

Software Procedure

SWP-0003 tConsult Server Active Directory Integration

Revision: 3

Effective Date: 7/28/2010

Alaska Native Tribal Health Consortium
Division of Health Information & Technology
4000 Ambassador Drive
Anchorage, AK 99508
Tel: (907) 729-2260
Fax: (907) 729-2269



Contents

Purpose.....3

Audience.....3

Scope.....3

Additional Resources3

Acronyms and Abbreviations.....4

Active Directory Preparation4

tConsult Server Preparation7

Using AD Manager from AFHCAN tConsult Server.....9

Common Errors that may be Encountered.....16

Purpose

The purpose of this document is to detail the necessary steps to integrate the AFHCAN tConsult Server software within Active Directory for Domains.

Audience

This document applies to persons who work in the Information Technology department within Domains and have a basic working knowledge of Active Directory for Windows Server.

Scope

As a measure of security, many applications require a secondary logon to that of the Domain User account. AFHCAN recognized the increased burden to users to remember multiple passwords and developed the means to integrate their logon into the tConsult software application with that of their Domain User account. Most organizations have instituted the policy of requiring password changes of the Domain User account every 90 days. This process will eliminate the necessity of having to change the password within the tConsult software and reduce the possibility of a user forgetting what their password might be.

The overall process involves creating Security Groups within AD that mirror the Security Roles within the tConsult software. Adding Domain Users to the appropriate Security Group within AD automatically uploads to the tConsult Server once per day as a scheduled task run from the tConsult Server. This reduces the burden on the IT staff.

Additional Resources

SWP-0004 Joining tConsult Servers to a Domain

SWP-0005 How to Establish an Authoritative Time Source

SWP-0007 AFHCAN tConsult Server Software v5.X Installation Procedures

SWP-0023 AFHCAN tConsult Server Software Upgrade Procedures

SWP-0010 tConsult Licensing

Acronyms and Abbreviations

Table 1 lists the abbreviations and acronyms used in this document.

Table 1 Acronyms and abbreviations

Acronym	Meaning
SWP	Software Procedures
IT	Information Technology
AD	Active Directory
WCF	Windows Communication Foundation

Active Directory Preparation

This section outlines the steps to create a service account to be used by the tConsult Server Service and five new Security Groups that will mirror the roles within the tConsult software.

1. Within Active Directory Users and Computers, select the Users OU, and create a new Domain user. This account will be used as a *service account* by the tConsult Server Service.

The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: TEST2.local/Users'. Below that, there are several input fields: 'First name' with 'Service', 'Initials' (empty), 'Last name' with 'Account', and 'Full name' with 'Service Account'. Under 'User logon name', there is a text box with 'ServAccount' and a dropdown menu showing '@TEST2.local'. Below that, 'User logon name (pre-Windows 2000)' has a text box with 'TEST2\' and another with 'ServAccount'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 1 – New User creation dialog box

