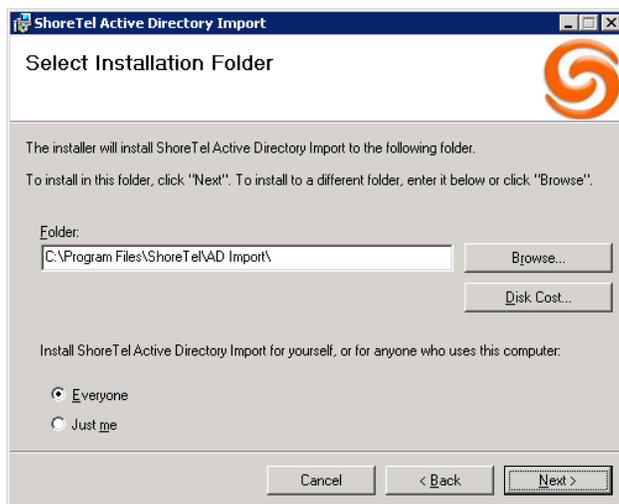
“-t” option) to log the changes needed to System Directory for all AD users returned from the LDAP search.

## Installation

The application must be installed on the ShoreTel Director (HQ) server.

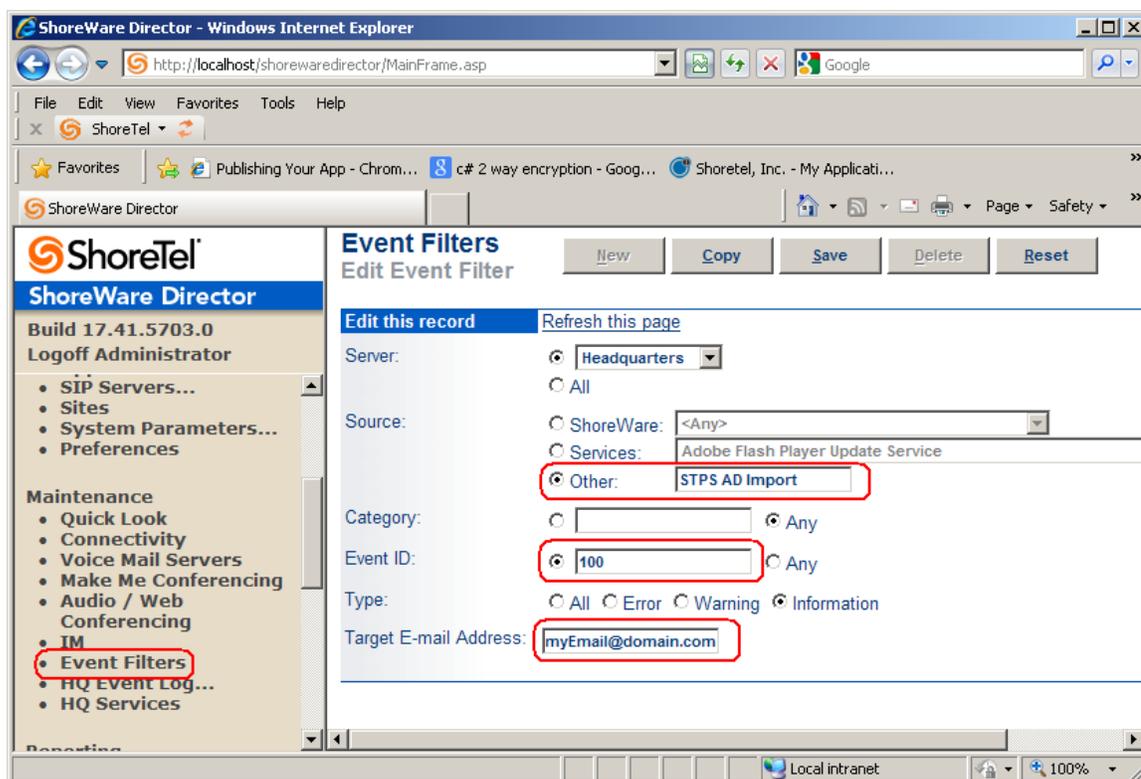
- You should have received a zip file named “STPSAdImport.X.Y.Z.zip”.
- Unzip the file to a folder.
- From the folder run the STPSAdImportSetup.exe.
- If you have not already installed the Microsoft .NET 2.0 runtime on the server you will be prompted to do so. If so, follow the prompts which should automatically download and install .NET from the Internet. Once this completes, continue with the install.

