Application Note

ShoreTel®

AN-10233
June 2009

ShoreTel 9: Active Directory Integration

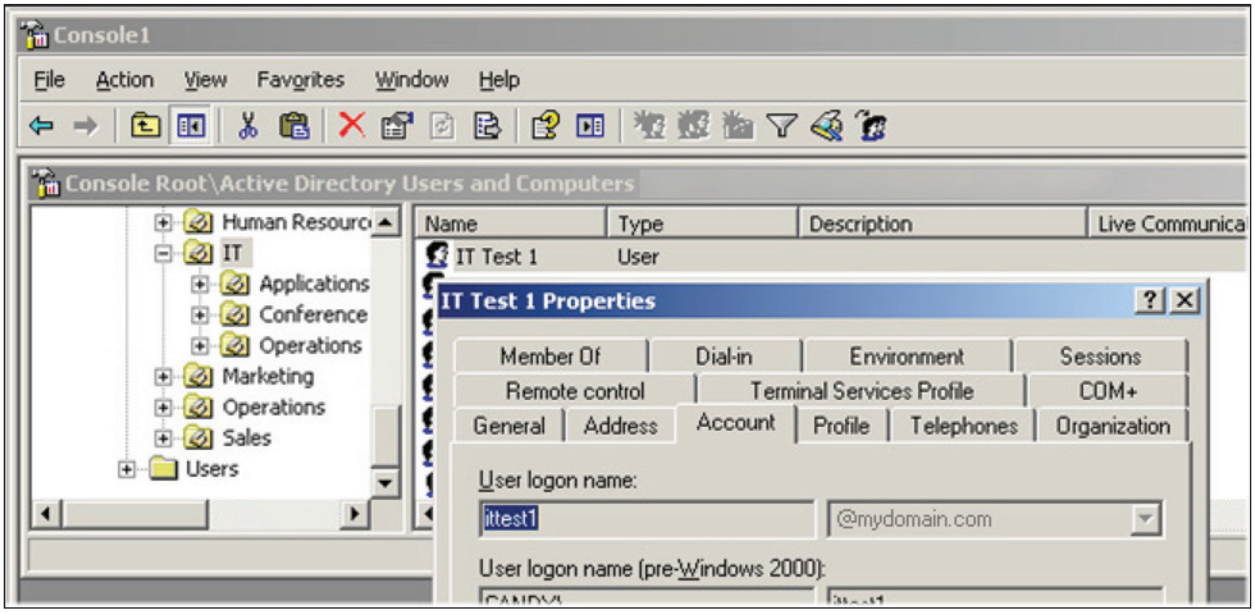
This application note outlines the configuration required to prepare a customer's Microsoft Active Directory environment for use with ShoreTel 9 or later. To effectively understand and implement this application note, the reader must have a working knowledge of both Microsoft Active Directory and ShoreWare® Director.

Integration checklist

When a customer chooses to use the Microsoft Active Directory feature in ShoreTel 9 or later, they must have a fully functional Microsoft Active Directory deployment with a populated user database.

Step 1 : Identify user as ShoreWare System Administrator

From the Microsoft Active Directory administration console, identify (or create if required) the user in Microsoft Active Directory whose identity is to be associated with the system administrator role in ShoreWare Director. In the following example, a user with the login name of "ittest1" will be a ShoreWare System Administrator.



Name	Type	Description	Live Communica
IT Test 1	User		

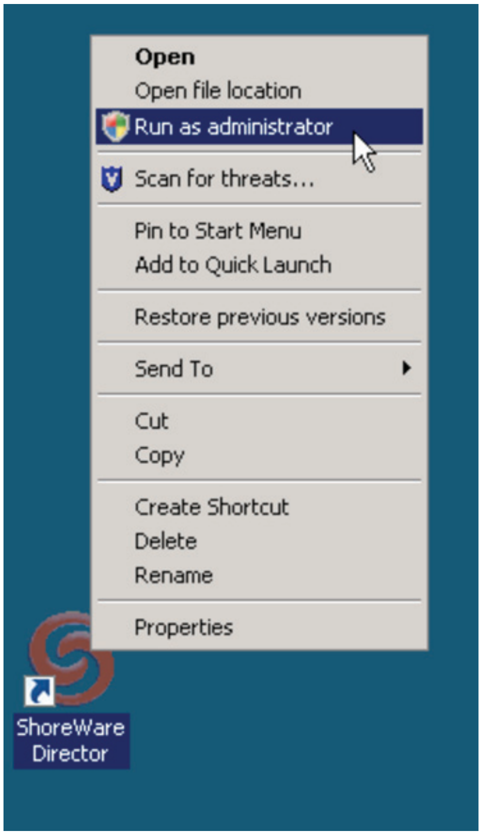
User logon name: ittest1 @mydomain.com

User logon name (pre-Windows 2000):