2. Use a complex password and ensure that the user account password is set to never expire.

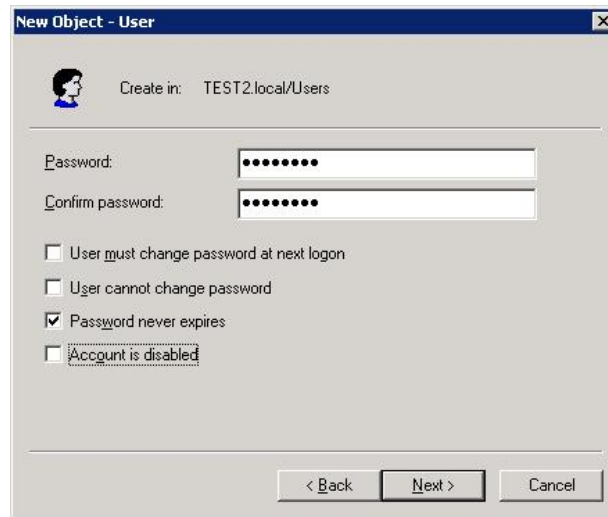


Figure 2 – New User creation dialog box cont'd

3. The newly created user account is a member of *Domain Users* only.

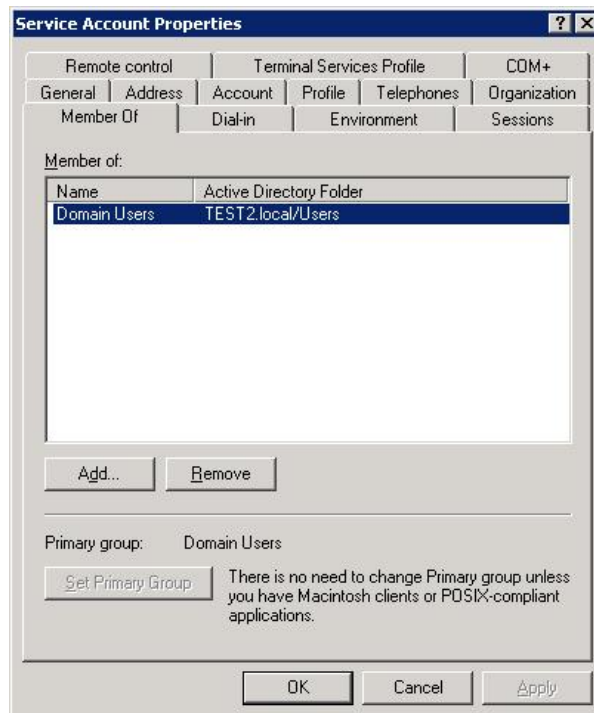


Figure 3 – Service Account Group Member Properties

4. The five roles within the tConsult software are:

Table 2 Roles and Activities associated with each role within tConsult software

Test User	Can only create test cases
Clinical Consultant	Can review and respond to test or real cases, cannot create cases
Clinical User	Can create test or real cases, can review and respond to cases
Clinical Admin	Performs as a Clinical User, but can also add providers, create groups, and manage alerts
System Admin	Can do all of the above plus manages server connections (trusts between organizations)

Create five new Security Groups. Each of these groups will perform one of five roles within the tConsult software as shown in Table 2. (Note: Naming convention for these security groups is up to the organization. It is recommended that the name be representative of the role.)



Figure 4 –New Security Group dialog box

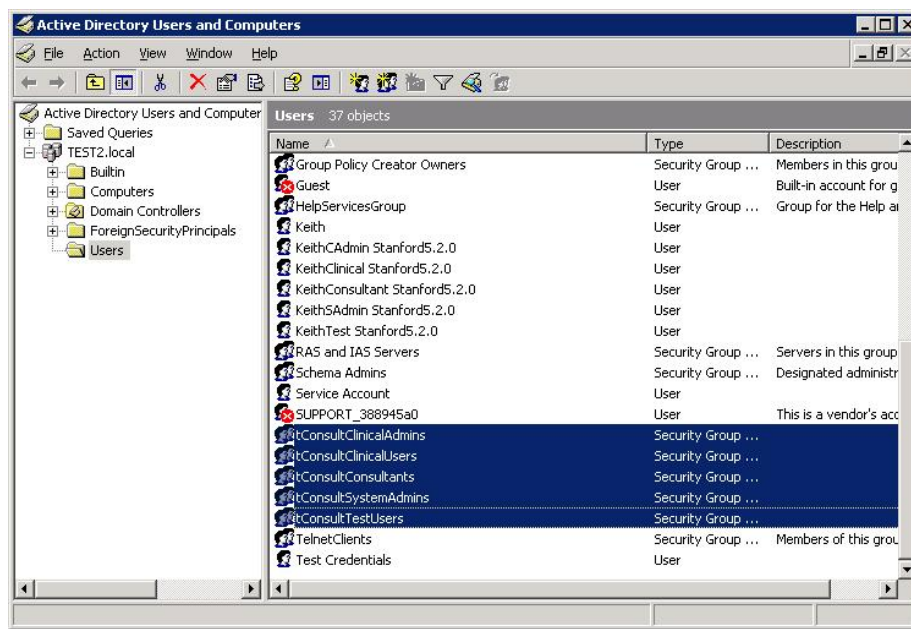


Figure 5 – Active Directory Users and Groups

5. Add each Domain user who utilizes tConsult software in one of the five roles to the appropriate AD Security Group. Ensure that each user has a first name, last name and email account.