Follow the install prompts:





- “Target E-mail Address” must be configured with an email address



## Application Command Line Options

A command line option consists of a '-' (minus) followed by the option name and then followed by a space and optional command data. Square bracket surrounding an option name or option data indicates these are optional items. Command data must be enclosed in double quotes (") if it contains a '-'.

For example "-lp [<ldap path>]" indicates the "lp" option is required but the option data is not required. Note: "<ldap path>" indicates you would substitute this string with the actual LDAP path (e.g., "LDAP://pacifica.shoretel.com/dc=shoretel,dc=com"). An option specification of "[-c [<ldap property>]]" indicates the option can be omitted; only the option name may be specified, and both the option name and option data may be specified.

Listed below are the command line options:

- **[-t]**  
Runs the application in "test mode". Test mode logs the changes in the application log file but does NOT modify the system.
- **-lp [<LDAP path>]**  
Specifies the LDAP path. If the optional "LDAP path" is not provided, the application will use the configured LDAP path in ShoreTel Director.

**[-lf <LDAP filter>]**

Optional LDAP filter. The default LDAP filter to select active AD users is:

`(&(sAMAccountType=805306368)(!(objectClass=inetOrgPerson)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))` **Note:**  
Only user objects can be imported into the System Directory.

- **[-r]**  
Removes (deletes) all System Directory entries for non ShoreTel users that were created by this application.
- **[-a]**  
Only imports AD information for ShoreTel AD users. This option will not create ShoreTel AD users or System Directory for new AD users.
- **[-np [<prefix string>]]**  
Optional phone number prefix string. Ignores Active Directory phone numbers which do not begin with a '+' (default) or the specified prefix. Note: the invalid phone numbers are logged in the application log file when the log level is set to "WARNING".
- **[-f <property name>]**  
Overrides the default LDAP property name of "givenName" which is used for the user's first name. If the specified property name does not exist, this user will NOT be added to the System Directory.
- **[-l <property name>]**  
Overrides the default LDAP property name of "sn" which is used for the user's "Last Name" in the System Directory. If the specified property name does not exist, this user will NOT be added to the System Directory.
- **[-e <property name>]**  
Overrides the default LDAP property name of "userPrincipalName/mail" which is used for the user's "Email Address" in the System Directory. The "Email Address" is only updated if it is empty (not set) unless the "-ef" option is specified.
- **[-ef]**  
Specifies the AD email value should always be used for the user's "Email Address" in the System Directory. This option prevents users from assigning a different email address for voicemail notifications.
- **[-dn ]**  
Specifies the "displayName" LDAP property is used for the "First Name" and "Last Name" fields in the System Directory. If the "displayName" does not contain a comma, all characters up to the last space are used for the "First Name" and all characters following the last space are used for the "Last Name".
- **[-h [<property name>]]**  
Specifies the LDAP property used for the "Home Number" field in the System Directory. The default LDAP property is "homePhone". The "Home Number" will not be saved in the System Directory if only the -h option is provided or if the specified property name does not exist for the user. Note: Calls will not be placed properly unless the phone number in the Active Directory starts with an optional "+" followed by the country code.