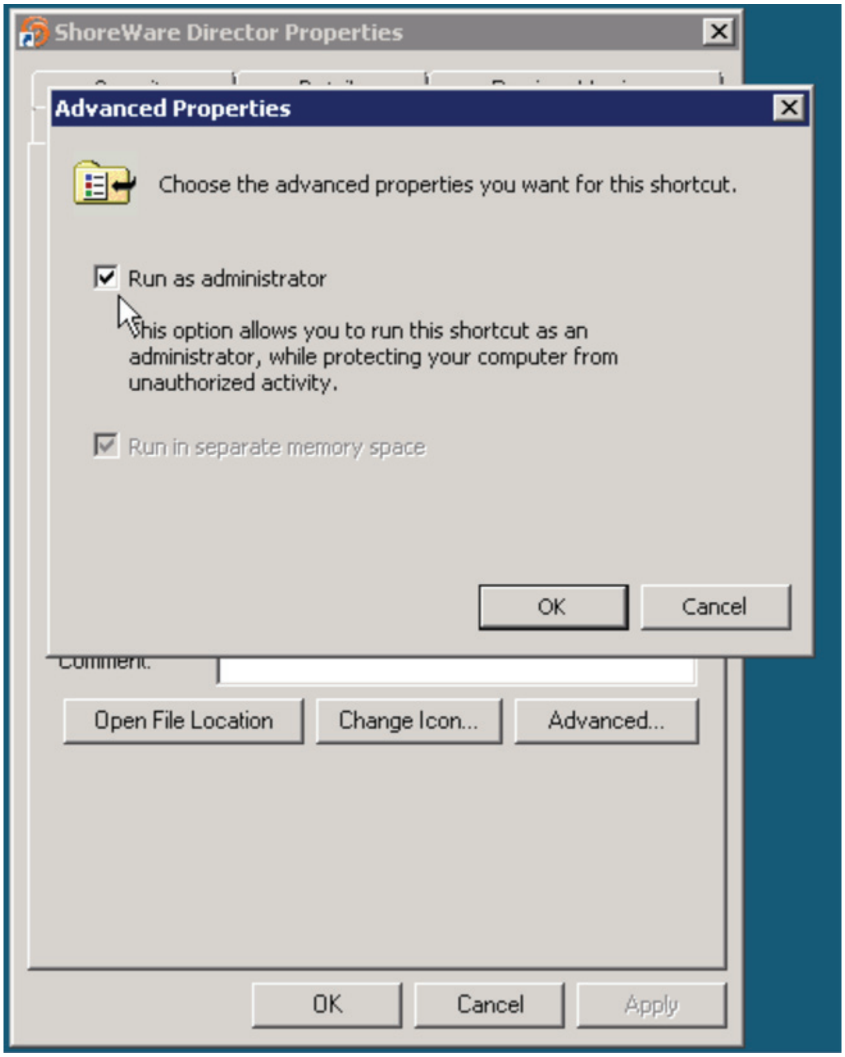
Please note that starting with ShoreTel 9.1, ShoreWare can be installed on the Windows 2008 Server. This version of the operating system introduced a new User Account Control (UAC) security configuration that causes problems with ShoreWare Director access for Microsoft Active Directory users configured as members of the local administrators group on the HQ server. Active Directory domain administrators and the default local administrator account are not affected and they can continue to access ShoreWare Director as they normally would.

Two solutions are available to mitigate this problem:

a) The ShoreWare Director desktop shortcut now provides the option to "Run As Administrator" for these users, so they will need to do this before launching Director.



b) Alternatively, the system can be set up to always run the ShoreWare Director shortcut as an administrator by changing the configuration of the shortcut in the Advanced Properties dialog:



Advanced Properties

Choose the advanced properties you want for this shortcut.

☑ Run as administrator

This option allows you to run this shortcut as an administrator, while protecting your computer from unauthorized activity.