tConsult Server Preparation

This section outlines the steps to be accomplished to prepare the tConsult Server for Active Directory integration.

1. The tConsult Server must be a member of a Domain. If the server is not already a member of the Domain, logon to the tConsult server with an administrative account and join it to the domain using a Domain Administrator account.
(Note: If this is an AFHCAN built server, or was built in accordance with AFHCAN specifications, please refer to SWP-0004 Joining tConsult Servers to a Domain.)
2. tConsult Software now uses WCF (Windows Communications Foundation) to authenticate users. As a result, tConsult Server needs an authoritative time source. If one exists for the Domain, no further action is needed, please proceed to step 3.

If a Domain is not utilizing an authoritative time source, please refer to SWP-0005 How to Establish an Authoritative Time Source. Enable the w32Time service within Services under Computer Management.

3. Enabling Ports on the Windows Firewall. tConsult Servers uses Windows Firewall as part of the overall security strategy. By default, only 3 ports are open: HTTP port 80, HTTPS port 443 and RDP port 3389. WCF and Time Server requires two additional ports be enabled.

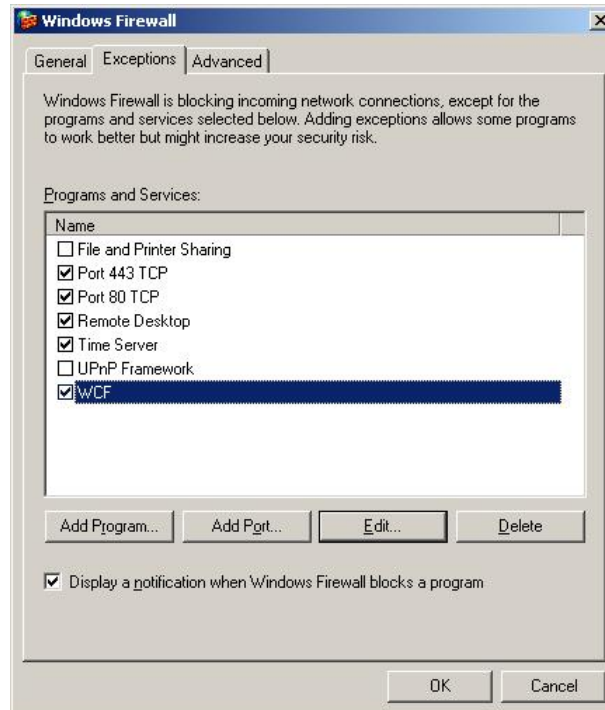


Figure 6 – Windows Firewall – Exceptions

Select Add Port and enter WCF, Port 6968, TCP

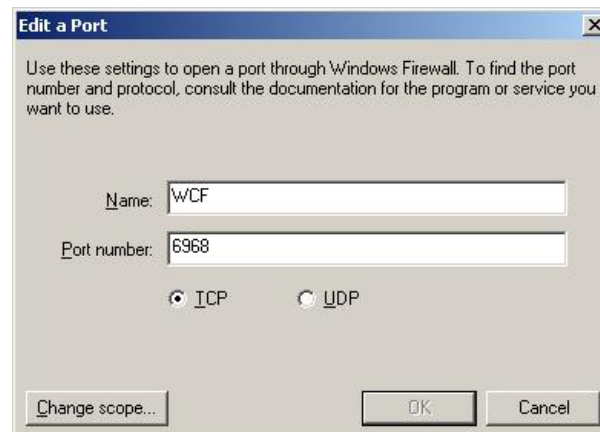


Figure 7 – Adding WCF Port

Select Add Port and enter Time Server, Port 123, UDP

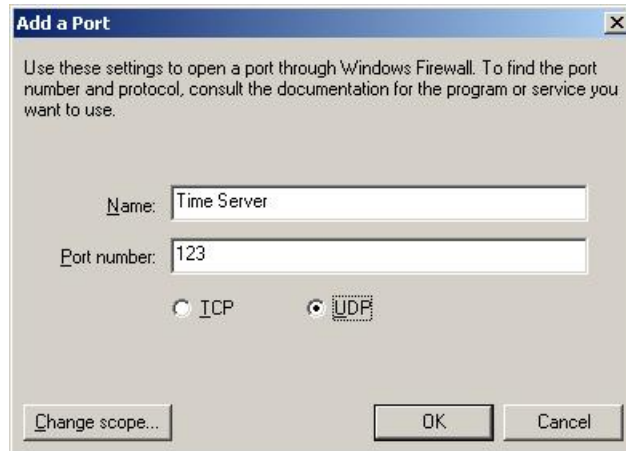


Figure 8 – Adding Time Server Port

4. Add the Domain User service account created in the Active Director Preparation (step 1) to the local administrators group on the tConsult Server.