- **[-w <property name>]**  
Specifies the LDAP property used for the “Work Number” field in the System Directory. The default LDAP property is “telephoneNumber”. The “Work Number” will not be saved in the System Directory if only the –w option is provided or if the specified property name does not exist for the user. Note: Calls will not be placed properly unless the phone number in the Active Directory starts with an optional “+” followed by the country code.
- **[-F<property name>]]**  
Specifies the LDAP property used for the “Fax Phone” field in the System Directory. The default LDAP property is “facsimileTelephoneNumber”. The “Fax Phone” will not be saved in the System Directory if only the –f option is provided or if the specified property name does not exist for the user. Note: Calls will not be placed properly unless the phone number in the Active Directory starts with an optional “+” followed by the country code
- **[-c [<property name>]]**  
Specifies the LDAP property used for the “Cell Phone” field in the System Directory. The default LDAP property is “mobile”. The “Cell Phone” will not be saved in the System Directory if only the –c option is provided or if the specified property name does not exist for the user. Note: Calls will not be placed properly unless the phone number in the Active Directory starts with an optional “+” followed by the country code
- **[-p [<property name>]]**  
Specifies the LDAP property used for the “Pager” field in the System Directory. The default LDAP property is “pager”. The “Pager” will not be saved in the System Directory if only the –p option is provided or if the specified property name does not exist for the user. Note: Calls will not be placed properly unless the phone number in the Active Directory starts with an optional “+” followed by the country code.
- **[-i [<property name>]]**  
Specifies the LDAP property used for the “IMUri” field in the System Directory. The default LDAP property is “msrtcip-primaryuseraddress”.
- **[-CN [<property name>]]**  
Specifies the LDAP property used for the “CompanyName” database field in the System Directory. The default LDAP property is “company”. Note: the company name is visible in ShoreTel Communicator’s directory tab.
- **[-d [<property name>]]**  
Specifies the LDAP property used for the “DepartmentName” database field in the System Directory. The default LDAP property is “department”. Note: the department name is visible in ShoreTel Communicator’s directory tab.
- **[-sd]**  
Saves the ShoreTel Active Directory users DID number in the AD LDAP default property “telephoneNumber” or the LDAP property associated with the “Work Number”. The users DID number will be formatted as “+1 (nnn) nnn-nnnn” for NANP (US) phone numbers and will be an unformatted number (e.g., “+nnnnnnnnn...”) for all other countries. The AD is only updated if the phone number digits (excludes formatting characters) are different.

- **[-SD]**  
Saves the ShoreTel Active Directory users DID number in the AD LDAP default property “telephoneNumber” or the LDAP property associated with the “Work Number”. The users DID number will be formatted as “+1 (nnn) nnn-nnnn” for NANP (US) phone numbers and will be an unformatted number (e.g., “+nnnnnnnnn..”) for all other countries. The AD is only updated if the number strings are different.
- **[-se [<property name>]]**  
Saves the ShoreTel Active Directory users extension number in the AD LDAP default property “otherTelephone” or in the specified LDAP property.
- **[-cd]**  
Creates ShoreTel System Directory entries for new AD users.
- **[-cu [<filename>]]**  
Creates ShoreTel AD users for new AD users based on information in the AD and the default configuration parameters specified in the DB Import Template csv file.
- **[-ns]**  
Do not synchronize the ShoreTel services with the database. This option is used when running multiple AD Imports from command (bat) file so the synchronization only occurs on the last AD Import command.
- **[-OF <filename>]**  
Reads the command line options from the specified filename. Each command option must begin on a new line. The optional command data may follow the command option and span multiple lines.

## Running the Application

The name of the executable for the application is “STPSADImport.exe”.

The application is run using the following command:

```
<installation folder>\STPSADImport.exe -lp <optional command line parameters>
```

**WARNING:** The application should always be run first in test mode (-t option) to prevent unexpected changes to the System Directory.

**Note:** By default the application will not run with administrator access when running on Windows 2008 with UAC. You must either disable UAC or configure the Task Scheduler to run the application with administrator privileges

## Best Practices

The following procedure is highly recommended to ensure that the proper data is imported into the the ShoreTel database:

1. Run the application in test mode (-t option) and examine the log file to verify the changes which would be made to the ShoreTel database.
2. Run the application **without** the “-t” option to test the importing of data for a specific user by setting an LDAP filter (e.g., “-lf (samaccountname=userName)”).
  - Note: the log file and Event Log entry will falsely indicate ShoreTel AD users may be deleted because they were not found in the AD.
  - Examine the log file and verify the change using ShoreTel Director.
3. Finally, run the full command

## Deployment Scenarios

### Synchronize Existing ShoreTel AD Users

The following command synchronizes existing ShoreTel AD users with the AD:

```
STPSADImport.exe -lp
```

This command will not create new ShoreTel AD users or System Directory entries.