☑ Run in separate memory space

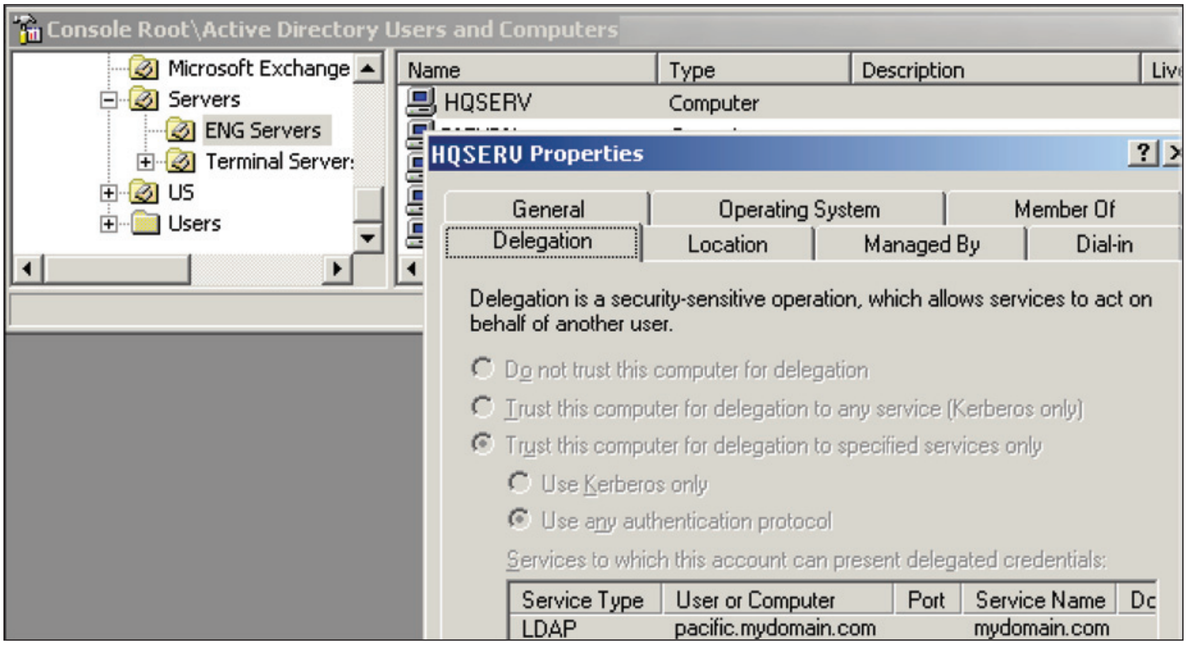
Step 2: Defining Server for ShoreWare

From the Microsoft Active Directory administration console, identify (or create if required), the server in Microsoft Active Directory that will act as the HQ Server for the ShoreTel system.

Define the necessary delegation rights to this computer.

On the HQ server computer, right click to select Properties, click the Delegation tab, make the appropriate radio button selections similar to the diagram below, then “Add…” to bring up the “Add Services” window. Next, click “Users or Computers” to bring up the “Select Users or Computers” window, and fill in the name of the Domain Controller in the box of “Enter the object name to select.”

Next, click the "Check Names" button to check the name, then click "OK": now the "Add Services" window is populated with all the services, so select "LDAP" service. In this example, the server "HQSERV" is the ShoreWare HQ Server, defined as a trusted entity for the LDAP service with respect to the Domain Controller "pacific."



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation
○ Trust this computer for delegation to any service (Kerberos only)
● Trust this computer for delegation to specified services only
○ Use Kerberos only
● Use any authentication protocol

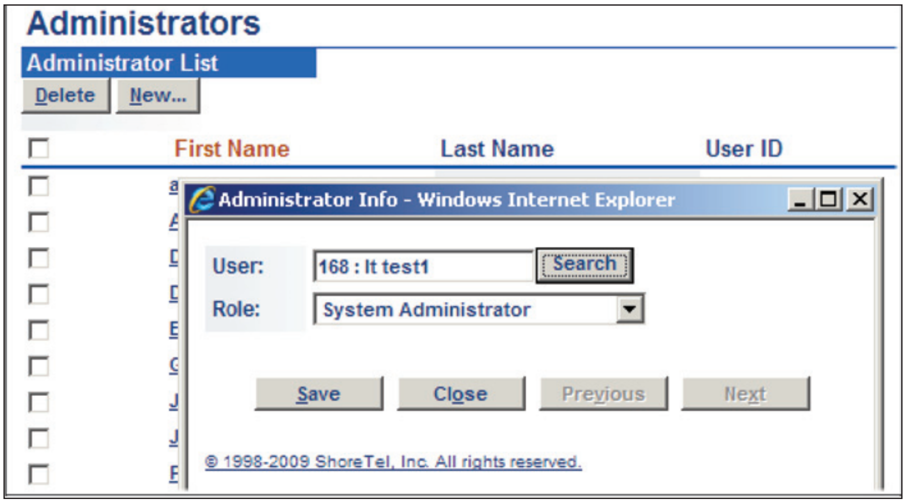
Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service Name	Dc
LDAP	pacific.mydomain.com		mydomain.com	

Step 3: Define system administrator in ShoreWare Director

In ShoreWare Director, create the user to be associated with the user identified in Step 1, and assign that user with system administrative privileges. Make sure this user's Client User ID matches the Microsoft Active Directory User Logon Name.

> *Note: as with previous ShoreWare releases, creating a user with system administrator privileges in ShoreWare Director will remove the default admin/changeme account.*