5. tConsult Server software v5.2.x or greater must be installed. Please refer to SWP-0007 AFHCAN tConsult Server Software v5.X Installation Procedures if a new installation or SWP-0009 AFHCAN tConsult Server Software Upgrade Procedures if an upgrade is necessary.

Using AD Manager from AFHCAN tConsult Server

In this section, the detailed steps are provided for the actual integration between tConsult Server and Active Directory. There are two modes with which to run tConsult Server when using Active Directory:

1. **Mixed Mode:** This allows a combination of local tConsult accounts from within the software and Active Directory accounts that have been merged with tConsult Server for authentication. This can lead to duplicate accounts and creates a workload for both IT and Clinical Admin personnel.
2. **Full Active Directory Integration:** This allows only Active Directory accounts that have been merged with tConsult Server for authentication. From a Domain perspective, this is the easiest for IT support as all they will need to do is add/remove users from the appropriate AD Security Group created in the first section of this document.

IMPORTANT NOTE: *Once an organization has made the decision to use Active Directory Integration and completes this section, the software is NOT designed to reverse the authentication configuration.*

It is best to not have personnel using the tConsult software during this process.

1. Log on to the tConsult Server and add the service account created within Active Directory to the Local Administrators group within Computer Management.
2. Use this service account for the tConsult Server Service logon vs. the local system account.

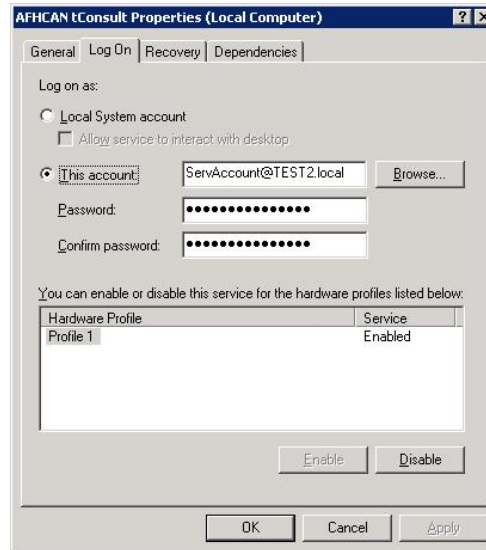


Figure 9 – Using Domain Service Account as Logon

3. Restart the tConsult Server Service.
4. Start AFHCAN tConsult Server. At the Opening dialog box, select **AD Manager** from **Options**.

