ENCENTUATE
Security Through Convenience

Encentuate Training Guide

for Encentuate IAM v3.X

Last Updated: Feb 2008

info@encentuate.com
www.encentuate.com

Copyright Notice

Table of Contents

Objective of this guide

This training guide is intended to be used with a Virtual Machine (VM) training environment for the installation and setup of the Encentuate solution. The objective of this guide is to:

- Provide our customers and partners with hands-on training and familiarization of the Encentuate solution
- Provide a quick start environment for evaluating and learning the Encentuate solution

This training material is most effective when accompanied with a hands-on training session conducted by certified Encentuate trainers.

What you will learn

At the end of this training guide, you will be able to:

- Install and setup an IMS server to work with Microsoft Active Directory (AD)
- Install and setup AccessAgent on Microsoft Terminal Services to provide Roaming Desktops
- Install and setup AccessAgent on Windows XP, configured to work in Private Desktop[*] mode
- Install AccessStudio and profile the following example applications for single sign-on:
    - A Windows 32 application
    - A teletype (TTY) application
    - A mainframe green screen application
    - A web application
- Sign up Bob and Alice to use the Encentuate solution

[*] Encentuate provides comprehensive session management capabilities and can be configured to provide Personal Desktop, Shared Desktop, Private Desktop, and Roaming Desktops. Shared Desktop allows multiple users to share a generic desktop login and is useful in kiosk environments, such as those on clinical floors, warehousese or manufacturing facilities. Roaming Desktop provides a remote desktop on a Terminal Server or Citrix and “follows” the user as he roams from workstation to workstation.

- Test and evaluate the product

What is not covered

This training guide covers a typical setup in a moderately complex kiosk environment. It does not cover all the capabilities of the Encentuate solution. For example, it does not cover the set up of:

- Strong authentication
- Web Workplace for remote access
- AccessAgent for Citrix
- Password self-service
- AccessStudio Advanced

Separate training is available for the above topics.

Pre-requisites

The use of this training guide requires a confidentiality agreement, a software evaluation agreement, or a reseller agreement to be in place.

This training guide is intended to be used with a VM training environment.

Please contact your Encentuate Account Executive or Partner Manager to get a copy of the agreements and the VM training environment.

Getting Help

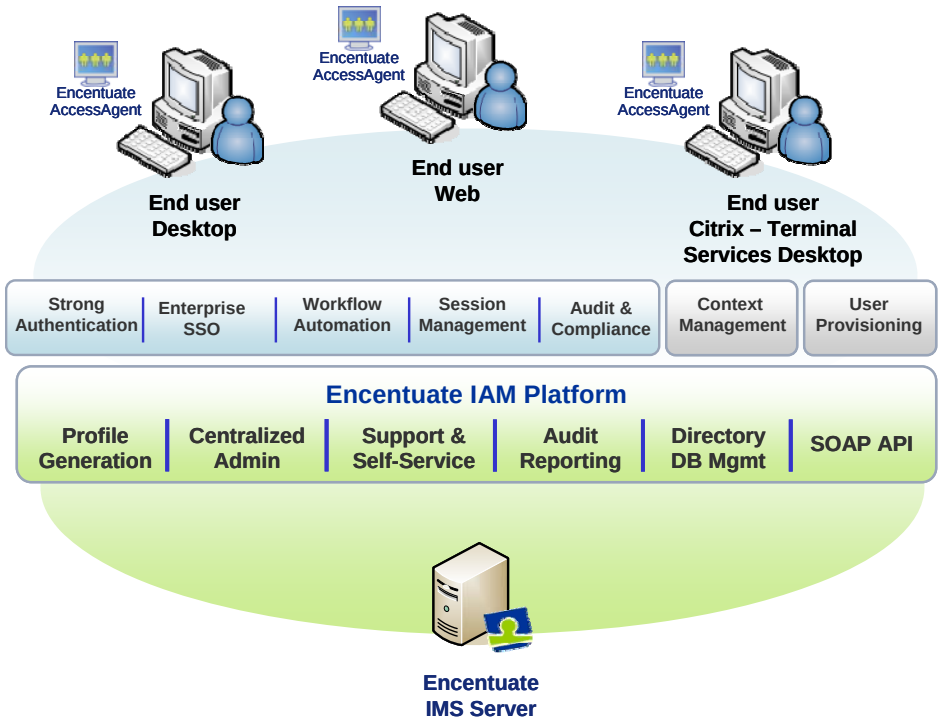
To get help anytime, please contact support@encentuate.com.

To submit feedback, requests new features or report defects, please login to http://customercare.encentuate.com or http://partnercare.encentuate.com. You may contact your Account Executive or Partner Manager to get an account.

Encentuate IAM

Encentuate IAM is the first solution that delivers a simple, flexible, and complete identity and access management solution at the enterprise end-points. Encentuate intelligently migrates the user-centric identity and access management (IAM) functions, such as enterprise single sign-on, authentication, and audit and compliance services, to the enterprise end-points, while integrating with provisioning and directory services at the enterprise back end.

The figure below summarizes the key functions:



For more information, refer to the whitepapers "*Identity and Access Management at the Enterprise End-points*" and "*Encentuate IAM – A Product Overview*"

Training scenarios

The training scenario outlined in this section is intended to be used on the supplied VM training environment.

This training scenario will cover the following:

- Install and setup an IMS server to work with Microsoft Active Directory
- Install and setup AccessAgent on Microsoft Terminal Services to provide Roaming Desktops
- Install and setup AccessAgent on Windows XP, configured to work in Private Desktop mode
- Install AccessStudio and profile the following types of applications:
    - A Windows 32 application
    - A teletype (TTY) application
    - A mainframe green screen application
    - A web application
- Register an administrator Bob and a user Alice
- Test and evaluate the product

About the Training VM

The VM training environment comprises of:

- A Server VM with the following software installed to simulate a typical enterprise environment:
    - Windows 2003 server, where IMS server will be set up
    - Microsoft Active Directory
    - Microsoft Terminal Server

- A Client VM running Windows XP where AccessAgent will be installed to simulate a typical enterprise kiosk (shared workstation in private desktop mode)

The VM training environment needs to be installed and set up on a workstation with the following requirements:

- 2GB RAM minimum
- 10 GB of hard disk space

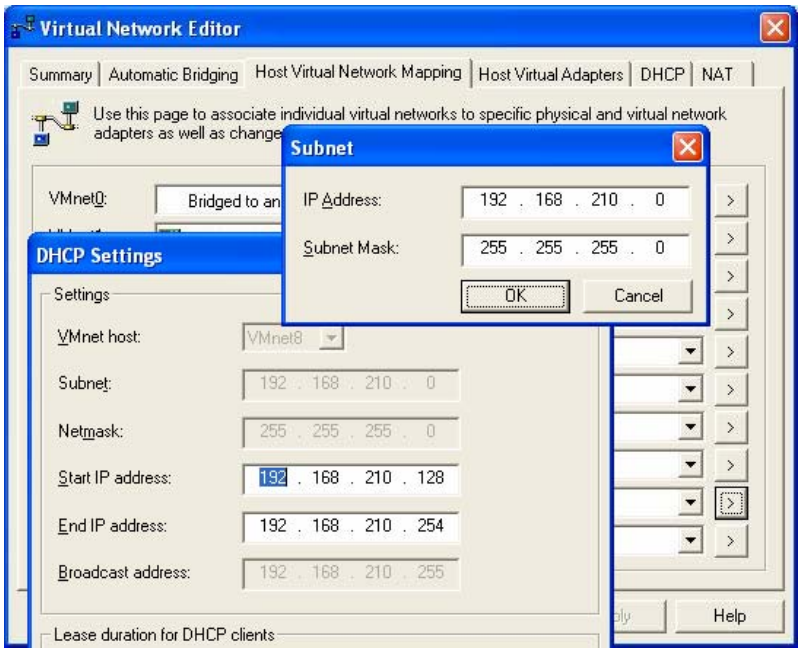
To install the VM training environment:

- Install VMWare Workstation v6.0 or later on the target workstation
    - A VMWare installer is included as part of the Training VM package. To activate a free trial license, register at http://www.vmware.com/vmwarestore/newstore/wkst601_eval_login.jsp
- The Training VMs are packaged as two .RAR archives. Copy the two files below to the target workstation:
    - ENC IMS Domain Server.rar
    - ENC AA XPSP2.rar
- Expand the two .rar files

- Run Start >Programs >VMWare >Manage Virtual Networks

  - Configure a NAT network for subnet 192.168.210.0

    (**Note**: This training VM requires this subnet to work. If you need help configuring the network for this VM, please refer to http://pubs.vmware.com/ws6_ace2/wwhelp/wwhimpl/js/html/wwhelp.htm for assistance.)



  - To test that you have properly configured the network, please do the following:
    - Start up the Server VM (ENC IMS Domain Server)
    - Start up the Client VM (ENC AA XPSP2). Note that Windows automatically logs in with the user name: "private" and the password "himmss"[†].
    - Click on the "Medscape Local" icon on Client VM's desktop to see if it can connect to the Win2003 Server
    - If a Medscape Local web page displays successfully, then the network has been configured properly

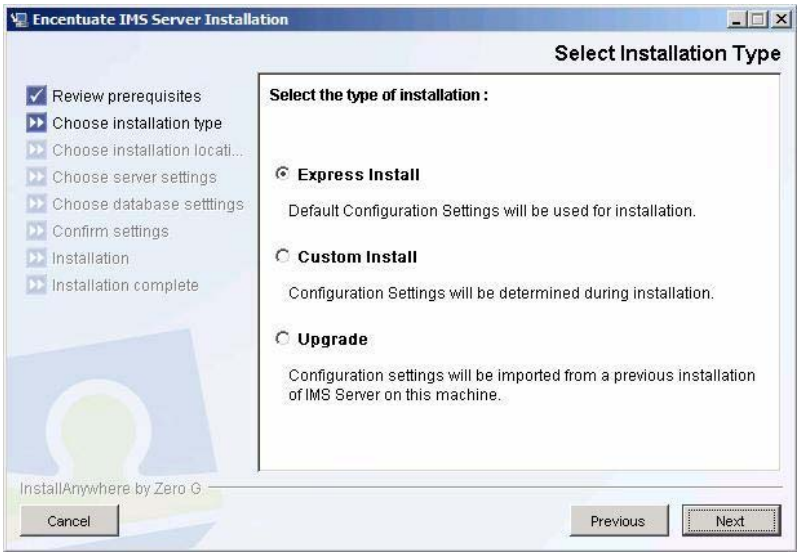
This Training Guide does not cover how to setup and use a Virtual Machine. For more information, see http://pubs.vmware.com/ws6_ace2/wwhelp/wwhimpl/js/html/wwhelp.htm.

[†] To simulate a windows kiosk, the Windows registry flags AutoAdminLogon and ForceAutoLogon are pre-set to auto logon to the shared desktop account "private".

Installing Encentuate IMS

In the Server VM (ENC IMS Domain Server), you will find the IMS Installer. To install and configure the IMS:

- Login to Windows with user name: administrator, and password: encentuate
- Run the IMS installer provided on the desktop
- Once the installer starts, click ”Next”
- Choose “Express Install”[‡] and click ”Next”

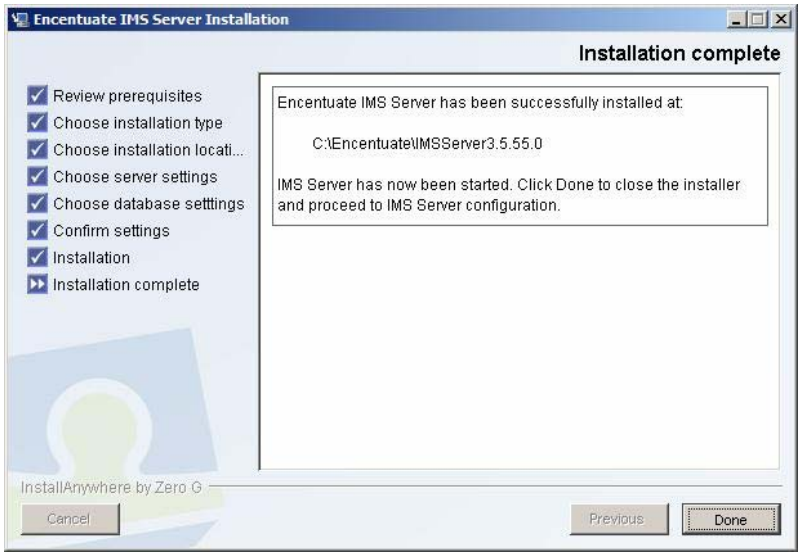


- Since a database will be installed as part of Express Install, you will be asked to select a password for the database administrator
    - Enter the database administrator’s password (eg, sso123!) for the newly created MSSQL server; click ”Next”

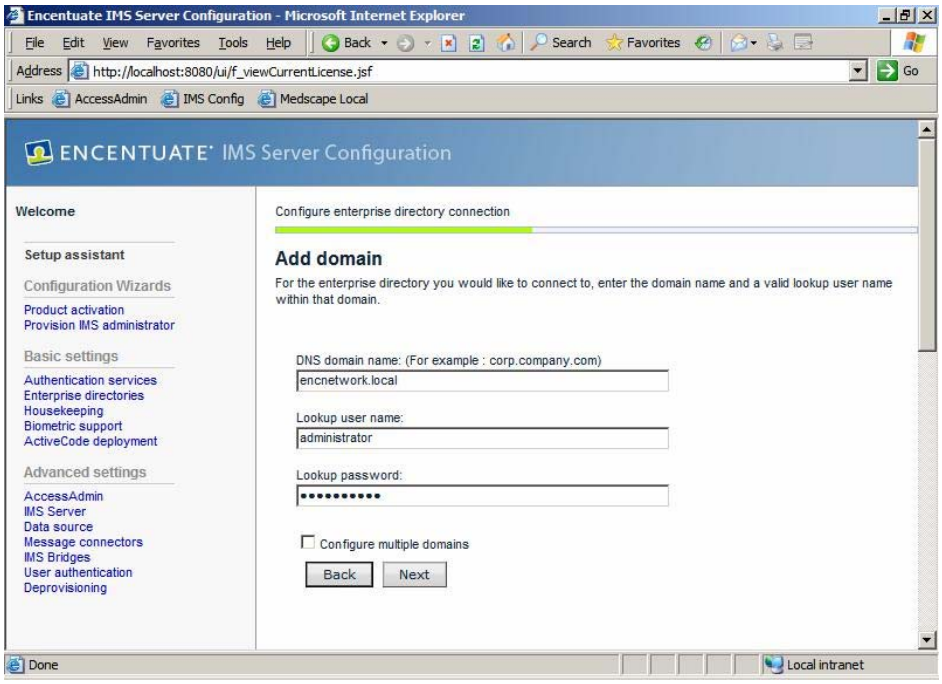
[‡]Express install will automatically install a database with IMS.