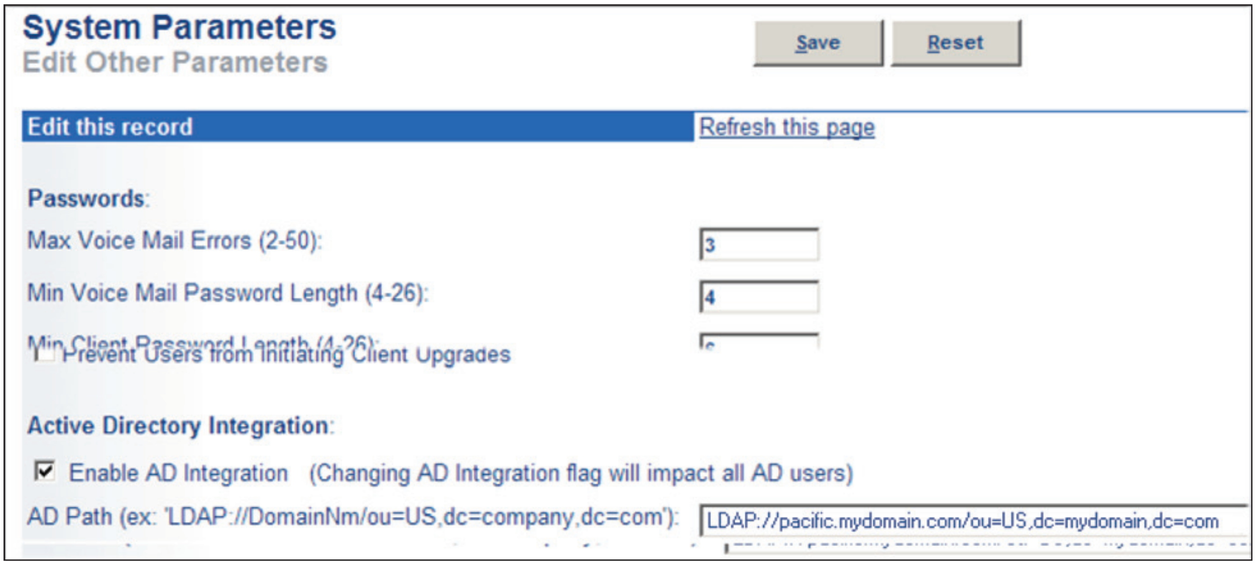


User: 168 : lt test1

Role: System Administrator

Step 4: Define LDAP path

In ShoreWare Director, [System Parameters/Other], define the path to the Microsoft Active Directory server. This path defines both the domain controller and the scope of data that ShoreWare Director can access for user lookup. The path must be chosen with the customer's Microsoft Active Directory hierarchy in mind.



System Parameters
Edit Other Parameters

Passwords:

Max Voice Mail Errors (2-50): 3

Min Voice Mail Password Length (4-26): 4

Min Client Password Length (4-26): 6

□ Prevent Users from Initiating Client Upgrades

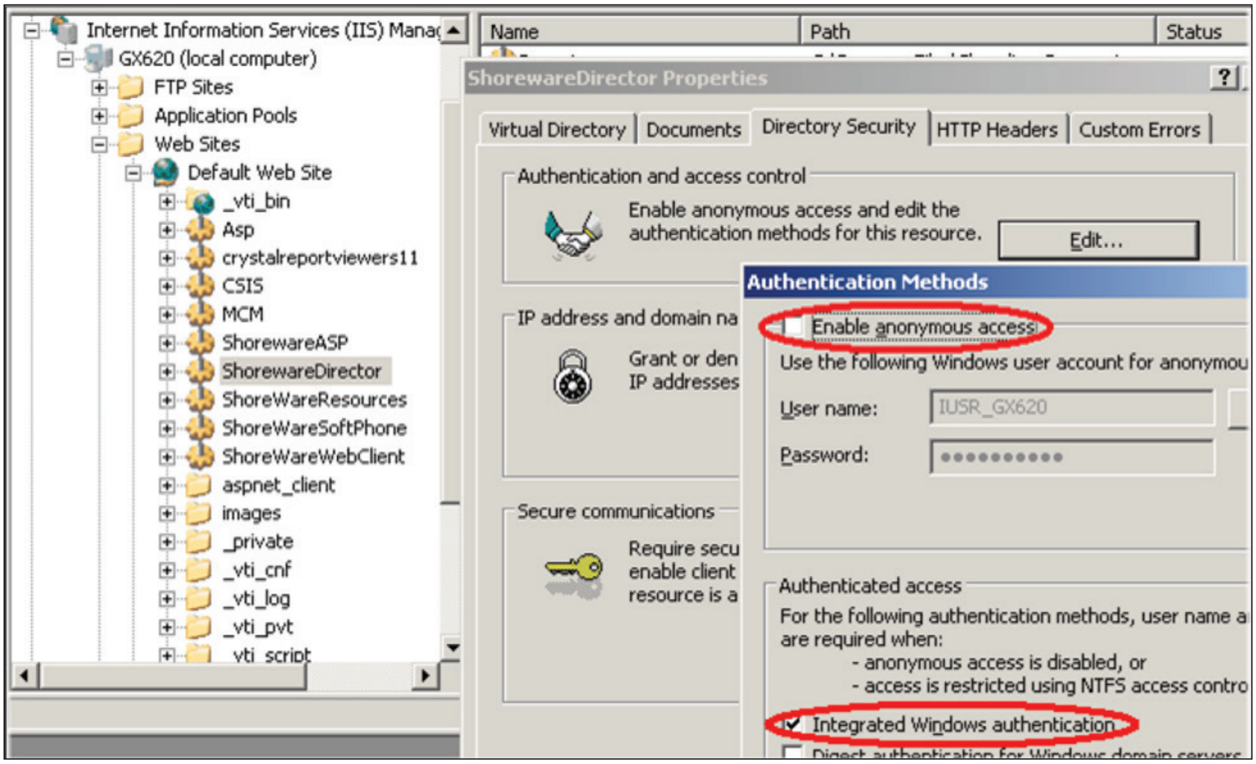
Active Directory Integration:

☑ Enable AD Integration (Changing AD Integration flag will impact all AD users)

AD Path (ex: 'LDAP://DomainNm/ou=US,dc=company,dc=com'): LDAP://pacific.mydomain.com/ou=US,dc=mydomain,dc=com

Please note, the domain controller specified in Step 2 to define, the delegation trust relationship (in this case "pacific"), should be specified in this step as well.