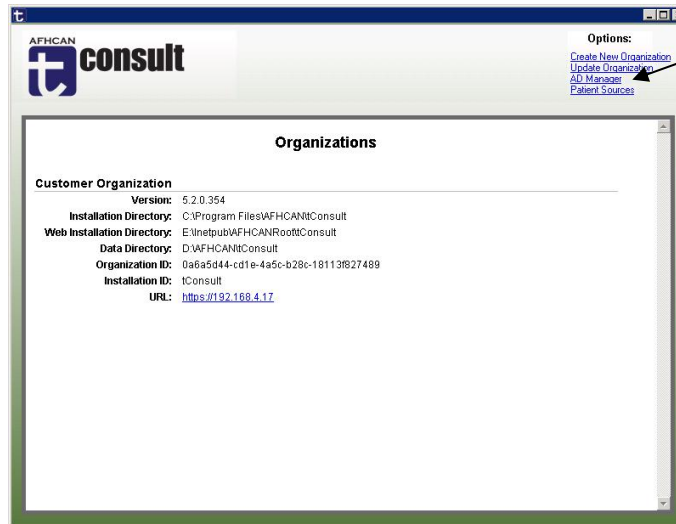


Figure 10 – Start up Screen for AFHCAN tConsult Server

5. Using the drop-down arrow, select the organization that will be integrated within Active Directory.

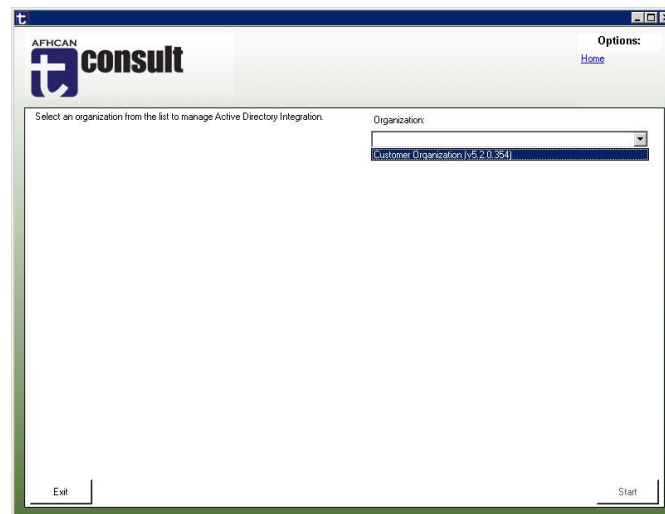


Figure 11 – Selecting Organization

6. Enter the IP address or name of the Active Directory Domain Controller that will be used for authentication. Then enter a valid Domain Administrator account and password. Click on *Authenticate User*.

Figure 12 – Entering IP/Host Name and valid Domain Admin account information

7. Once successfully authenticated, click on **Enable**. As a last cautionary note – this action is non-reversible. Clicking on **OK** will enable Active Directory authentication.

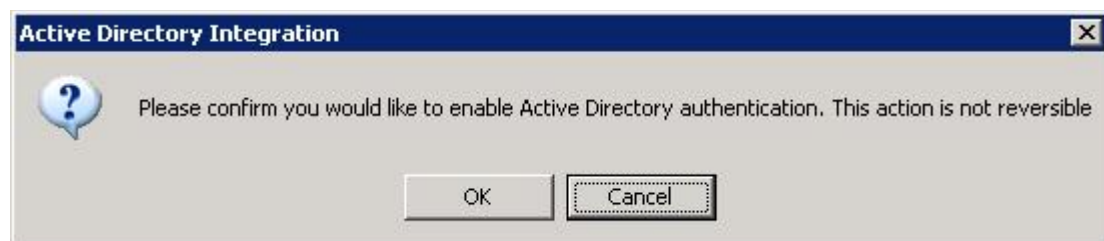


Figure 13 – Verification dialog box for Active Directory Integration

8. Enter the five Security Groups created in Active Directory during the first section of this document. What is entered here must exactly match the names from Active Directory.