- On the pre-installation summary screen, click on “Install”

- When you see the screen below, the installation is complete. You are now ready to start configuring the IMS

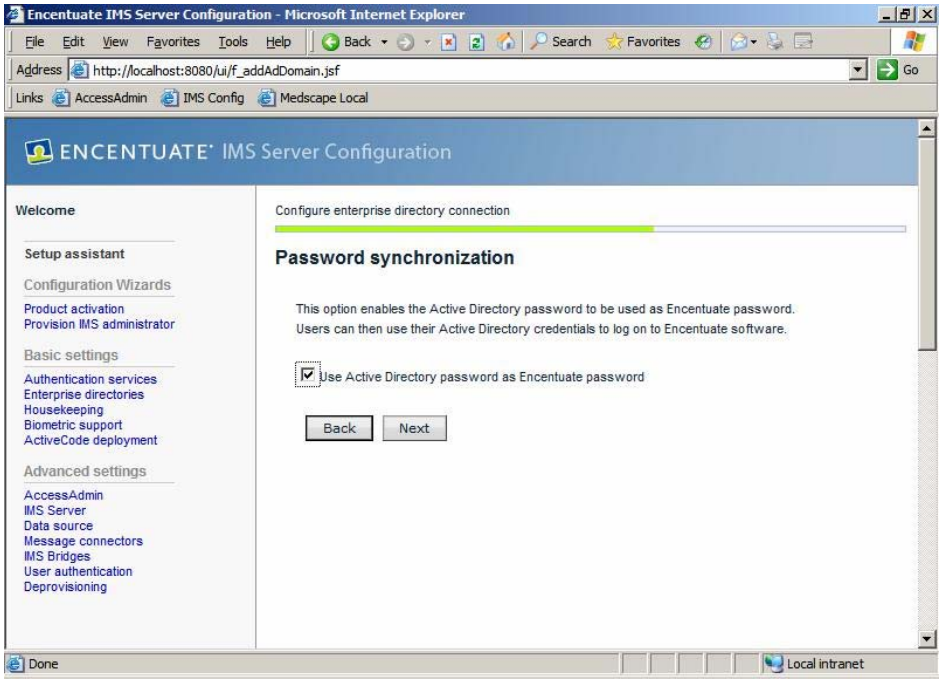


- The IMS Configuration Utility will start now, enter the following AD information:
    - DNS Domain Name: encnetwork.local
    - Lookup User name: administrator
    - Lookup Password: encentuate
    - Click ”Next”



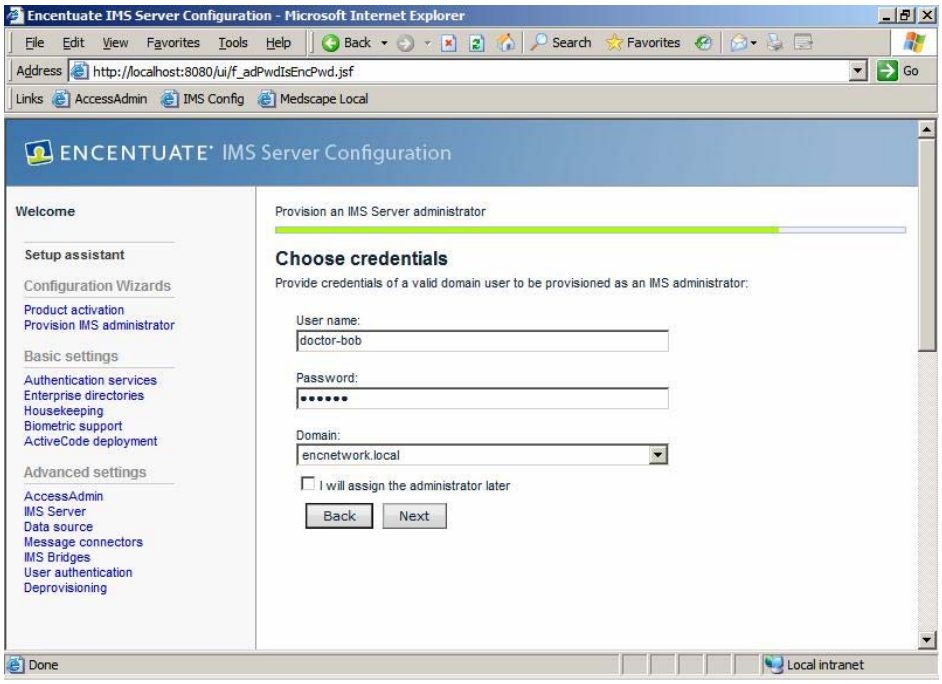
This configures Encentuate IMS with the rights to query AD for user information. Note that Encentuate does not extend the AD schema.

- Check “Use Active Directory password as Encentuate password”[§]. Click ”Next”



[§] Encentuate may be configured to allow users to use a unique password or to use their AD password as the Encentuate password.

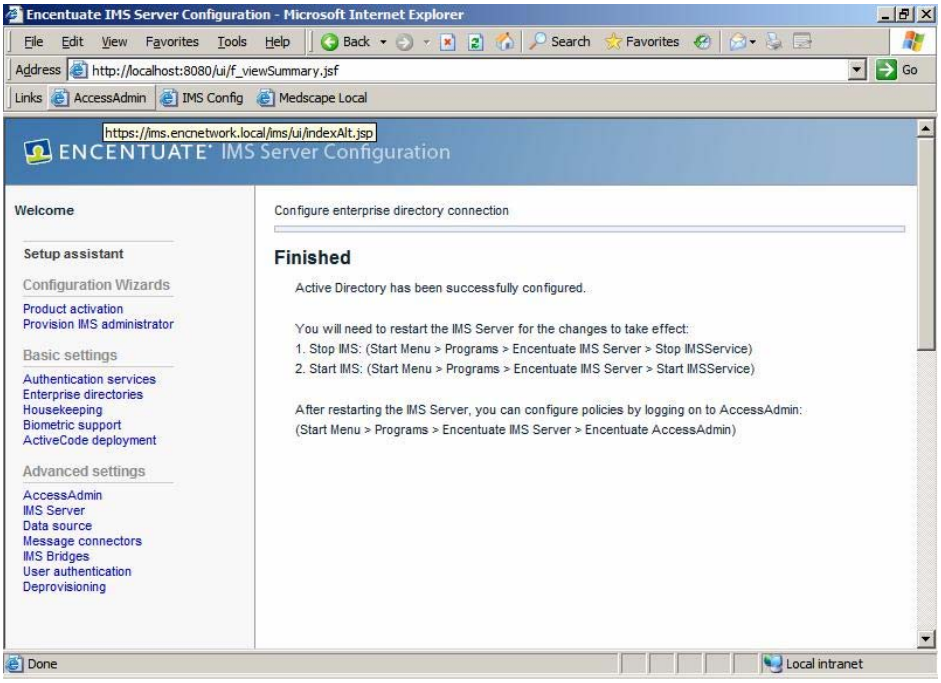
- You will be asked to specify the login credentials for the initial IMS Administrator. Enter the following AD information:
    - User name: doctor-bob
    - Password: himmss
    - Domain: encnetwork.local
    - Click ”Next”**



The user “doctor-bob” is now pre-registered with IMS. Registration will be complete when “doctor-bob” first logs on to his Encentuate account from a client. This will be covered in the next section.

** This initial administrator will have administrative rights to promote other users to the “administrator role” or”Help desk Manager” role later.

- You have successfully configured IMS. You will be asked to restart the IMS service:
    - Click Start > All Programs > Encentuate IMS Server > Stop IMSService to stop the IMS service
    - Click Start > All Programs > Encentuate IMS Server > Start IMSService to restart the IMS service

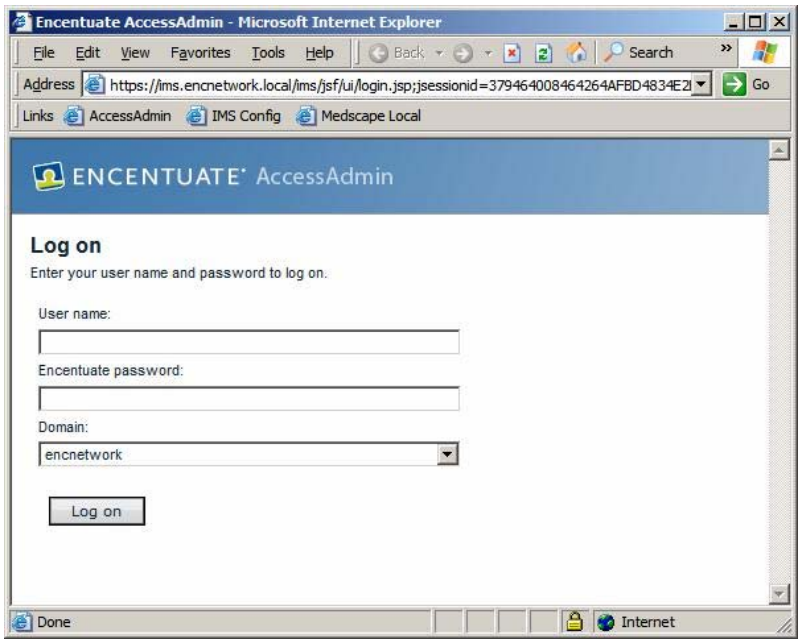


Configuring machine and user policies (AccessAdmin Setup Assistant)

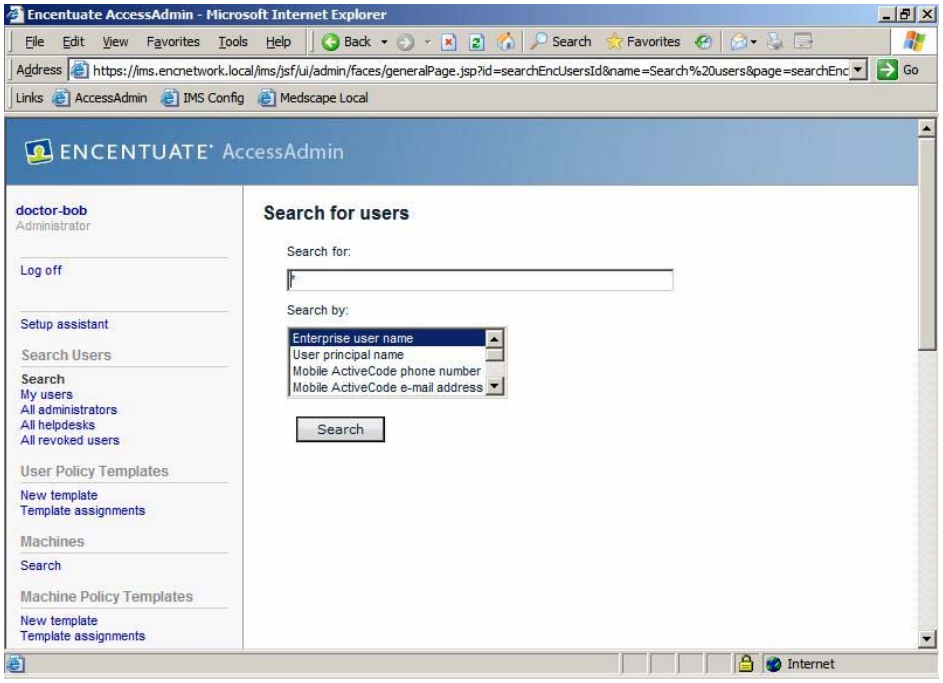
The IMS Server has been successfully installed. In this section, you will configure the policy templates for users and machines on the network. This is done on the IMS through the Encentuate AccessAdmin portal. There is a new Setup Assistant to help you to do it.

- Click on Start > All Programs > Encentuate IMS Server > Encentuate AccessAdmin.

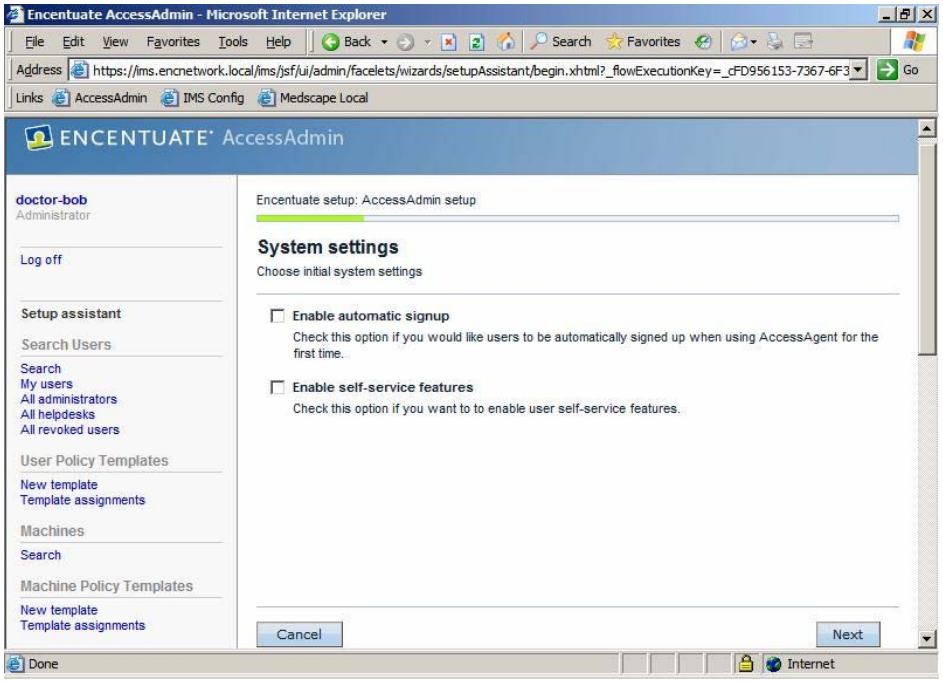
- Click Yes on the warning pop-up, then logon as username: doctor-bob and password: himmss



- Click on the “Setup assistant” link. On the next page, click on “Begin”.

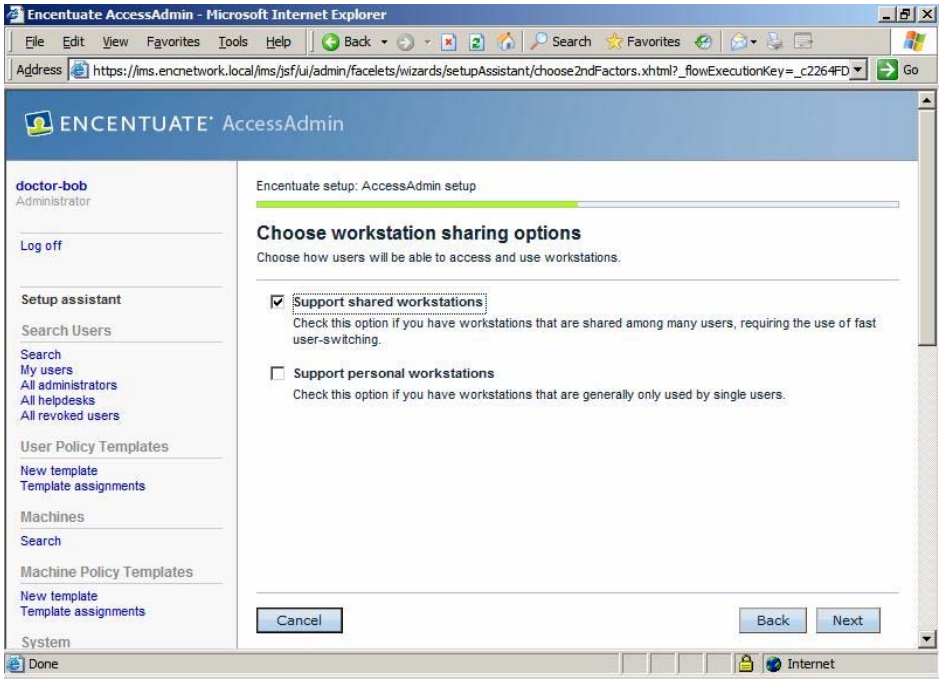


- Check the “Enable automatic signup” box and click “Next”.