Upon "Save", a warning message is displayed that the LDAP path cannot be verified (which is normal) and the current ShoreWare Director admin login session will be terminated. At this point the ShoreTel system is enabled for Microsoft Active Directory integration, i.e., the ShoreWare Director no longer allows anonymous login. This is shown in Figure 1a.



Authentication and access control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain na

Grant or den IP addresses

Secure communications

Require secu enable client resource is a

□ Enable anonymous access

Use the following Windows user account for anonymou

User name: IUSR_GX620

Password: ••••••••••

Authenticated access

For the following authentication methods, user name a are required when:

- anonymous access is disabled, or
- access is restricted using NTFS access contro

☑ Integrated Windows authentication

□ Digest authentication for Windows domain servers

Figure 1a – IIS screen (Windows 2003 Server)

In Windows 2008, the IIS screen appears as shown in Figure 1b and 1c.

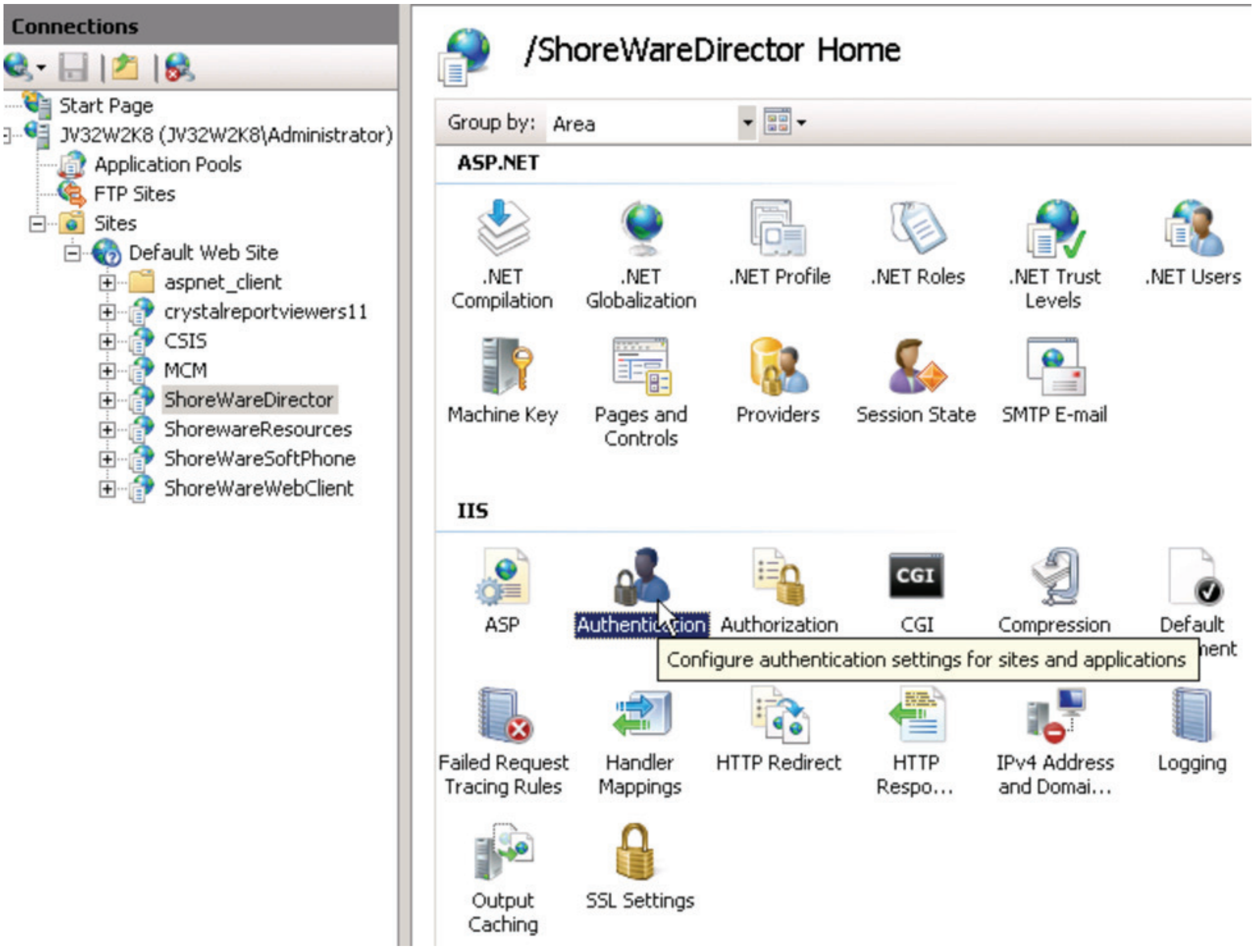
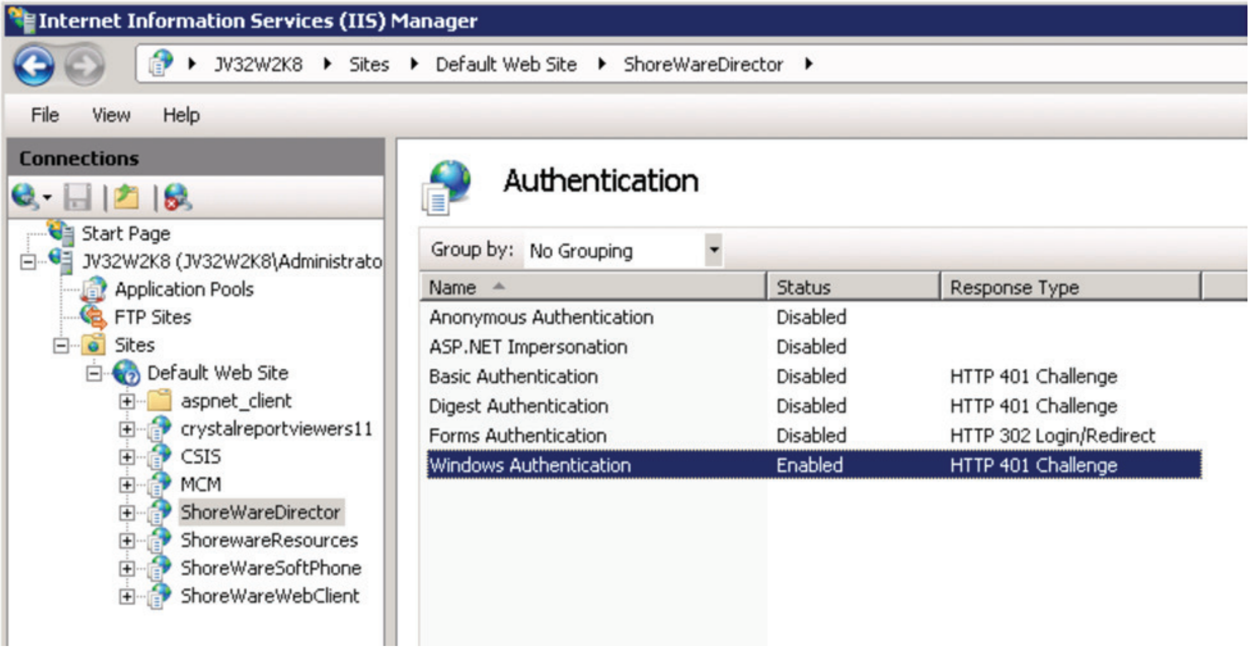