### Migration from Legacy PBX

The following command creates System Directory entries for non-ShoreTel AD users so ShoreTel users can easily communicate with non-ShoreTel users:

```
STPSADImport.exe -lp -cd
```

When a ShoreTel Administrator manually creates a ShoreTel AD user account for this user, the

application will remove the previous created System Directory entry.

This approach is most usefully when the migration will occur over a long time period.

## Creation of ShoreTel Users

The following command creates new ShoreTel AD users when users are added to the AD:

```
STPSADImport.exe -lp -cu
```

The ShoreTel administrator complete the configuration for each added user.

## Creation of ShoreTel Users from Multiple AD Forests

ShoreTel users can be created from multiple AD forests by running the application twice; once for each AD forest.

A Windows command (“bat”) is run containing the following:

```
STPSADImport.exe -lp -cu -ns  
STPSADImport.exe -lp <ldap path to other AD forest> -cu “c:\temp\DBImportTemplatate.csv”
```

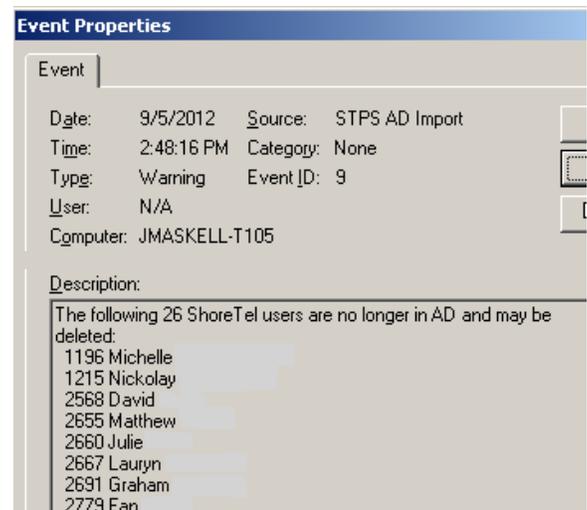
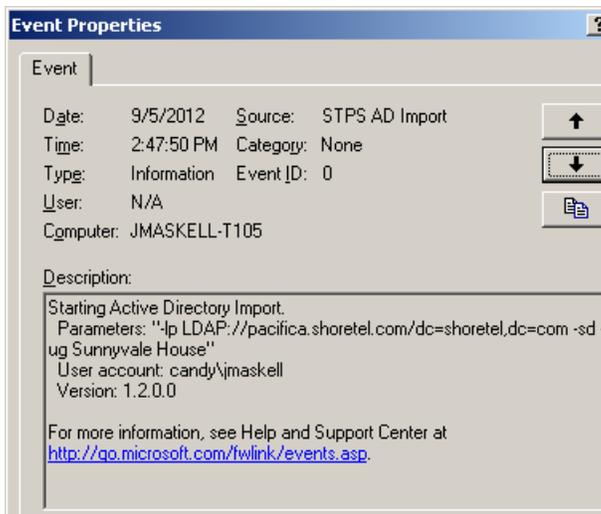
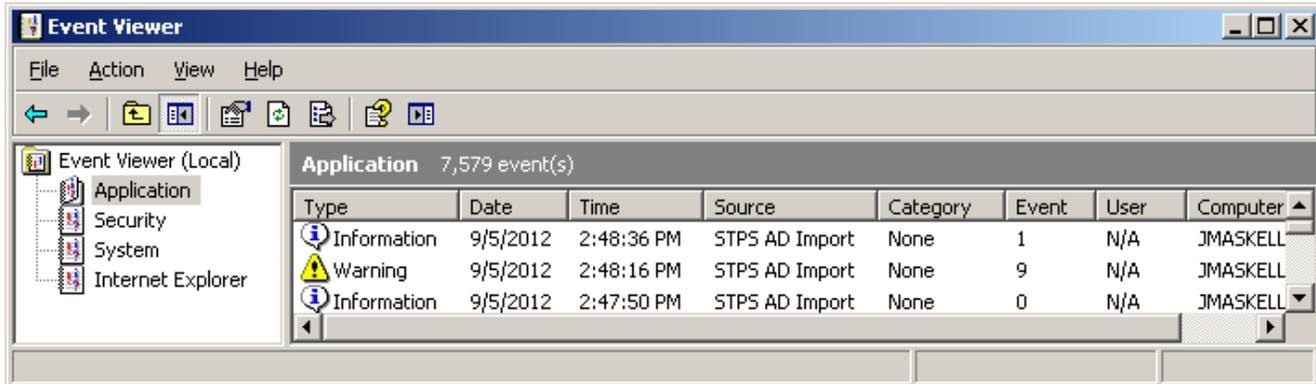
The first line performs the import using the configured LDAP path in the ShoreTel server and is set to not resynchronize the ShoreTel services with the database since another import will be run. The second line performs the import using the specified LDAP path for the other AD forest.