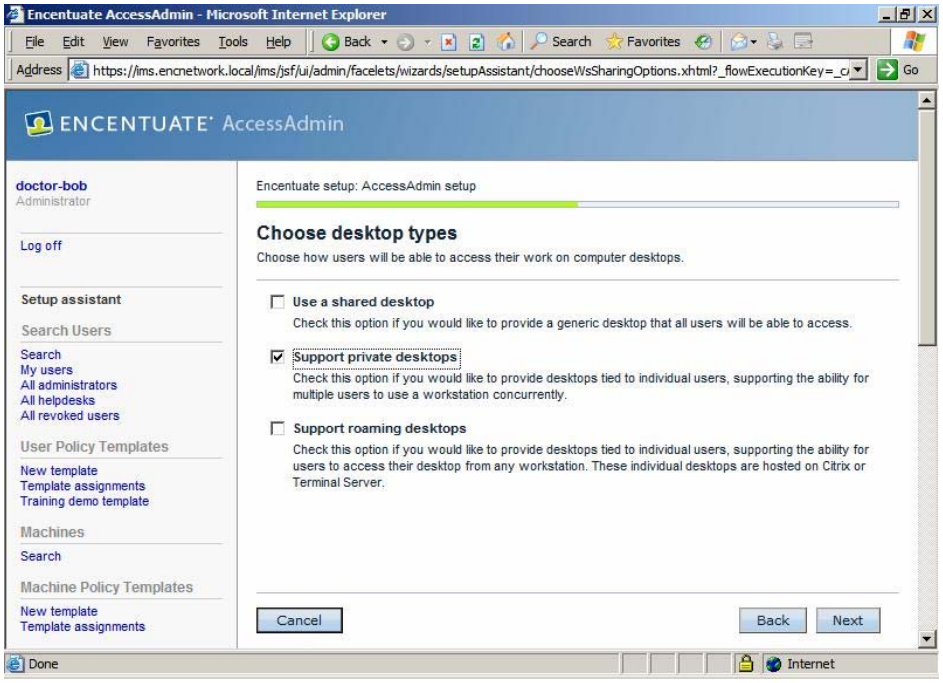


- On the “Choose second factors” page, just click “Next”.

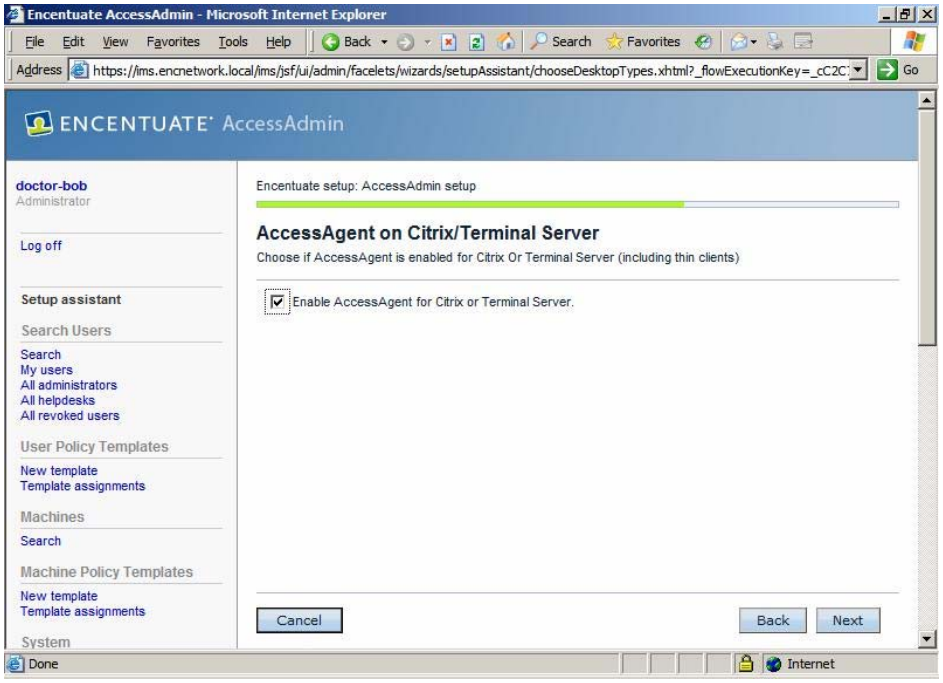
- Check the “Support shared workstations” box. Click “Next”.



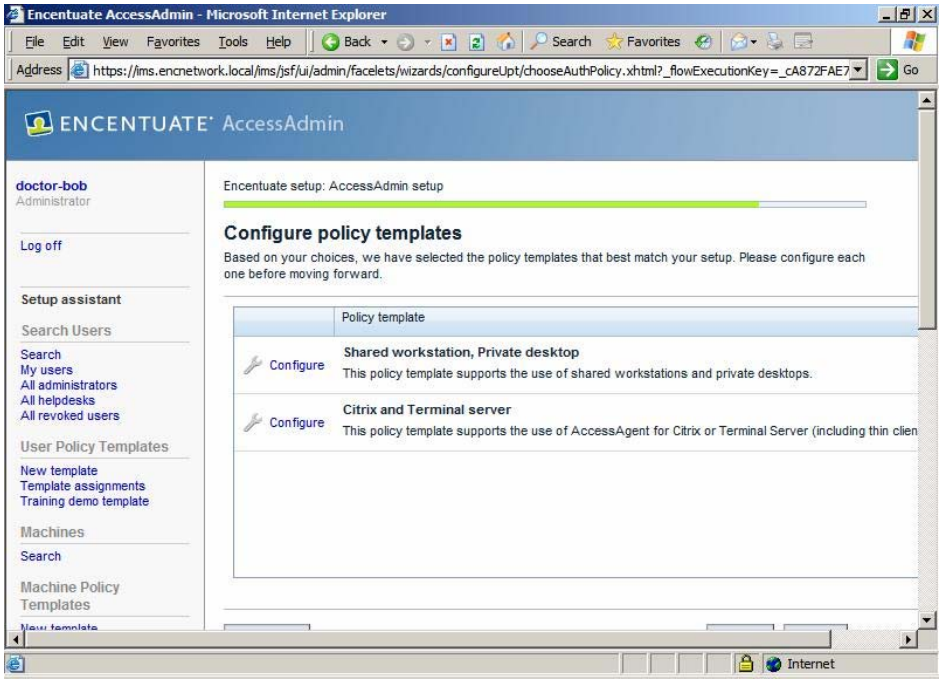
- Check “Support private desktops”. Click “Next”.



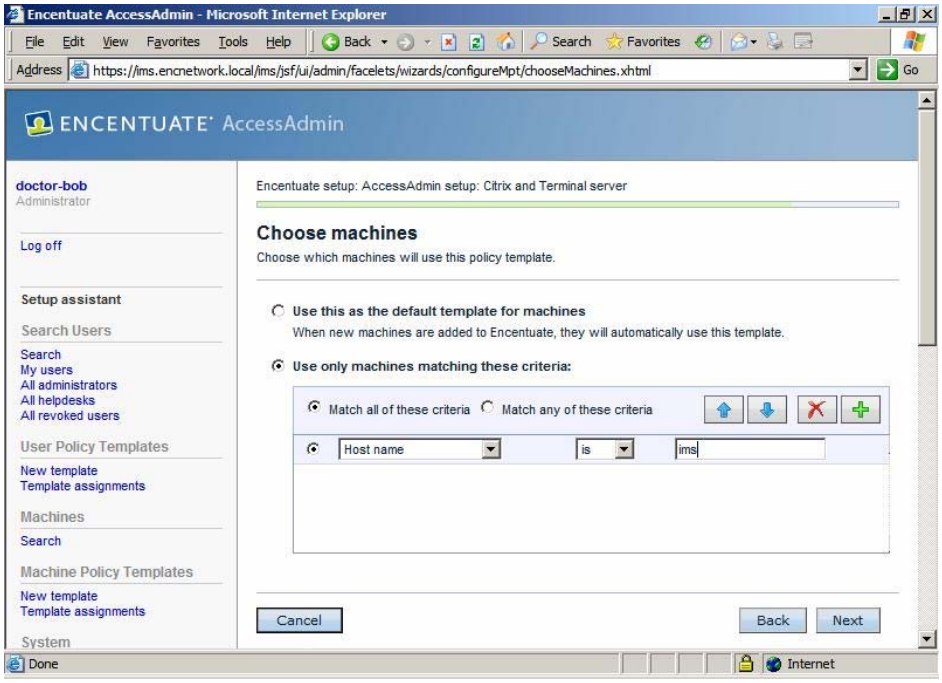
- Check “Enable AccessAgent for Citrix or Terminal Server”. Click “Next”.



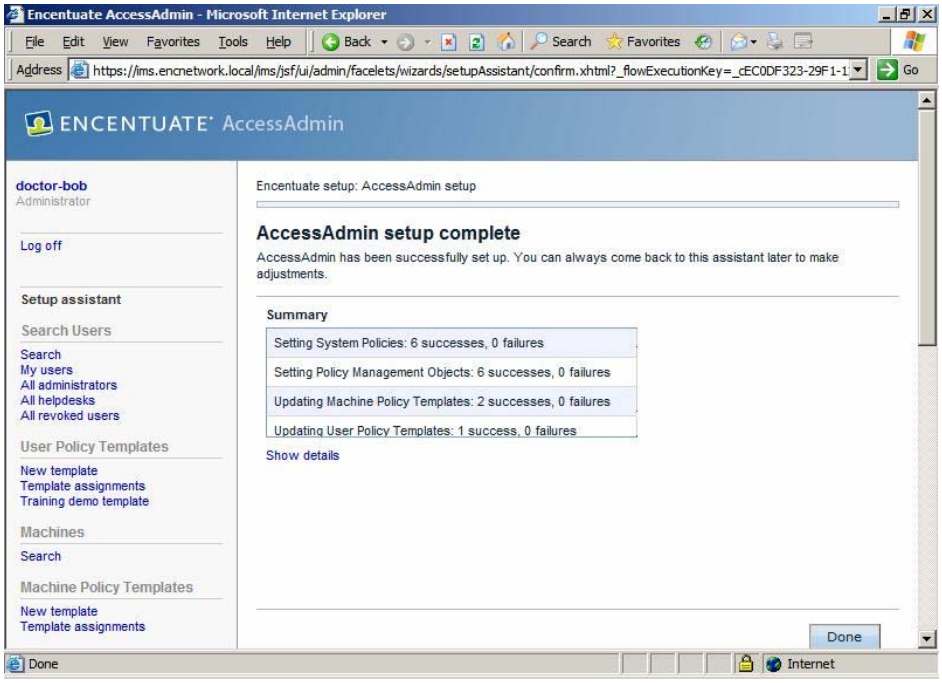
- Enter “Training Demo Template”. Click “Next”.
- On the “Choosing authentication policies” page, just click “Next”.
- Click on the top “Configure” link to work on the shared desktop policies.



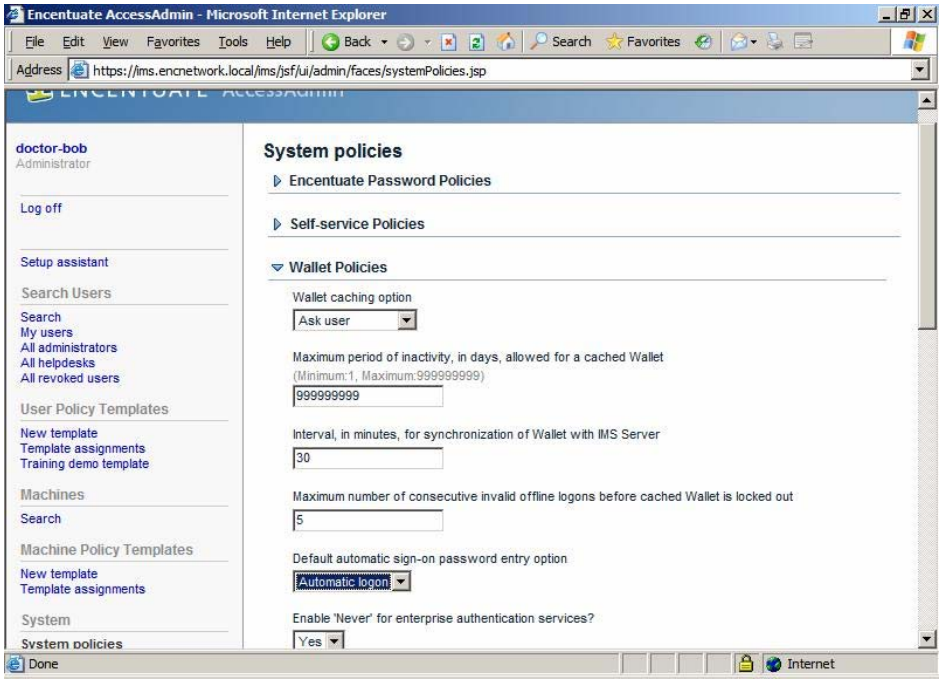
- Click on “Next” to keep the chosen name.
- Click on “Next” to choose Lock computer as desktop inactivity behavior.
- Check “Use this as the default template”. Click “Next”.
- Back at the “Configure policy templates” page, click on the lower “Configure” link.
- Click on “Next” to keep the chosen name.
- Check “Automatically log on to AccessAgent”. Click “Next”.
- Check “Use only machines matching these criteria”. Set “Host name is ims” as shown. Click “Next”.



- Back at the “Configure policy templates” page again, now click on “Next”.
- On the “Confirm settings” page, click “Next”.
- On the “AccessAdmin setup complete” page, click “Done”.