Figure 1b – IIS screen (Windows 2008 Server)



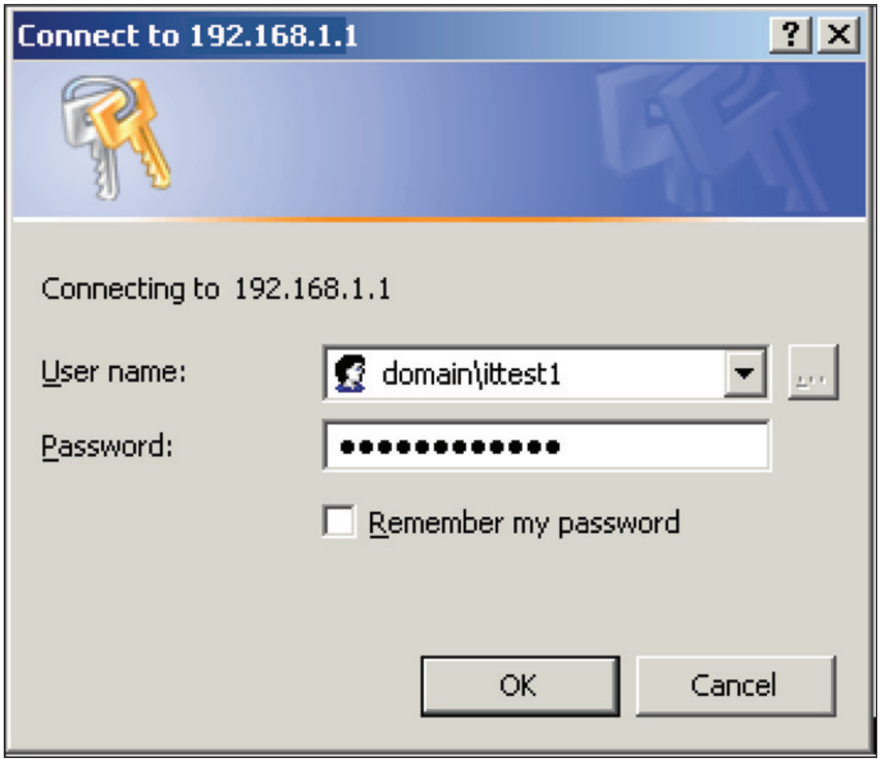
Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

Figure 1c – IIS screen (Windows 2008 Server)

Please note that at this point, the individual user "ittest1" in ShoreWare Director is not yet configured as a Microsoft Active Directory User, i.e., Single Sign On for "ittest1" is not yet available.