Active Directory Group	tConsult Role
iConsultSystemAdmins	System Administrators
iConsultClinicalAdmins	Clinical Administrators
iConsultClinicalUsers	Users
iConsultTestUsers	Test Users
iConsultConsultants	Consultants

Figure 14 – Entering Active Directory Security Groups

Keep the checkmark in front of **Allow Users to merge their own tConsult and AD accounts** only if it is desired to run tConsult software in mixed mode. Allowing email notifications is up to the organization, however it is recommended when a new tConsult account has been

created via AD integration that an email alerts the user to when he/she can log into the tConsult software.

Click on *Next*.

- Figure 15 is a sample screenshot of the AD Manager that has compared tConsult accounts to those found in the AD Security Groups. The first are those accounts that are an Exact Match. The default action for Exact Matches is “Merge”.

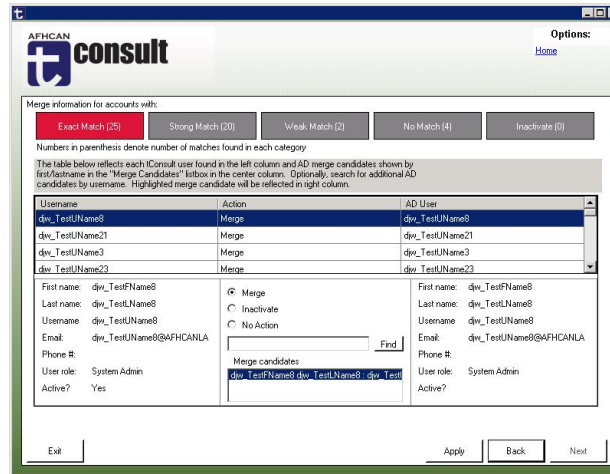


Figure 15 – Merging Information for Accounts

Should an account need to be inactivated, highlight the account in question and select the Inactivate radio button. (Note: It will still read Merge under Action until the mouse is moved to a different account. At that time, it will change to read Inactivate).

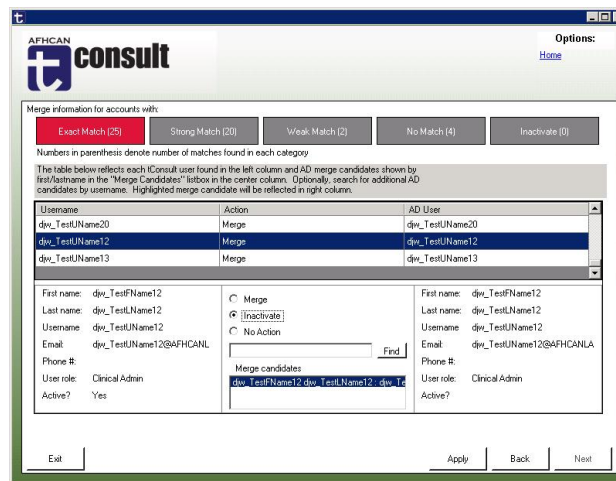


Figure 16 – Merging to Inactivate Information for Accounts

No Action radio button: **For fully integrated Active Directory every account must be merged or inactivated.** Every single account needs to be addressed. When it has been determined that all accounts are correct, click on *Apply*. Upon completion, the dialog box will advance to the Strong Matches if there are any. If there aren't any strong matches, it will go to Weak Match, then No Match.

- AD Manager will stop at Inactivate if there are any accounts that have been marked for Inactivate.