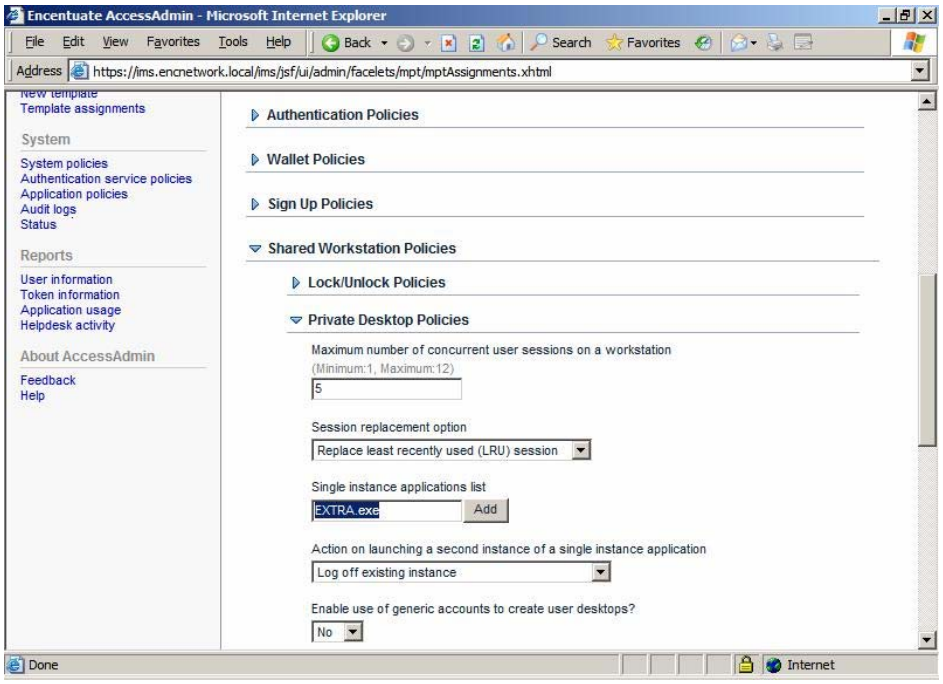
- Click on the “System policies” link. Expand “Wallet Policies” on the right pane.



- Set “Default automatic sign-on password entry option” to “Automatic”.

- Click on the “Update” button below.

- Click on Machine Policy Templates > Template Assignments. Click on "Shared workstation, Private desktop".
- Expand "Shared Workstation Policies" then "Private Desktop Policies" within.
- Under Single instance applications list, type "EXTRA.exe" and click "Add".



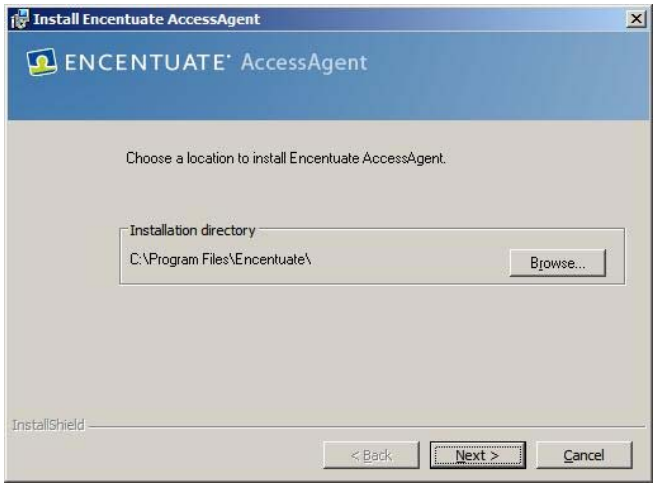
- Click on the "Update" button below.

Installing Encentuate AccessAgent on Terminal Services

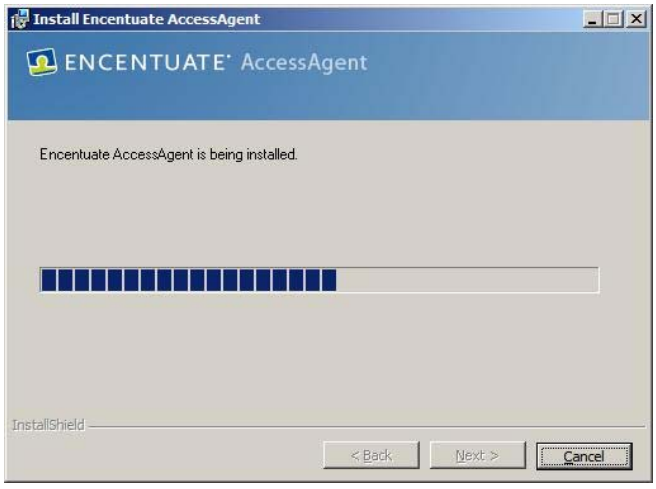
The IMS Server has been successfully configured. In this section, you will set up AccessAgent on the Microsoft Terminal Server.

In the Server VM (ENC IMS Domain Server), you will find the AccessAgent Installer. To install and configure AccessAgent for Terminal Server:

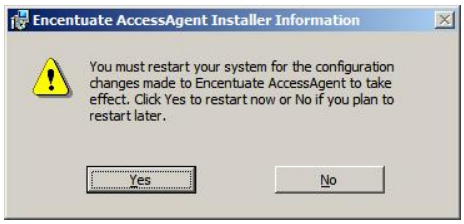
- Login to Windows with the user name: administrator and the password: encentuate
- Run the AccessAgent installer provided on the desktop
- Click "Next" to accept the default install folder



- The installation starts



- Click “Yes” to restart



- AccessAgent is now successfully installed on the Terminal Server

Installing Encentuate AccessAgent on an XP Kiosk

The IMS Server and AccessAgent on Terminal Server have been successfully installed. In this section, you will set up AccessAgent on a kiosk PC running Windows XP.

In the Client VM (ENC AA XPSP2), you will find the AccessAgent Installer. To install and configure the AccessAgent as a Private Desktop[††]:

- Start the Client VM (ENC AA XPSP2) if it is not already started. Note that Windows is automatically logged on with the user name: private and the password: himmss[‡‡].

  NOTE: the VMWare Tools Utility running in the guest OS conflicts with Encentuate's private desktop operation and therefore has been disabled for this VM. As a result, you must use the key sequence <Ctrl>-<Alt> each time you need to move the mouse cursor out of the AAXP1 VM's window.

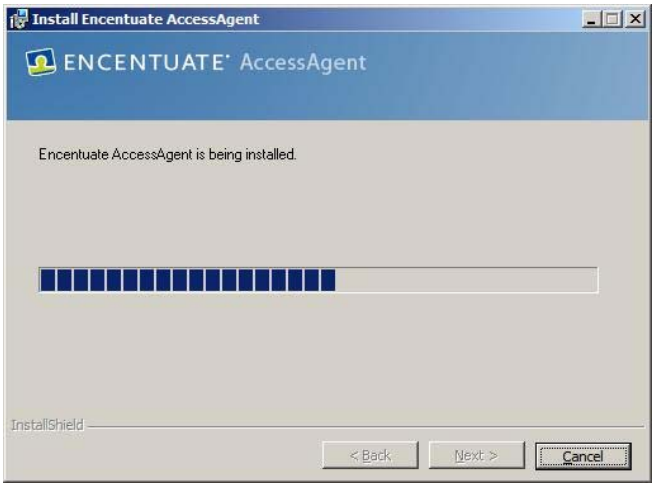
- Run the AccessAgent installer provided on the desktop

- Click "Next" to accept the default install folder

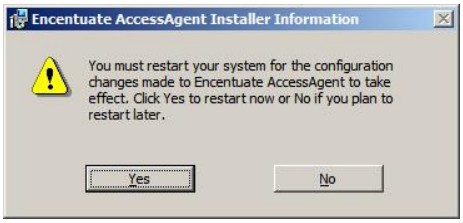
- The installation starts

[††] Encentuate also provides other means of session management, including Shared Desktop and Roaming Desktop. Private Desktop is unique to Encentuate and provides separate private desktops for each user of a shared workstation.

[‡‡] The Windows registry AutoAdminLogon and ForceAutoLogon are set to auto logon to the private desktop default local Windows account "private".



- Click “Yes” to restart



- After the VM restarts, Windows automatically logs on as the user “private” as before. Encentuate now locks the desktop.
- Click “Go to Windows to Unlock”. Type himmss as password, then reboot the VM again.
- AccessAgent is now successfully installed on the Client VM.

Registering an Administrator

Now that the server and client software have been set up, the system is ready to be used by end users and administrators. For simplicity, the users will be registered to use the system without strong authentication[§§].

To complete the registration of the IMS Administrator:

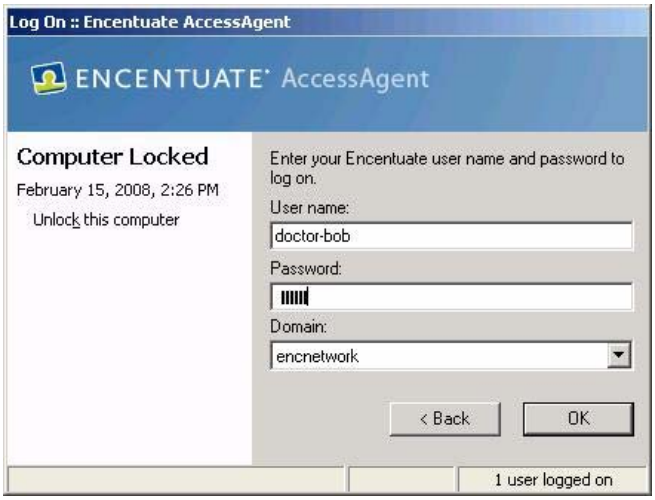
- On the Client VM (ENC AA XPSP2), click CTRL-ALT-DEL to lock screen if it is not already locked

  Note: To send CTRL-ALT-DEL inside a VM, either:

[§§] Encentuate supports a wide range of strong authentication options including building access badges, iTag, active RFID badges, fingerprint biometrics, USB smart tokens, mobile authentication and one-time password tokens.

- ***Click on the VMware tool bar VM >Send Ctrl+Alt+Del, or***
- ***Enter <Ctrl>-<Alt>-<Ins> from your keyboard***

- Click "…My logon user name is not in the list" then enter the username: doctor-bob and the password: himmss



Note that Bob has been pre-provisioned as an IMS Administrator, Encentuate will now complete the registration process.

- You will be prompted to answer a personal question, which is required for password resets[***]. Choose a recovery question and enter your secret. Click "OK"

[***] Encentuate may be configured to require M of N personal questions for password self-service. For simplicity, this setup only requires 1 personal question.

- Click “Yes” to cache[†††] the Encentuate wallet locally on this machine

- Since the administrator wallet was pre-provisioned, for security reasons, you will be asked to update your Encentuate password the first time you login. For simplicity, re-enter the same password: himmss. The rest of the document assumes you use the password: himmss for Bob’s account. Click “OK”

- This completes the registration for the IMS Administrator. Bob is now an IMS Administrator

Registering End Users

In this section, Alice will be registered as an end-user:

[†††] Caching the Encentuate Wallet enables offline use.

- On the Client VM (ENC AA XPSP2), click CTRL-ALT-DEL to lock screen if it is not already locked
- At the Encentuate lock screen, click on "…My logon user name is not in the list"
- Enter user name: nurse-alice, password: himmss

- Choose a recovery question and enter your secret. Click "OK"

- Choose to cache wallet. Click "OK"

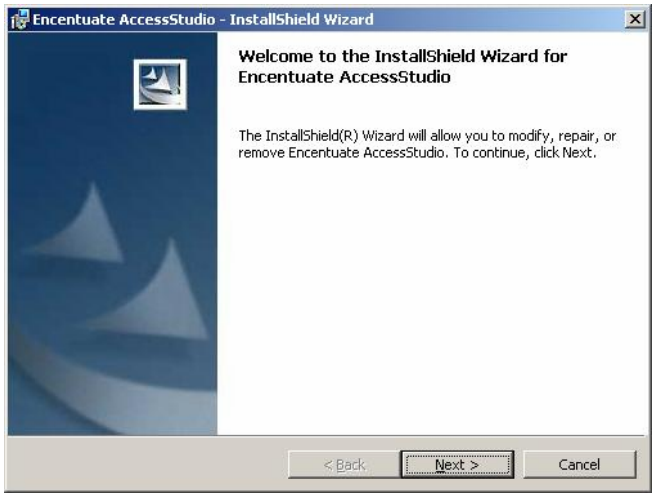
- This completes the registration of user Alice

Installing AccessStudio for SSO Profile Generation

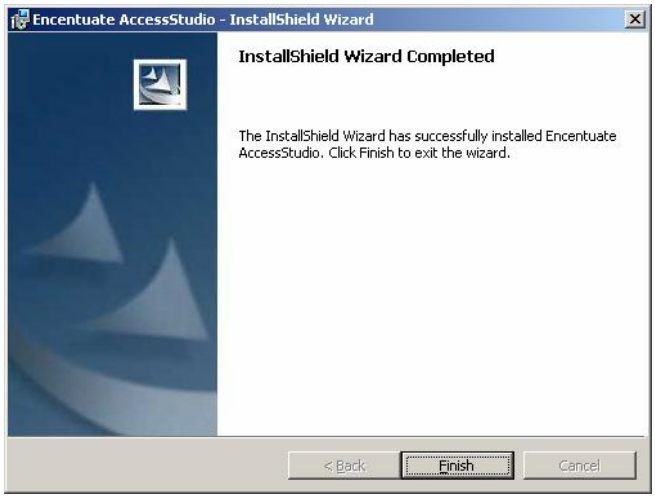
To enable single sign-on (SSO) for applications, an AccessProfile for the application needs to be generated and uploaded to the IMS server. Most profiles can be auto-generated using the AccessStudio Wizard. You will now install AccessStudio on the Client VM:

- On the Client VM (ENC AA XPSP2), click CTRL-ALT-DEL to lock screen if it is not already locked
- Logon as username: AAXP1\private and password: himmss

- Run the AccessStudio installer provided on the desktop
- Click “Next” and follow the instructions



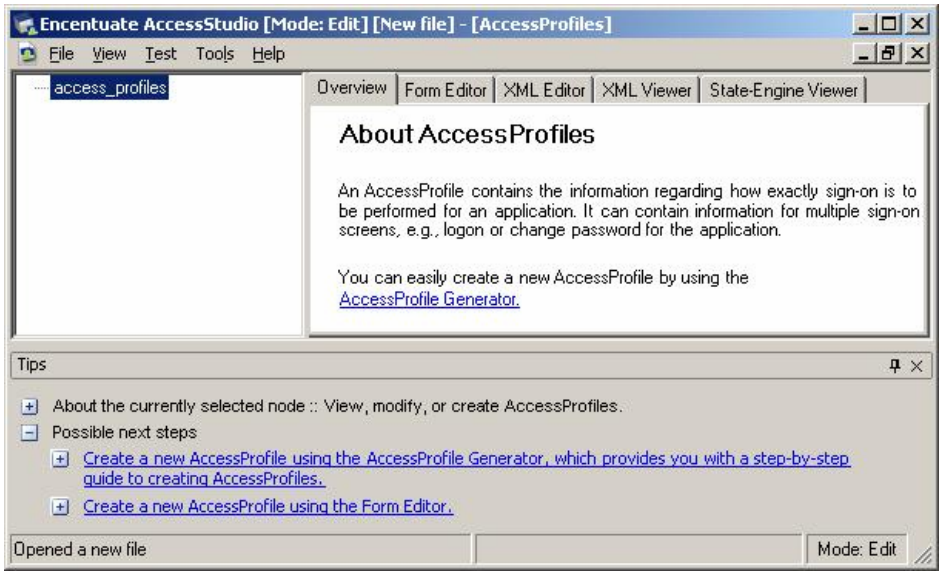
- Click “Finish” when prompted. AccessStudio is now successfully installed on the Client VM