Step 5: Login to ShoreWare Director and configure administrative user as Microsoft Active Directory User

Launch a new IE browser window, access ShoreWare Director using the explicit IP address of the HQ server, e.g., http://192.168.1.1/ShorewareDirector/login.asp, and the following prompt should appear:



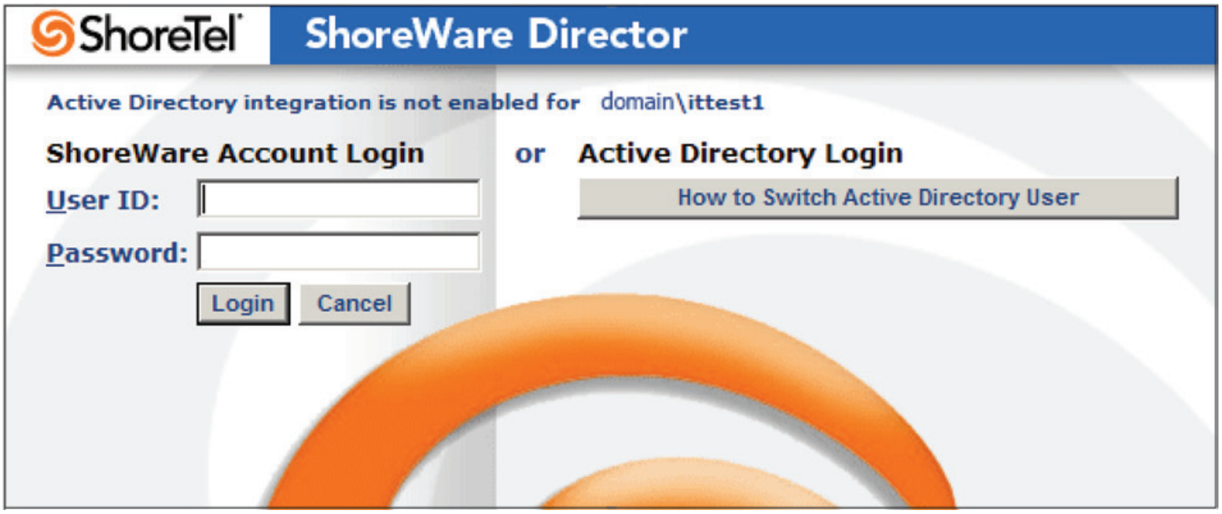
Connecting to 192.168.1.1

User name: domain\ittest1

Password: ●●●●●●●●●●●●●

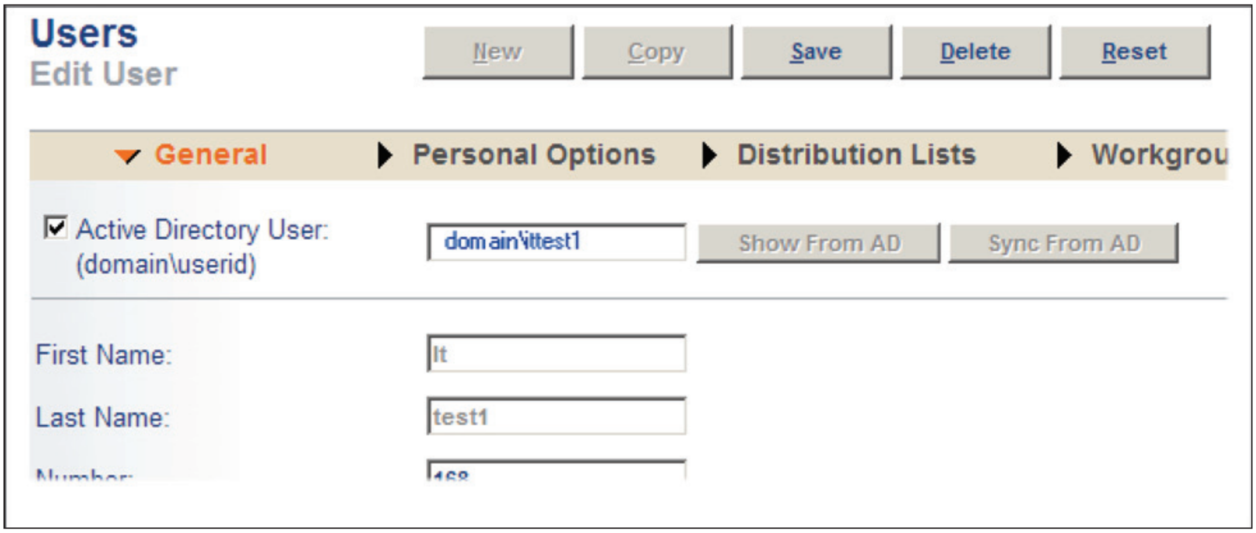
□ Remember my password

Authenticate with the user "ittest1". The ShoreWare Login page will then display.



Active Directory integration is not enabled for domain\ittest1

Login with “ittest1” and the password, and navigate to the User Edit page, and enable “ittest1” as a Microsoft Active Directory user.