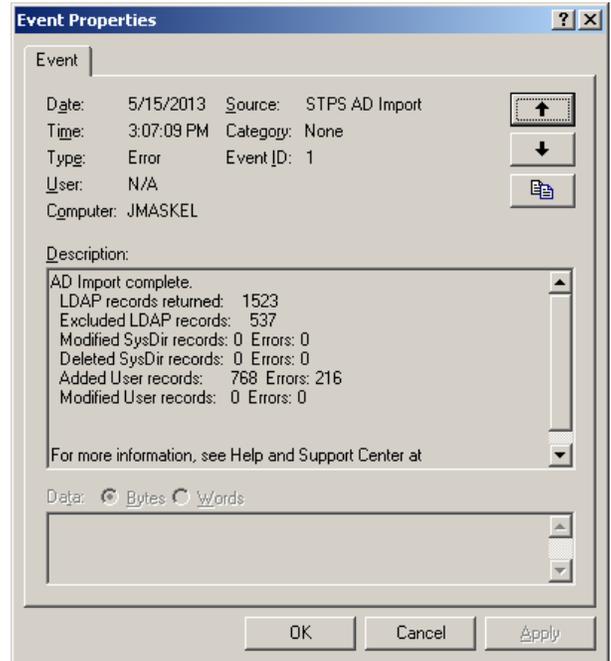
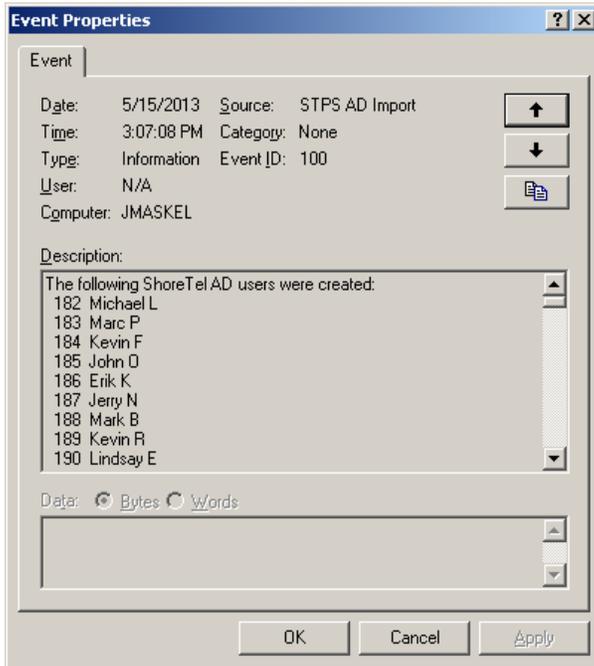
## Restrictions

- You cannot run the application to create ShoreTel AD Users if the application has previously been run to create System Directory entries. You must remove the previously created System Directory entry by running the application with the “-r” option.
- Running the application with a different LDAP path or a different LDAP filter will create a Windows Event Log entry listing the ShoreTel AD users which were not found by the LDAP search.

## Event Log

The application logs information in the Windows Event Log. Listed below are some of the events logged when the application starts, creates ShoreTel AD Users, and ends.