Profiling a Windows Application for SSO support

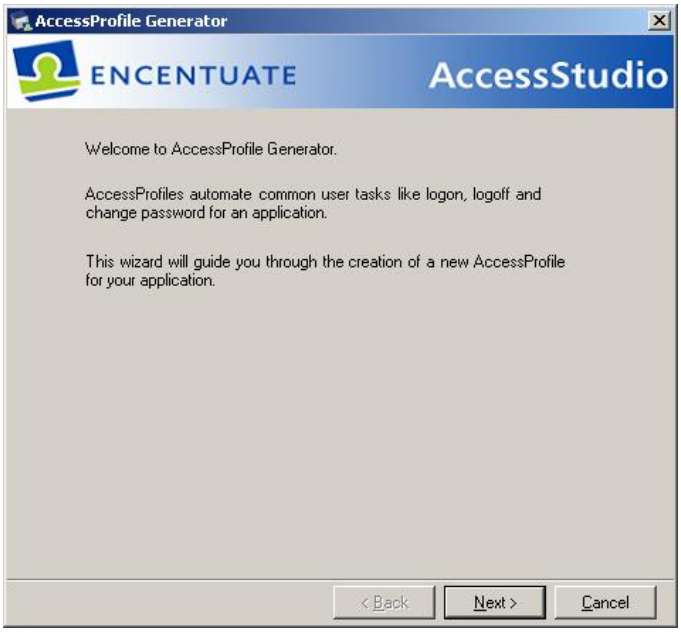
Now that AccessStudio has been set up on the Client VM, we can auto-generate the AccessProfiles for applications we intend to single sign on to. In this training sequence, the AccessProfile for Patient Information Manager (PIM) will be auto-generated:

- On the Client VM (ENC AA XPSP2), click CTRL-ALT-DEL to lock screen if it is not already locked
- Logon with the username: doctor-bob and the password: himmss
- Run Start >All Programs >Encentuate AccessStudio >AccessStudio

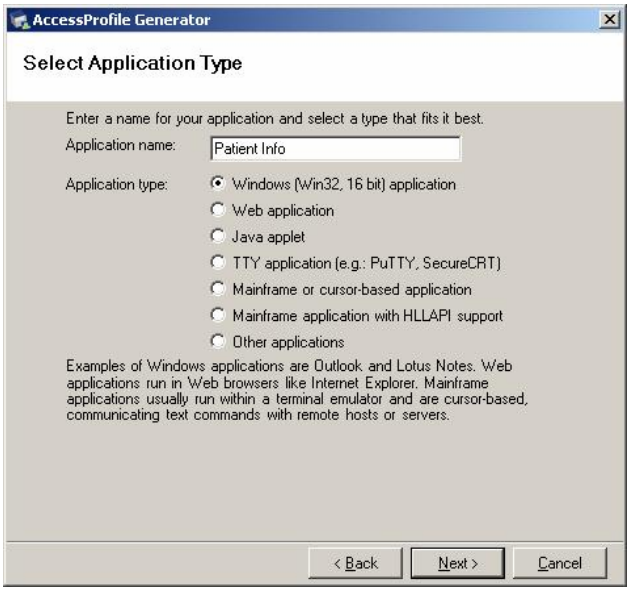


- Click on Tools >Start AccessProfile Generator

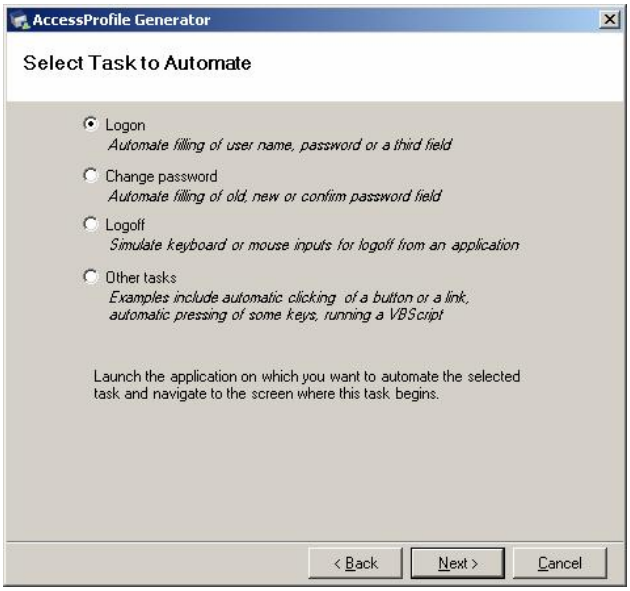
- On the “Welcome” screen, click “Next”



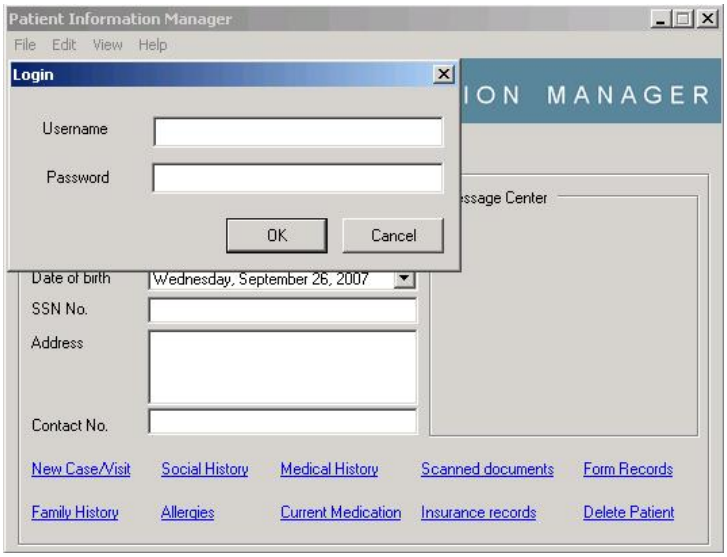
- Enter “Patient Info” in the application name field and choose “Windows” for “Application Type”; click “Next”



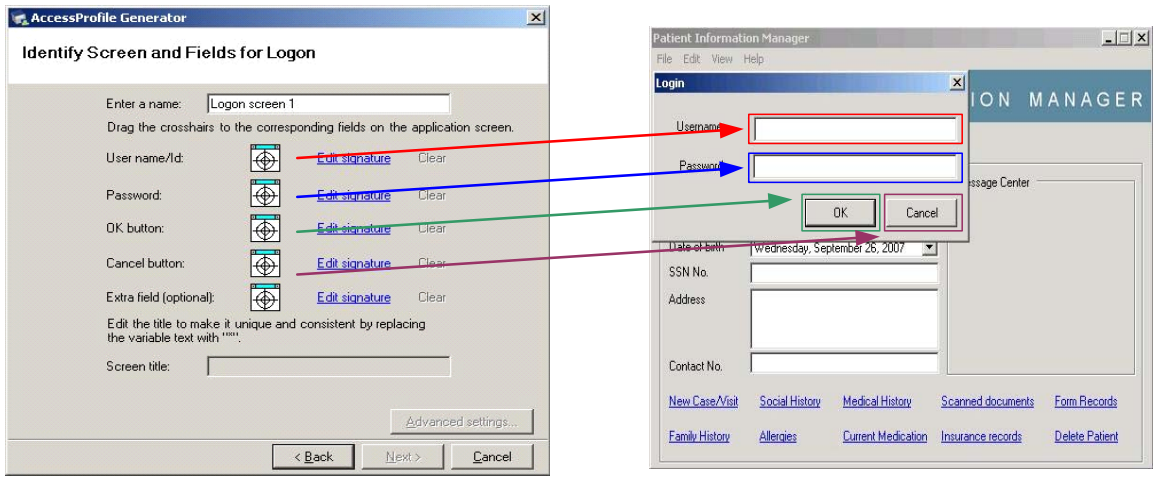
- Select the “Logon” task; click “Next”



- Double-click the desktop icon of PIM to start the program

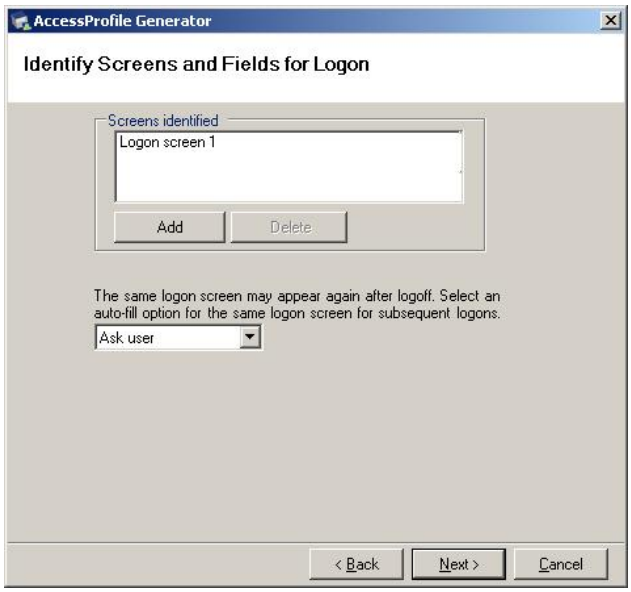


- Click and drag the crosshairs for the following onto the PIM logon screen:
    - The “User name” crosshair should be dropped at the user name field of PIM
    - The “Password” cross hair should be dropped at the password field of PIM
    - The “OK button” cross hair should be dropped at the OK button of PIM
    - The “Cancel button” cross hair should be dropped at the Cancel button of PIM

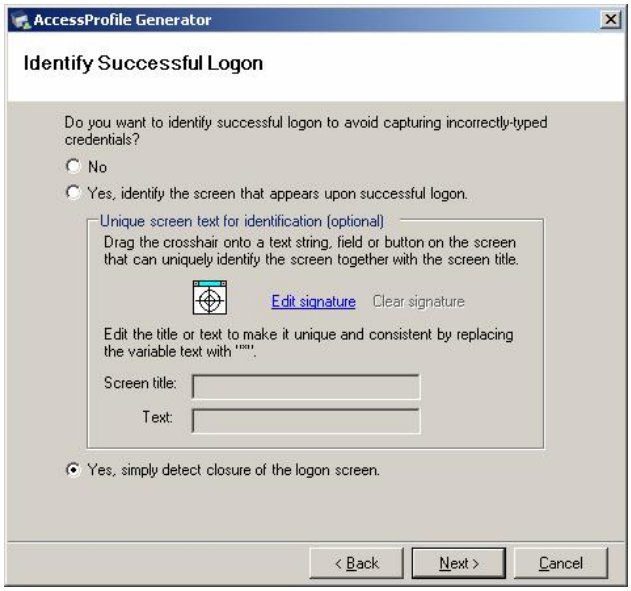


- Click “Next”

- To avoid logon loops when the logon prompt re-appears immediately after log out, select “Ask user” in the drop list and click “Next”



- In the next screen, select “Yes, simply detect the closure of the logon screen” to identify successful logon[‡‡‡]. Click “Next”



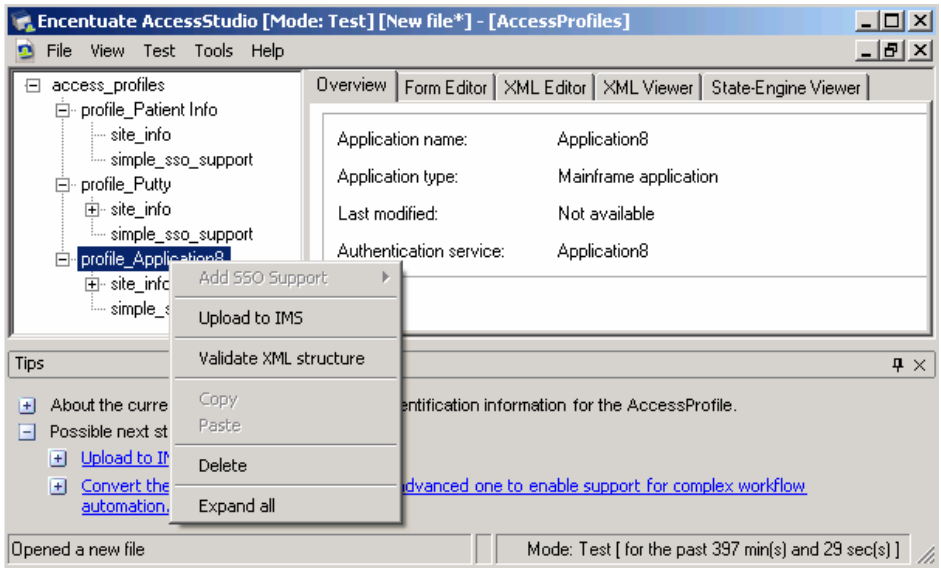
[‡‡‡] Encentuate can be configured to recognize a successful login before storing an application credential. In this case, closure of the Patient Information Manager log on screen indicates successful login.

- Choose ”Create one for me automatically” to automatically create an authentication service[§§§].

- Click “Finish”. This completes the profile generation for PIM.

If you made an error in the above profile generation:

- Right click on the profile in the left pane of AccessStudio and select “Delete”

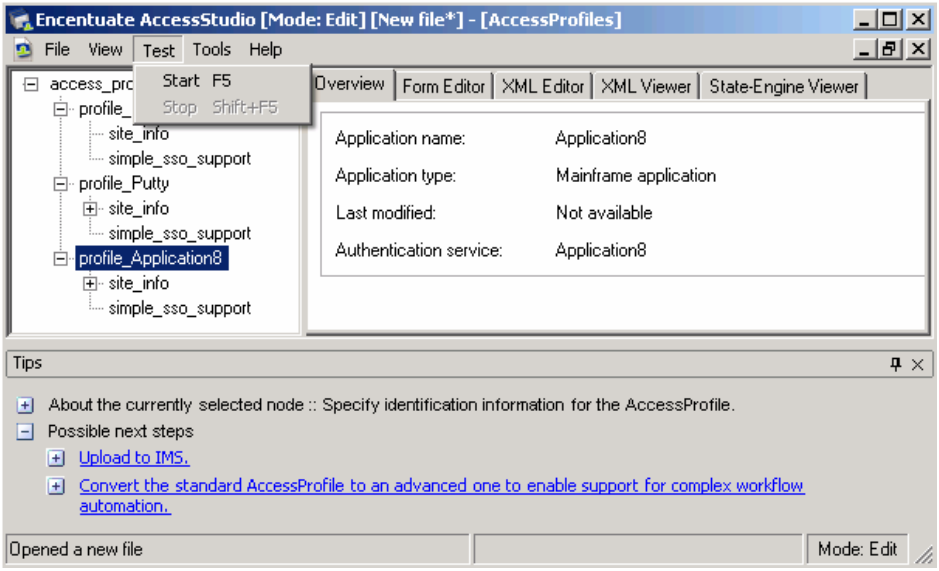


[§§§] Most applications are configured to authenticate against their own user stores, however some may rely on a common directory service for authentication. This step allows you to specify the authentication service for the application.

- Repeat the steps in this section to re-generate the profile

To test the profile generated:

- Exit PIM without login.
- In AccessStudio, click on menu Test >Start.