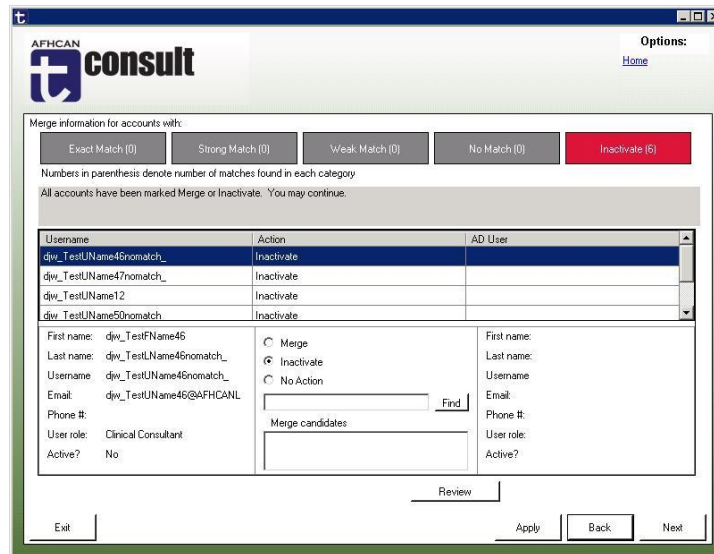


Figure 16 – Inactivating accounts

Click on the *Review* button to review each account if necessary.

- Once AD Manager has determined that all accounts have been accounted for, click on *Apply*, and then click on *Next*.

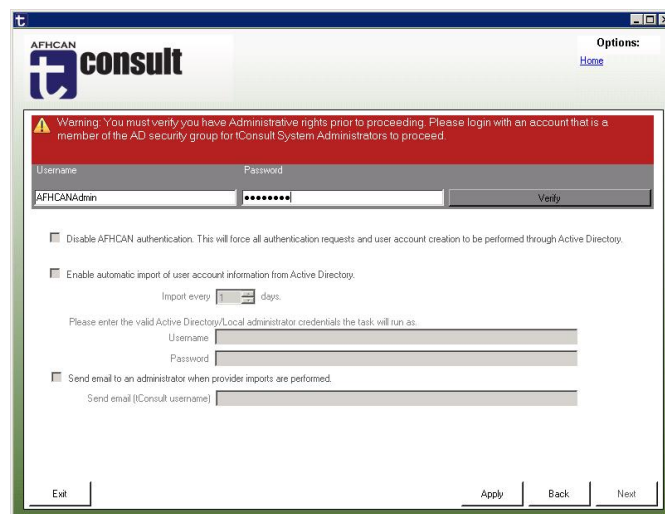


Figure 17 – Merging Information for Accounts

Enter a Username and Password of an account that is a member of the tConsult System Admin AD Security Group, then click on *Verify*.

12. The first checkbox will become active and is used to Disable AFHCAN authentication and use only user account information through Active Directory. **Place a checkmark** here to enforce the Full Active Directory Integration. Click on ***Apply***.

Figure 18 – Disabling AFHCAN authentication

13. Once apply has been clicked from Step 12, the next checkbox will become active. This will set up a scheduled task to be completed at the organizations time schedule to import any new user accounts that have been added by the IT support staff and placed into the appropriate tConsult Security Group within AD. **Enter the Service Account name and password** created in Step 1 of the first section.

Figure 19 – Setting of Scheduled Import Task

Sending of an email to an administrator when provider imports are performed are at the discretion of the organization. Click on ***Apply***.

Note: At this time it will appear that no action has taken place, Click on **Next**.

14. This last step within AD Manager may be used if any inactivated user accounts were not merged. To see these inactivated user accounts, click on the Dry-Run Import Users, however if all accounts were successfully merged, click on **Exit** to return to the AFHCAN tConsult Server.



Figure 20 – Finishing AD Manager

Common Errors that may be Encountered

With full Active Directory Integration, providers may only be added through Active Directory and made a member of the appropriate AD Security Group. This is by design and not an error.

AD Manager will not process any merges if the number of tConsult client licenses are exceeded. Purchase and install more licenses. (Please refer to SWP-0010 tConsult Licensing.)

When first setting up AD Manager, the User account will not validate. Ensure the user account is a member of the Domain Admin group.

Unable to verify user account for merging. Ensure the user is a member of the tConsult System Admins AD Security Group.

The system will not setup a scheduled task to import AD users. Ensure that the service account used for the scheduled task is a member of the Local Administrators group.

End of procedure.