## Log Files

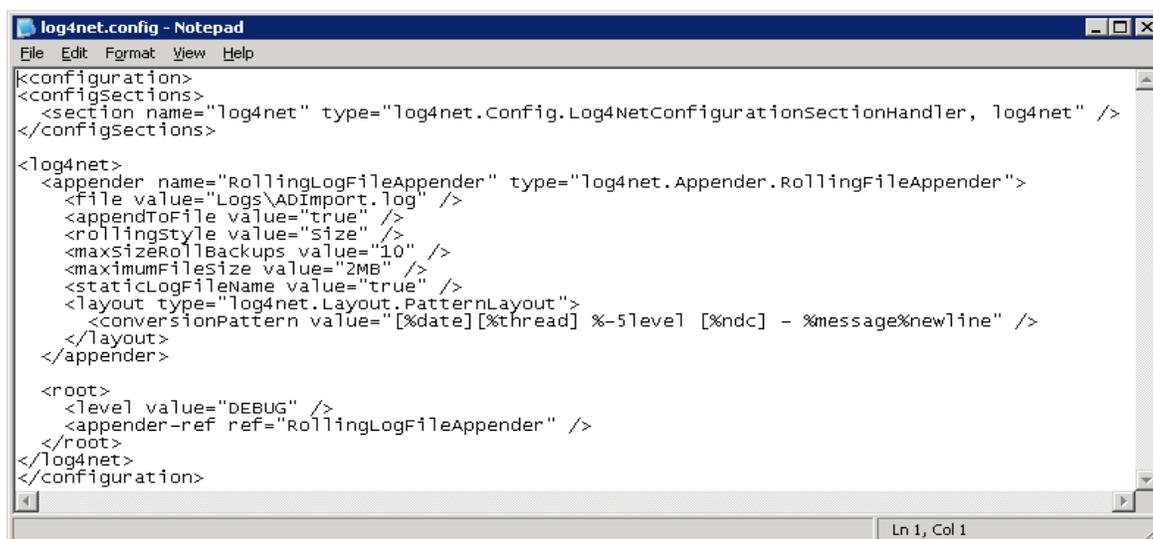
### Application Log File

By default, the application will write a log file containing informational and error messages. The logging feature allows more or less details to be logged by editing the logging XML file. The application will log all changes made to the ShoreTel System Directory include changes when running in “test” mode (-t option).

As configured, the application will maintain a rolling history of up to 10 log files with a maximum of 2 Megabytes in each file.

The application log files are named “ADImport.log” and are stored in the “Logs” subfolder.

The XML file which controls the logging is named log4net.config. If you edit the file with (for example) notepad.exe, this shows the contents of the file:



```

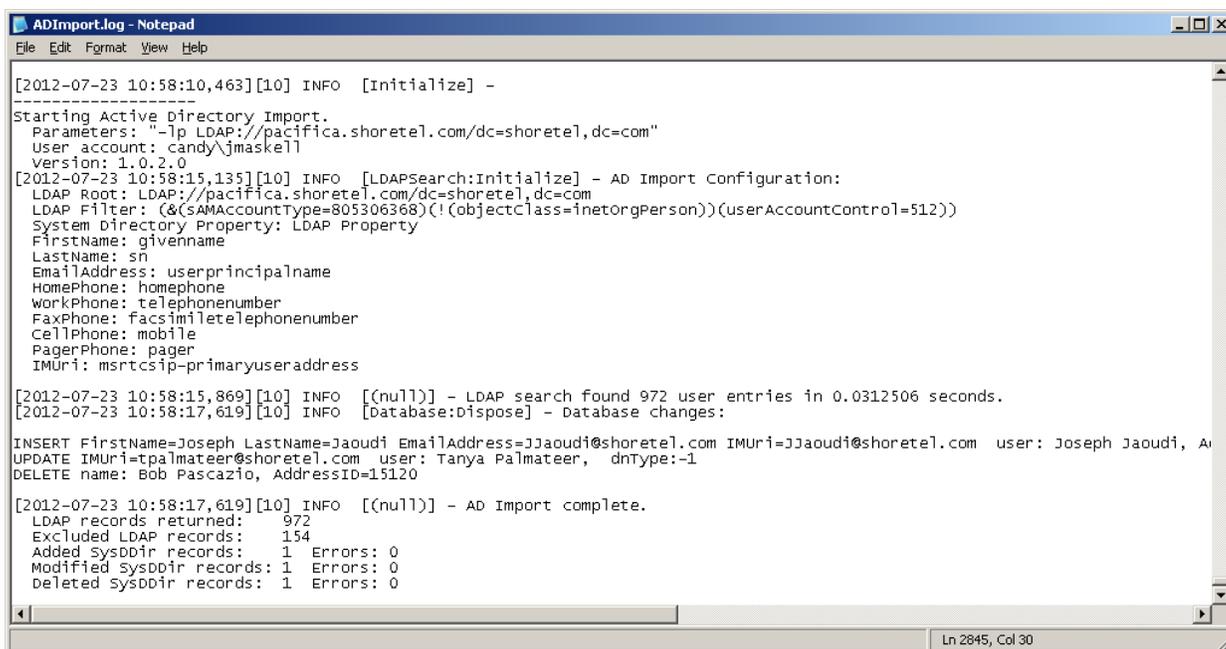
log4net.config - Notepad
File Edit Format View Help
<configuration>
<configSections>
<section name="log4net" type="log4net.Config.Log4NetConfigurationSectionHandler, log4net" />
</configSections>
<log4net>
<appender name="RollingLogFileAppender" type="log4net.Appender.RollingFileAppender">
<file value="Logs\ADImport.log" />
<appendToFile value="true" />
<rollingStyle value="Size" />
<maxSizeRollBackups value="10" />
<maximumFileSize value="2MB" />
<staticLogFileName value="true" />
<layout type="log4net.Layout.PatternLayout">
<conversionPattern value="%date [%thread] %-5level [%ndc] - %message%newline" />
</layout>
</appender>
<root>
<level value="DEBUG" />
<appender-ref ref="RollingLogFileAppender" />
</root>
</log4net>
</configuration>
Ln 1, Col 1