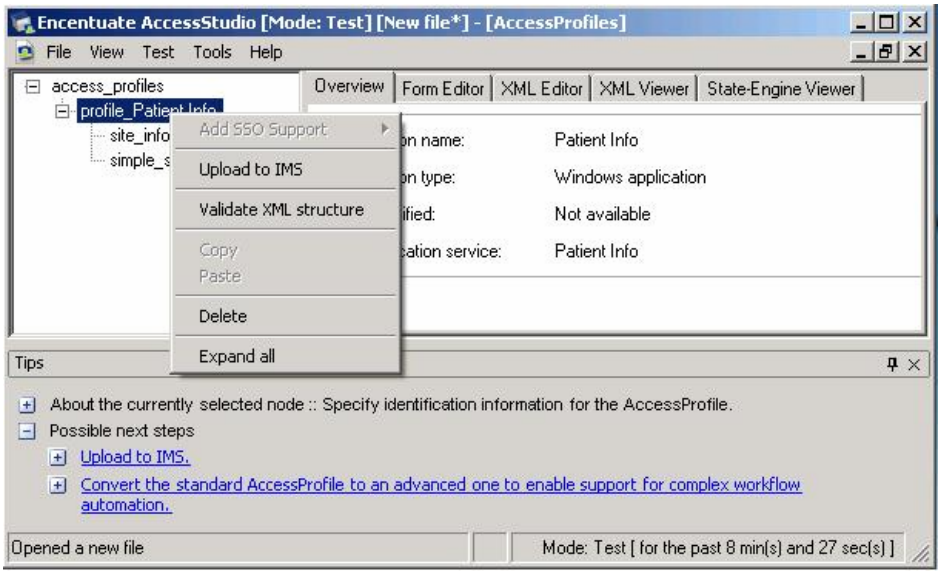


- Launch PIM again. Enter username: doctor-bob, password: encentuate.
- Click on “Yes” when prompted to save credentials into wallet[****].

- Exit and re-launch PIM. Observe that Encentuate now single signs-on to PIM

[****] In Test Mode, the credentials are only saved in a test wallet and will not affect the actual contents of the wallet. This protects against any errors; it also means that the credentials have to be re-captured once the profile is published.

- In AccessStudio, right click on “Profile_Patient Info” and choose “Upload to IMS” to publish the profile.



- Close AccessStudio when finished

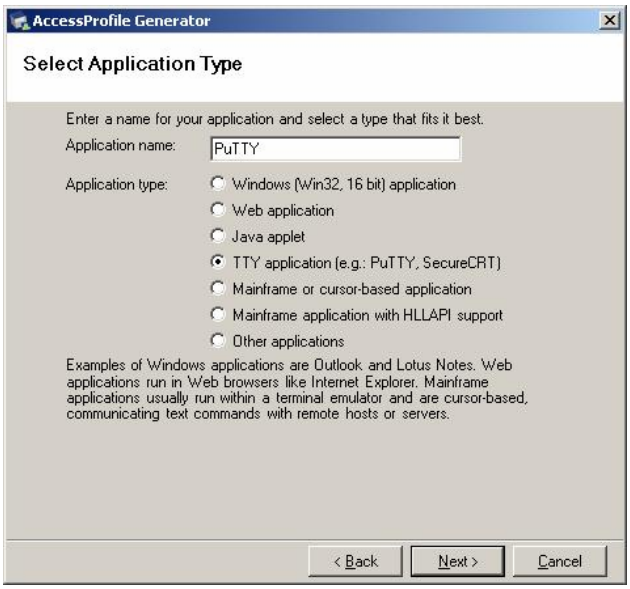
Profiling a TTY Application for SSO support

To enable single sign-on (SSO) for TTY applications, an AccessProfile for the application needs to be generated and uploaded to the IMS server. Most profiles can be auto-generated using the AccessStudio Wizard. In this training sequence, the AccessProfile for PuTTY, a common TTY application, will be auto-generated:

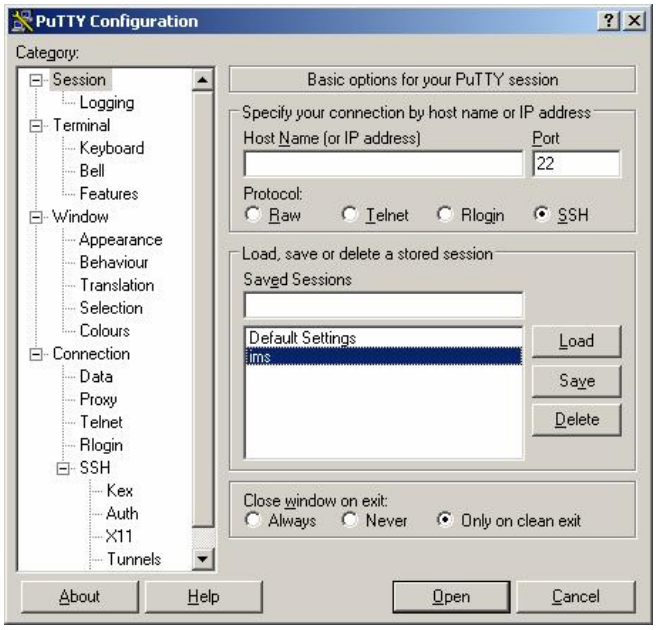
- On the Client VM (ENC AA XPSP2), click CTRL-ALT-DEL to lock screen if it is not already locked
- Logon as username: doctor-bob and password: himmss
- Click on Start >All Programs >Encentuate AccessStudio >AccessStudio
- Since there is already a predefined profile for PuTTY on the IMS, we need to remove it before we continue. Here are the removal steps:

    1. Click on File > Import Data from IMS
    2. Scroll down the left pane to find sso_site_wnd_putty
    3. Right click to delete it; click Yes to prompt to also remove from IMS.
    4. Click on File > New to clear the session data.

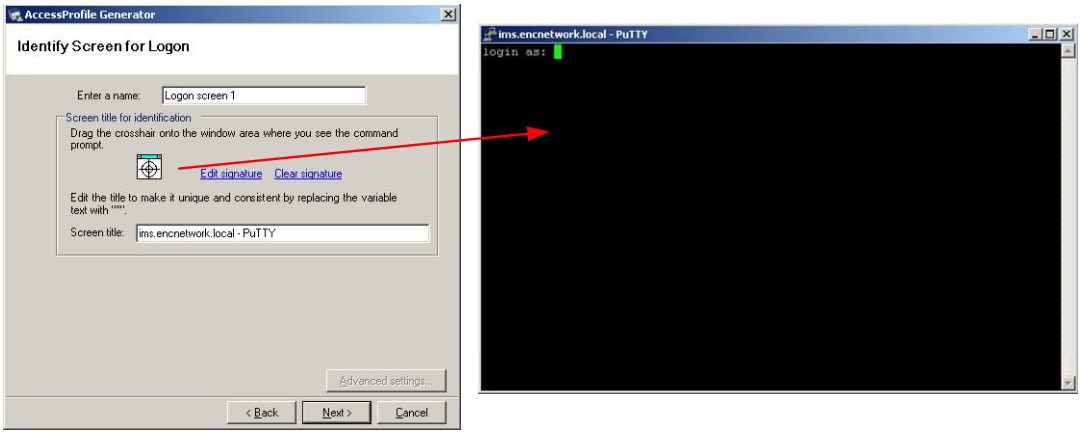
- Click on menu Tools >Start AccessProfile Generator
- In the “Welcome” screen, click “Next”
- Enter “PuTTY” in the application name field and select “TTY” as the application type; click “Next”



- In the “Select Task to Automate” screen, select task as “Logon”; click “Next”
- Double-click on the PuTTY icon located on the desktop to run it
- Choose the “ims” session and click “Open”

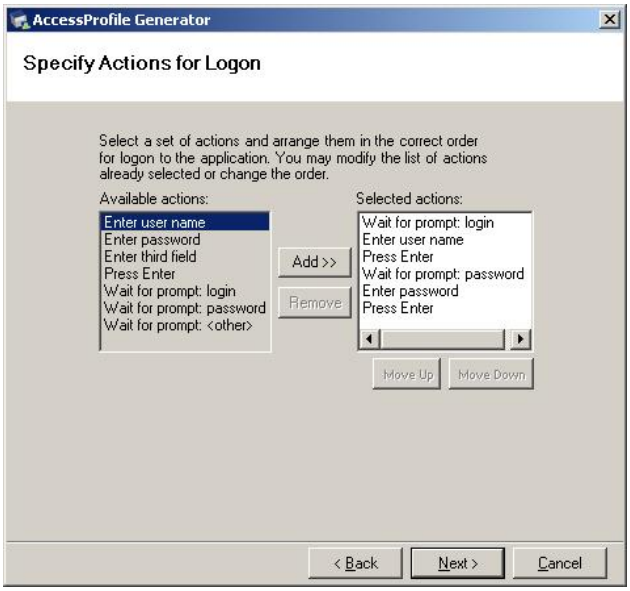


- In the AccessProfile Generator, click and drag the cross hair onto Putty's TTY screen.



- Click "Next"

- In the “Specify Actions for Logon” screen, click “Next” to accept the default action



- In the “Identify Successful Logon” screen, select “No”. Click “Next”
- In the “Select or Create Authentication Service” screen, select “Create one for me automatically”. Click “Next”
- Click “Finish”. This completes the profile generation for PuTTY

To test the profile generated:

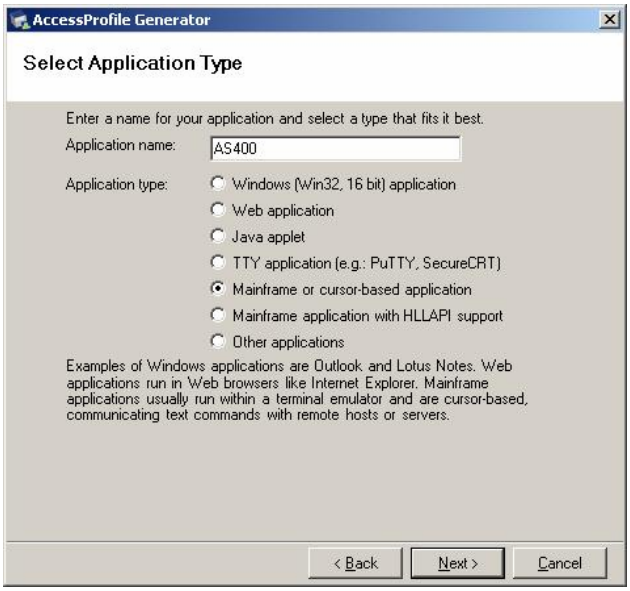
- Exit PuTTY without login.
- In AccessStudio, click on menu Test >Start.
- Launch PuTTY again. Enter user name: doctor-bob, password: himmss.
- Click on "Yes" when prompted to save credentials into wallet.
- Exit PuTTY. Launch it yet again. Observe that Encentuate now single signs-on to the PuTTY.
- In AccessStudio, right click on "Profile_PuTTY" and choose "Upload to IMS" to publish the profile.
- Close AccessStudio when finished.

Profiling a Mainframe Application for SSO support

To enable single sign-on (SSO) for mainframe applications, an AccessProfile for the application needs to be generated and uploaded to the IMS server. Most profiles can be auto-generated using the AccessStudio Wizard. In this training sequence, the AccessProfile for Attachmate (AS400), a common mainframe application, will be auto-generated:

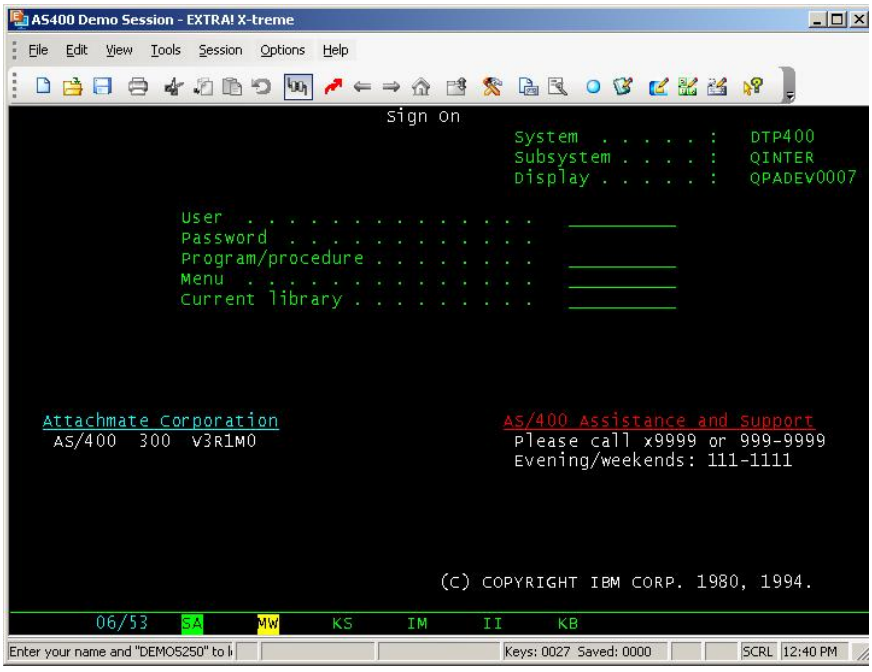
- On the Client VM (ENC AA XPSP2), click CTRL-ALT-DEL to lock screen if it is not already locked
- Logon as username: doctor-bob and password: himmss
- Click on Start >All Programs >Encentuate AccessStudio >AccessStudio
- Click on menu Tools >Start AccessProfile Generator.
- In the "Welcome" screen, click "Next"

- Enter “AS400” in the application name field and select “Mainframe or cursor-based” as the application type; click “Next”

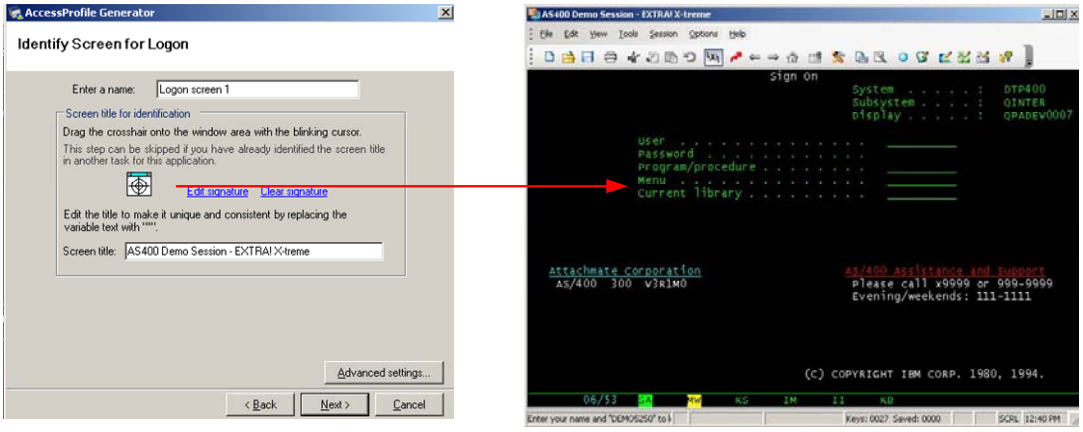


- In the “Select Task to Automate” screen, select task as “Logon”; click “Next”

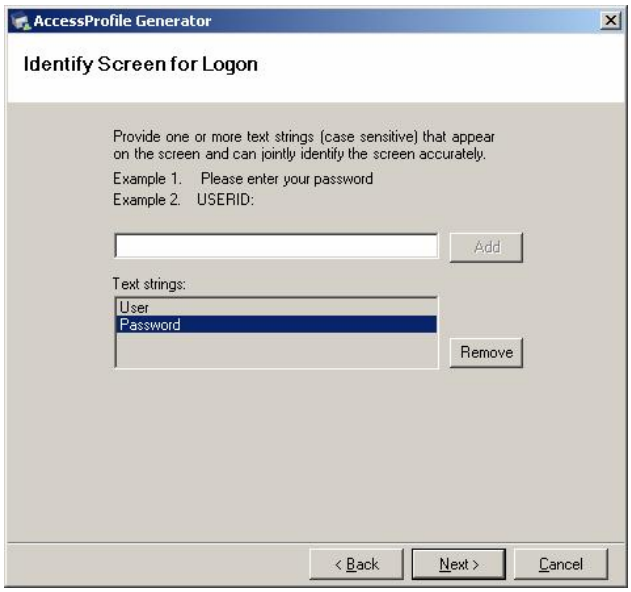
- Double-click on desktop icon AS400 Session to start it.