☑ Active Directory User: (domain\userid) domain\ittest1

First Name: It

Last Name: test1

Number: 168

Login with “ittest1” and the password, and navigate to the User Edit page, and enable “ittest1” as a Microsoft Active Directory user.

Now “ittest1” is a Microsoft Active Directory user. Log off from ShoreWare Director.

From this point on, Single Sign On is available for “ittest1”.

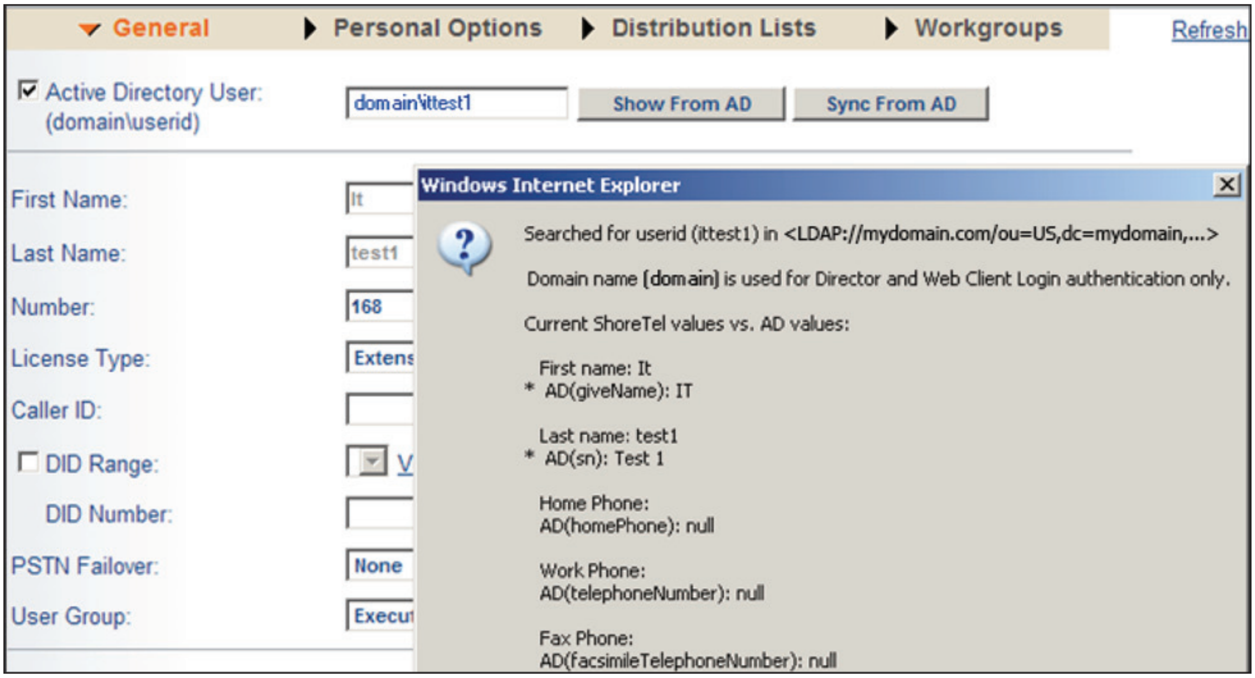
The user “ittest1” will automatically be logged in upon accessing ShoreWare Director using a URL such as: http://HQSERV/ShorewareDirector/login.asp

Please note that different URL formats may require authentication:

http://HQSERV/ShorewareDirector/login.asp
http://HQSERV.mydomain.com/ShorewareDirector/login.asp
http://192.168.1.1/ShorewareDirector/login.asp

In the above example, the first format is considered “Local Intranet”, while the second and third format are of the type “Internet”.

With the ShoreWare administrator now being a Microsoft Active Directory User, the option to fetch user properties from Microsoft Active Directory is now available. The "Show From AD" button fetches the attributes of user "domain\ittest1".



☑ Active Directory User: (domain\userid) domain\ittest1

First Name: It

Last Name: test1

Number: 168

License Type: Extens

Caller ID:

☐ DID Range:

DID Number:

PSTN Failover: None

User Group: Execu

Searched for userid (ittest1) in <LDAP://mydomain.com/ou=US,dc=mydomain,...>

Domain name (domain) is used for Director and Web Client Login authentication only.

Current ShoreTel values vs. AD values:

First name: It
* AD(giveName): IT

Last name: test1
* AD(sn): Test 1

Home Phone:
AD(homePhone): null

Work Phone:
AD(telephoneNumber): null

Fax Phone:
AD(facsimileTelephoneNumber): null

Issue	Author	Reason for Change	Date
1.0	Dieter Rencken	Initial Release	April 9, 2009
2.0	Dieter Rencken	Updated with Windows 2008 Server information	June 23, 2009

ShoreTel®

To receive regular updates and news on ShoreTel products, email shorecareadmin@shoretel.com

960 Stewart Drive Sunnyvale, CA 94085 USA   Phone +1.408.331.3300   +1.877.80SHORE   Fax +1.408.331.3333   www.shoretel.com