```

To change the level of detail logged, you would want to change the "level value" in the root section and save the changes. Changes to the log level do NOT require a service restart. The above screen shot shows the value. The valid values in order of increasingly detailed logging (each level includes lower levels) are as follows:

- FATAL Only fatal errors are logged.
- ERROR Errors are logged.
- WARN Warnings are logged.
- INFO Informational events are logged.
- DEBUG All logging is enabled.

Listed below is a sample log file:



```

ADImport.log - Notepad
File Edit Format View Help

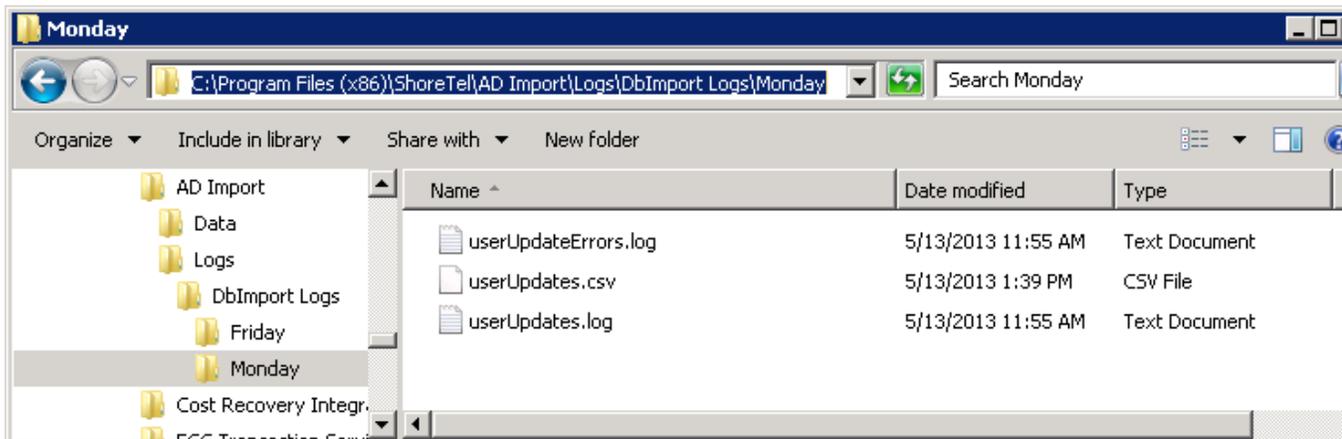
[2012-07-23 10:58:10,463][10] INFO [Initialize] -
-----
Starting Active Directory Import.
Parameters: "-lp LDAP://pacificca.shoretel.com/dc=shoretel,dc=com"
User account: candy\jmaske11
Version: 1.0.2.0
[2012-07-23 10:58:15,135][10] INFO [LDAPSearch:Initialize] - AD Import Configuration:
LDAP Root: LDAP://pacificca.shoretel.com/dc=shoretel,dc=com
LDAP Filter: (&(sAMAccountType=805306368)(!(objectClass=inetorgPerson))(userAccountControl=512))
System Directory Property: LDAP Property
FirstName: givenname
LastName: sn
EmailAddress: userprincipalname
HomePhone: homephone
WorkPhone: telephonenumber
FaxPhone: facsimiletelephonenumber
CellPhone: mobile
PagerPhone: pager
IMUri: msrtcslp-primaryuseraddress

[2012-07-23 10:58:15,869][10] INFO [(null)] - LDAP search found 972 user entries in 0.0312506 seconds.
[2012-07-23 10:58:17,619][10] INFO [Database:Dispose] - Database changes:
INSERT FirstName=Joseph LastName=Jaoudi EmailAddress=JJaoudi@shoretel.com IMUri=JJaoudi@shoretel.com user: Joseph Jaoudi, A
UPDATE IMUri=tpalmateer@shoretel.com user: Tanya Palmateer, dnType=-1
DELETE name: Bob Pascazio, AddressID=15120

[2012-07-23 10:58:17,619][10] INFO [(null)] - AD Import complete.
LDAP records returned: 972
Excluded LDAP records: 154
Added sysDDir records: 1 Errors: 0
Modified sysDDir records: 1 Errors: 0
Deleted sysDDir records: 1 Errors: 0
  