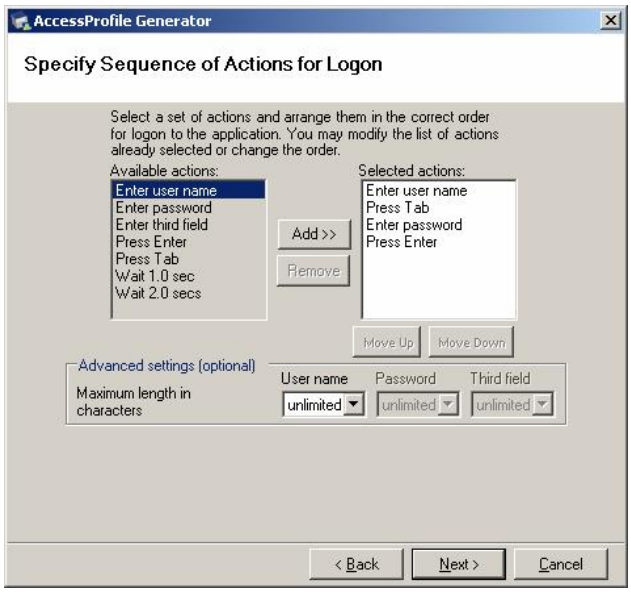
- In the AccessProfile Generator, click and drag cross hair onto AS400 Session’s black/green display; Click “Next”



- In the “Identify Screen for Logon” screen,
    - Enter “User” and click “Add”
    - Enter “Password” and click “Add”
    - Click “Next”



- In the next screen, accept the default sequence of actions. Click “Next”



- In the “Identify Successful Logon” screen, select “No”. Click “Next”

- In the “Select or Create Authentication Service” screen, select “Create one for me automatically”. Click “Next”
- Click “Finish”. This completes the profile generation for AS400.

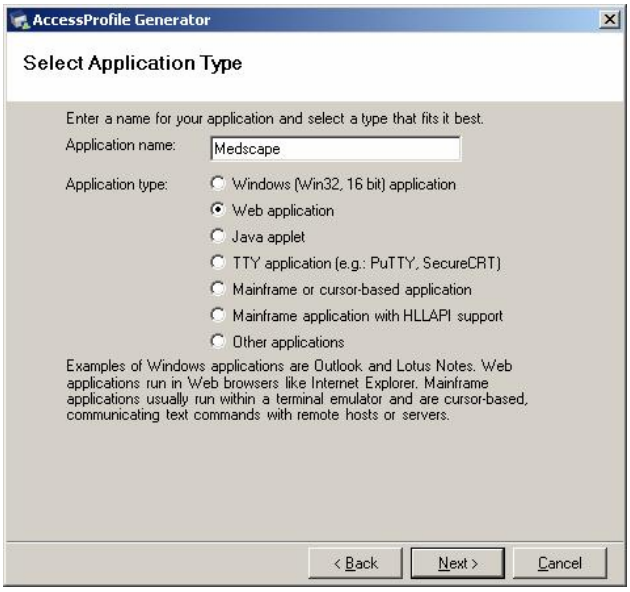
To test the profile generated:

- Exit AS400 without login
- In AccessStudio, click on menu Test >Start
- Launch AS400 Session again. Enter user name: bob, password: DEMO5250.
- Click on “Yes” when prompted to save credentials into wallet
- Exit AS400. Launch it yet again. Observe that Encentuate now single signs-on to the AS400
- In AccessStudio, right click on “Profile_AS400” and choose “Upload to IMS” to publish the profile
- Close AccessStudio when finished.

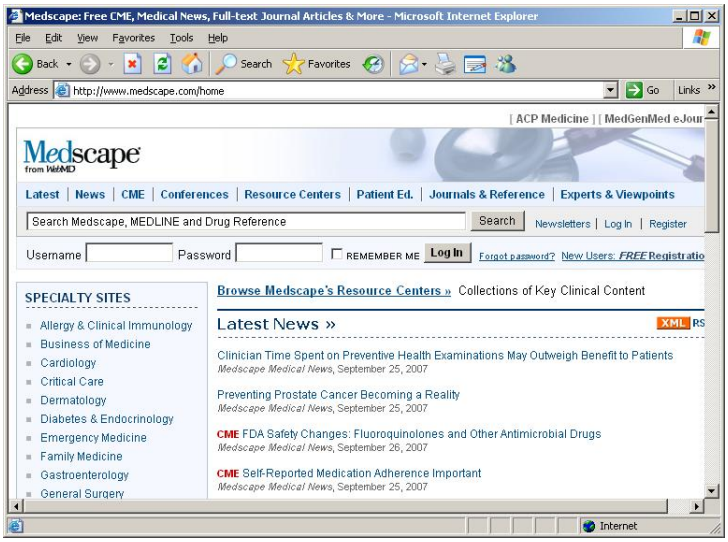
Profiling a Web Application for SSO support

Encentuate can single sign-on to most Web applications without an AccessProfile. Where necessary, an AccessProfile for the web application may be auto-generated and uploaded to the IMS server. In this training sequence, the AccessProfile for Medscape, a popular web medical application, will be auto-generated:

- On the Client VM (ENC AA XPSP2), click CTRL-ALT-DEL to lock screen if it is not already locked
- Logon as username: doctor-bob and password: himmss
- Click on Start >All Programs >Encentuate AccessStudio >AccessStudio
- Click on menu Tools >Start AccessProfile Generator
- Enter “Medscape” in the application name field and select “Web” for application type; click “Next”

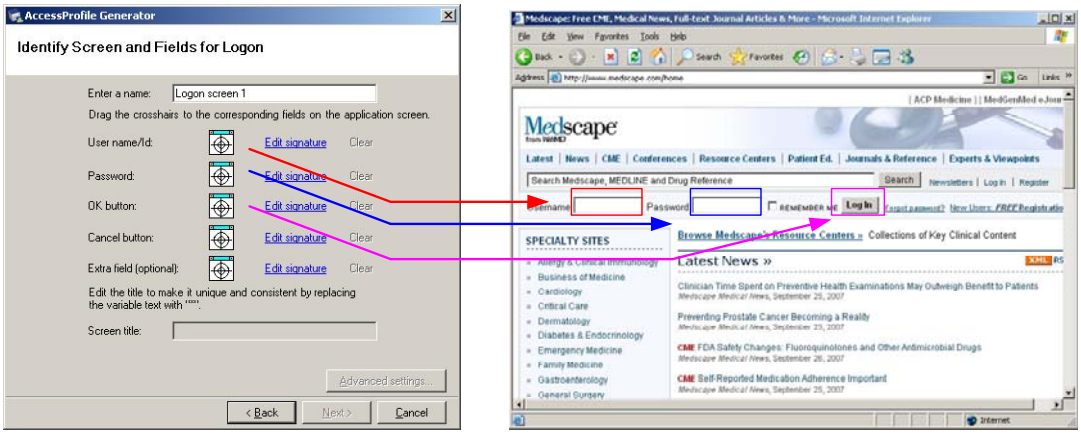


- In the “Select Task to Automate” screen, select task as Logon; click “Next”
- Double-click on desktop icon Medscape Online to start it



- Click and drag the cross hair for the following onto the Medscape logon screen:
    - The “User name” cross hair should be dropped at the user name field of Medscape.
    - The “Password” cross hair should be dropped at the password field of Medscape
    - The “OK button” cross hair should be dropped at the Log In button of Medscape

- Click “Next”



- In the “Identify Screens and Fields for Logon” screen, click “Next” to accept the default action
- In the “Identify Successful Logon” screen, select “No”. Click “Next”
- In the “Select or Create Authentication Service” screen, select “Create one for me automatically”. Click “Next”
- Click “Finish”. This completes the profile generation for Medscape

To test the profile generated:

- Exit Medscape by closing the browser.
- In AccessStudio, click on menu Test >Start.
- Launch Medscape Online again. Enter user name: doctor-bob, password: encentuate.
- Click on Yes when prompted to save credentials into wallet
- Exit Medscape Online. Launch it yet again. Observe that Encentuate now single signs-on to the Medscape.
- In AccessStudio, right click on “Profile_Medscape” and choose “Upload to IMS” to publish the profile.
- Close AccessStudio when finished.

Testing the End-user Functionalities

Now that the server and client environments have been set up, applications have been profiled for single sign-on, and users have been registered, you can now test drive the system as an end-user**. However, note that except for the AD credentials stored during registration, Bob's and Alice's Encentuate Wallets are empty as no application credentials have yet been captured for them**. In the following training sequence, Bob and Alice will use their applications as they normally do, and the application credentials will be transparently captured as they use their applications[††††]; Encentuate will automatically single sign-on to the applications the next time these applications are run.

- On the Client VM (ENC AA XPSP2), send CTRL-ALT-DEL to lock screen if it is not already locked. This simulates a typical kiosk waiting for user login

- Click "…My logon user name is not in the list" then enter username: doctor-bob and password: himmss

- Double click on Patient Information Manager on Bob's desktop. Enter user name: doctor-bob, password: encentuate.

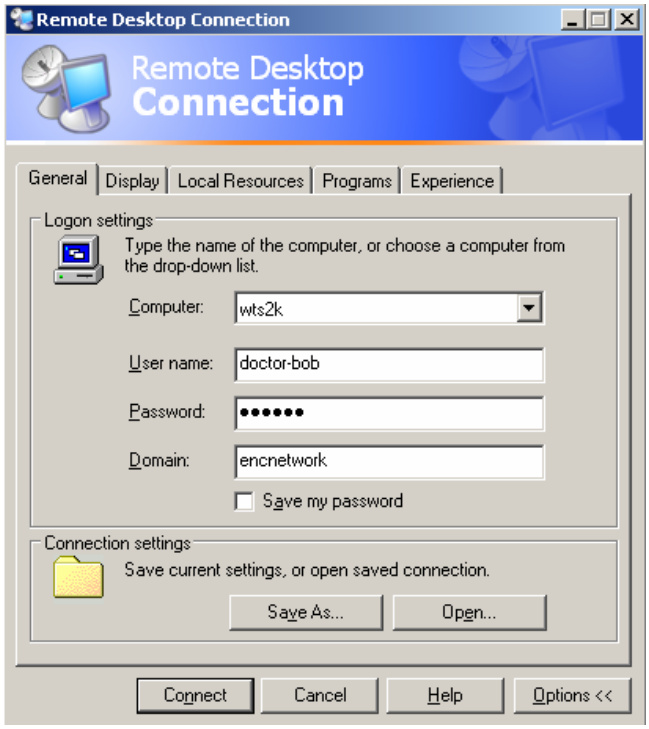
- Click on Yes when prompted to save credentials into wallet.

- Exit Patient Information Manager. Launch it yet again. Observe that Encentuate now single signs-on to the Patient Information Manager.

- Double click on Attachmate. Enter user name: bob, password: DEMO5250

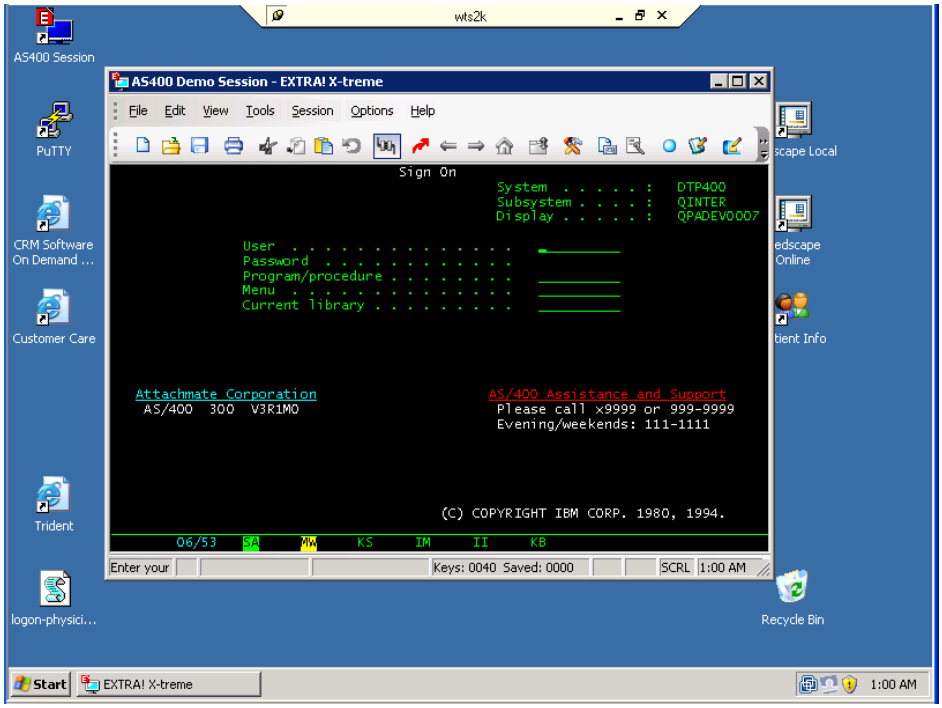
[††††] Alternatively, Encentuate can be integrated with provisioning systems and application credentials can be pre-provisioned into the users' Encentuate wallets.

- Click on Yes when prompted to save credentials into wallet.
- Exit Attachmate. Launch it yet again. Observe that Encentuate now single signs-on to Attachmate.
- Exit Attachmate.
- Double click on RDP to login to the Roaming Desktop on the Terminal Server.
    - Note the AD credential is automatically inserted into the screen below and the remote session is started without another login prompt.



Note that Encentuate is preconfigured to single sign-on to RDP using AD credentials by default and no custom AccessProfile is required.

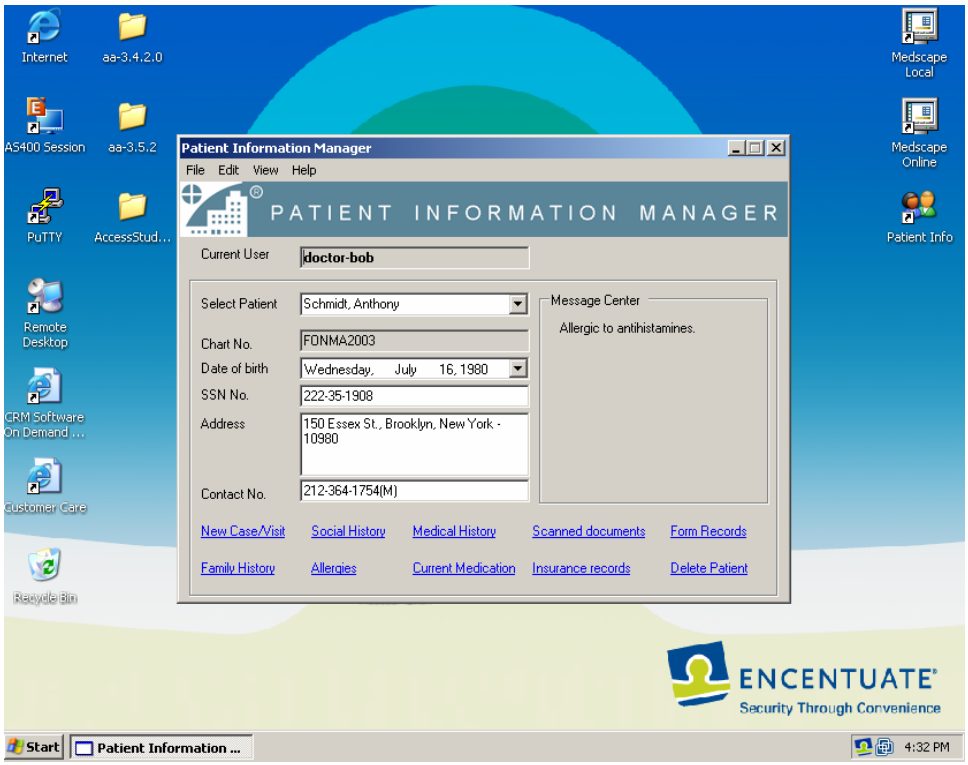
- On the remote desktop, double click on Attachmate. Observe that Encentuate single signs-on to Attachmate.



Note the single sign-on and the pass-through authentication from the Client VM to the Terminal Server to Attachmate on the roaming desktop. With Encentuate, users need only sign-on once even as they move from one server to another; supporting true single sign-on.

- Click on the [x] icon on the Remote Desktop to close the desktop. When prompted, click “OK” to close.

- You are back on the local desktop, and should see the following applications which you previously opened:



- If Alice wants to use this kiosk PC while Bob is away and screen is locked, she simply clicks "…My logon user name is not in the list" then types her user name and password on the Encentuate lock screen, and she is logged on her own desktop while Bob's desktop and open applications are preserved until he returns. To take over the desktop, send CTRL-ALT-DEL to the desktop[‡‡‡‡] (enter CTRL-ALT-INS from your keyboard) if it is not already on lock screen

- Click "…My logon user name is not in the list" then logon as username: nurse-alice and password: himmss

- Note that her own desktop appears with no app open (click on "Start" to see user's account name).

- Double click on Medscape. Enter user name: nurse-alice, password: encentuate.

[‡‡‡‡] If strong authentication is used, all that Alice has to do is to swipe her finger or tap her badge.

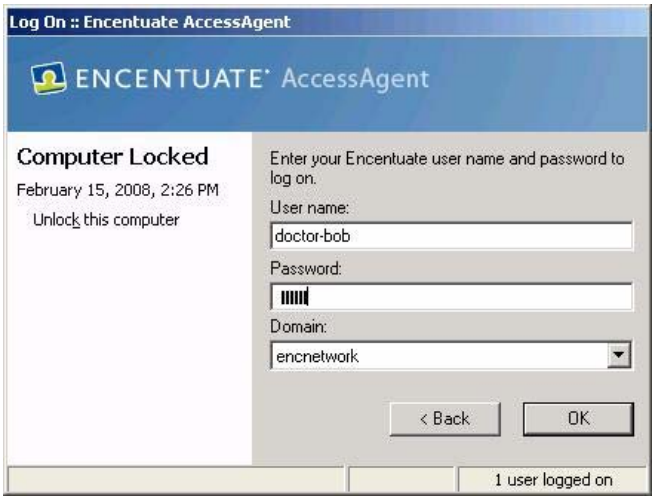
- Click on Yes when prompted to save credentials into wallet
- Exit Medscape. Launch it yet again. Observe that Encentuate now single signs-on to the Medscape.
- Send CTRL-ALT-DEL to screen lock the desktop.

Now when Bob returns, he simply clicks on his user name and types his password. He will then see the desktop with Patient Information Manager opened – exactly where he left his private session. If Bob then walks away and Alice returns to login again, she will see her own desktop with a Medscape browser session as she last left it. The private desktop mode provides fast user switching for multiple users sharing a kiosk while ensuring single sign-on for all users. It does this without the disruptive closure of running applications and session logoff with each user switch.

Testing the Administrator Functionalities

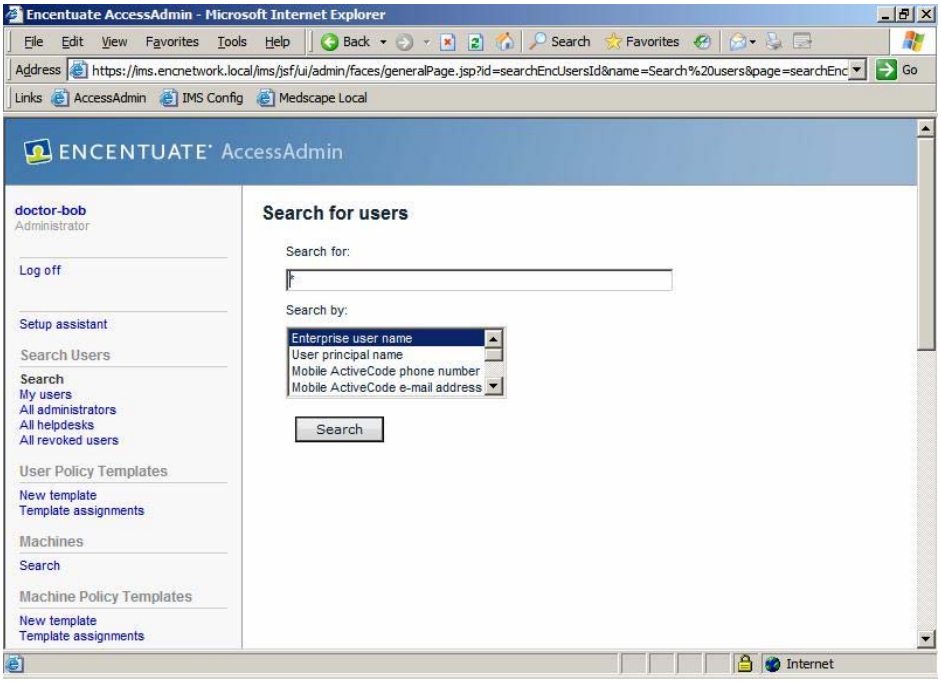
Now that the installation is complete, applications have been profiled, users are registered and you have test drove the system as an end user, you can now test drive the centralized web administration interface:

- On the Client VM (ENC AA XPSP2), click CTRL-ALT-DEL to lock screen if it is not already locked. This simulates a typical kiosk waiting for user login
- Logon as username: doctor-bob and password: himmss

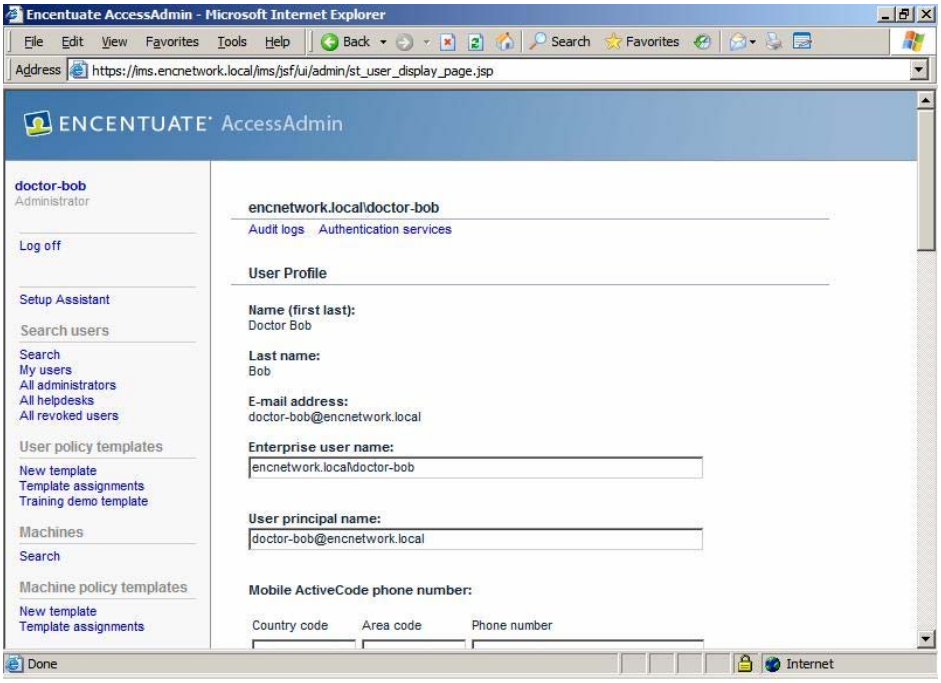


- Double click the AccessAdmin icon.
- Select the AccessAdmin link (only one on the left pane).

- In the search page, enter “d*” in the search field and click “Search”



- AccessAdmin provides policy templates that can be assigned to different user groups. Bob’s template is displayed below



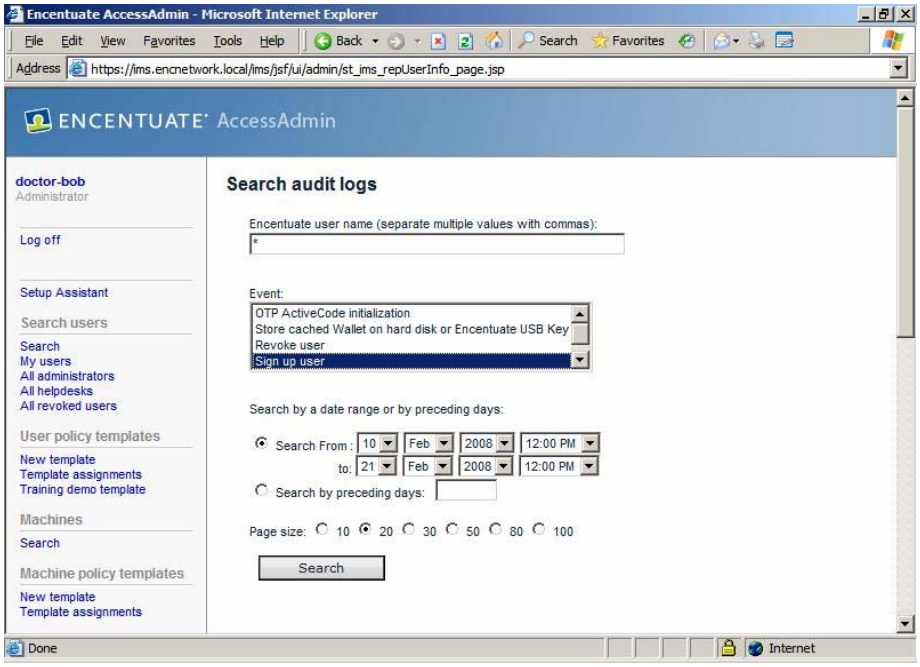
- Click through various sections to get a quick tour of policy types.

- Encentuate also provides centralized SQL reporting. Encentuate AccessAgent automatically tracks user activities from each end-point, including what applications they login to, who they login as, when they login, and from where. This is collated centrally in the SQL database used by IMS.

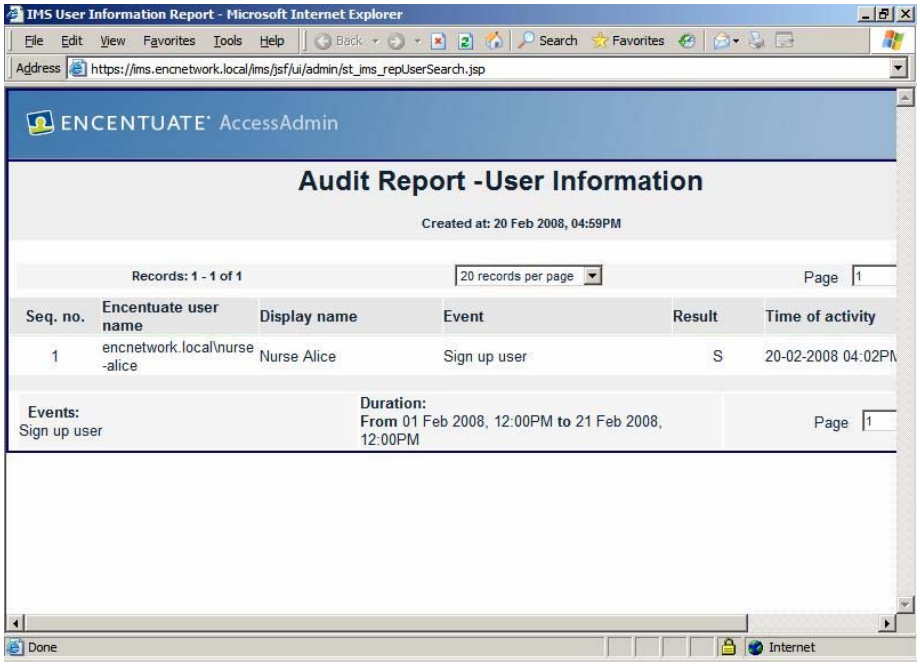
- To see a sample report:

    - Click on “User Information” in the Reports section on the left pane

    - Click on “User Signed-up” to report on new users registered.



- Click “Search” to generate the report



Encentuate provides centralized SQL logging and it works with major SQL reporting engines to provide centralized SQL reporting.

What you have learned

If you have successfully completed the training scenarios above, you have learned:

- How to install and setup an IMS server to work with Microsoft Active Directory
- How to install and setup AccessAgent on Microsoft Terminal Services to provide Roaming Desktops
- How to install and setup AccessAgent on Windows XP, configured to work in Private Desktop mode
- How to install AccessStudio and profile the following example applications for Single Sign On:
  - A Windows 32 application
  - A teletype (TTY) application

    - A mainframe green screen application
    - A web application

- How to register an administrator Bob and an end user Alice
- How to operate the system as an end-user: Bob and Alice, and
- How to operate the system as an Administrator.

For more in-depth training, please contact Encentuate for formal training courses.

About Encentuate

Encentuate is a leading provider of enterprise end-point identity and access management solutions that help customers cost effectively simplify access to corporate information, strengthen security, and track compliance at enterprise end points without requiring changes to existing IT infrastructure. Encentuate is headquartered in Silicon Valley, Calif. and has offices across North America and in Singapore. Encentuate's customers span a range of industries, including healthcare, biotechnology, government and financial services. In 2007, SC Magazine named Encentuate IAM the **best identity management solution**. Previously, Encentuate was also recognized by SC Magazine as the **best single sign-on** and **best two-factor authentication solution**. More information about Encentuate is available at www.encentuate.com or by calling +1.866.362.3688.

[This page intentionally left blank]