```

## DB Import Log Files

DB Import log files are located in the “Logs\DBImport Logs\” subfolders as shown below.



The three files are:

- userUpdateErrors.log contain errors from DB Import.
- userUpdates.csv contains the DB Import input file containing a line for each user to create.
- userUpdates.log is the DB Import log file.

## Application Data File

The application uses a data file to record which System Directory entries have been made for non-ShoreTel AD users. The data file is named “SysDirEntries.csv” and is in the “Data: installation subfolder.

This file must NOT be modified since the application requires this file to prevent the creation of duplicate System Directory entries and for deleting previously added System Directory entries.

## Appendix A – System Directory LDAP Property Mapping Options

Option	System Directory Field	Default LDAP Property	Disable
-f	First Name	givenName	
-l	Last Name	sn	√
-h	Home Phone	homePhone	√
-w	Work Phone	telephoneNumber	
-F	Fax Phone	facsimileTelephoneNumber	√
-c	Cell Phone	mobile	√
-p	Pager Phone	pager	√
-e	E-mail Address <sup>1</sup>	userPrincipalName/mail	√
-i	IMUri <sup>2</sup>	msRTCSIP-PrimaryUserAddress	√
-CN	CompanyName <sup>2</sup>	company	√
-d	DepartmentName <sup>2</sup>	department	√

<sup>1</sup> The default email LDAP property “userPrincipalName” can be overridden to use the “mail” LDAP property by a ShoreTel registry key.

<sup>2</sup> These are internal ShoreTel names which are not visible.

## Appendix B – Application Command Line Options

Option	Option Data	Required	Description
-t			Runs in “test mode” which only logs changes into the log file.
-r			Removes all System Directory entries added by the application.
-lp	LDAP Path (optional)	√	Overrides the ShoreTel configured LDAP path with the specified LDAP path.
-lf	LDAP Filter		Overrides the default LDAP filter (selects “enabled users”) with the specified filter.
-dn			Use AD “displayName” for First and Last names
-ef			Always import users AD email address.
-sd			Save user’s DID in the AD LDAP property specified for the Work Phone.
-SD			Same as above except the entire number string is used to determine if the numbers differ.
-se	LDAP Property		Save user’s extension number in the AD LDAP property “otherTelephone” if a LDAP property is not specified.
-np	Number prefix string (optional)		Ignores Active Directory phone numbers which do not begin with a ‘+’ (default) or the specified prefix.
-cd			Create System Directory entries for new AD users.
-cu	Filename		Create ShoreTel AD users for new AD users.
-ns			Do not synchronize the ShoreTel services with the database.
-OF	Filename		File containing the command line options.