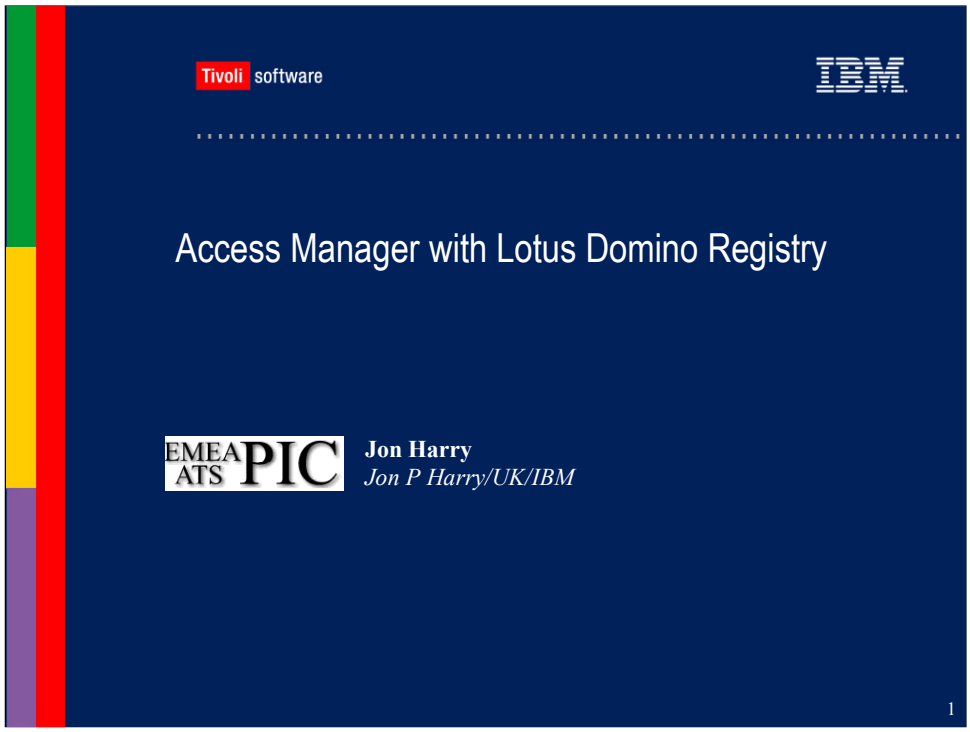
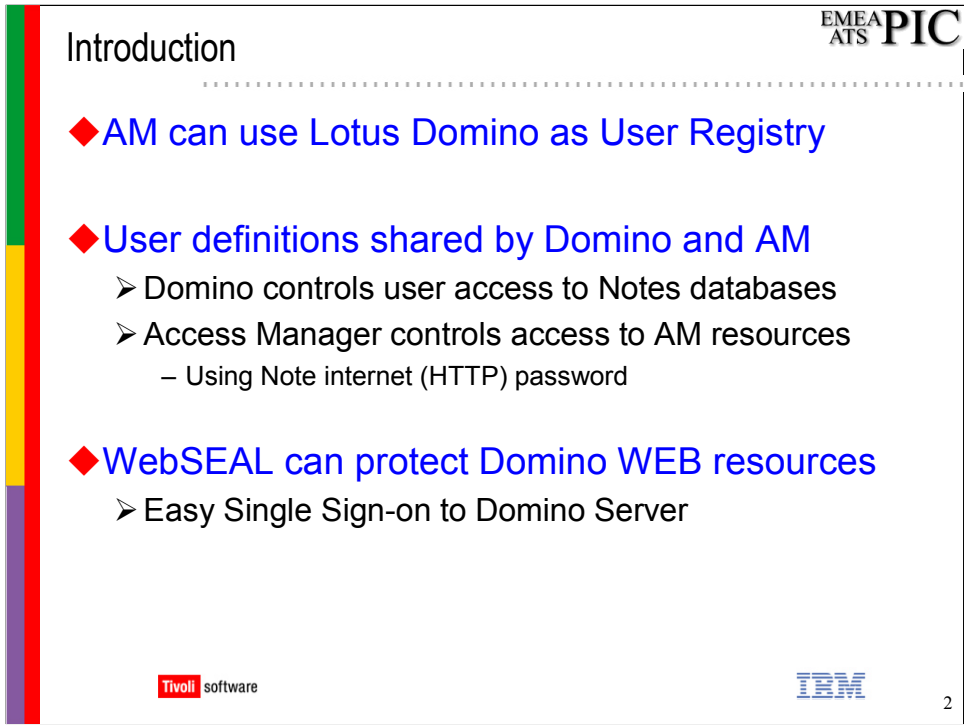


This presentation describes the support for a Lotus Domino user registry in Access Manager v3.9.

Originally partial support for Domino as a user registry was introduced in Policy Director v3.7 but this required a number of manual configuration steps and was subsequently withdrawn in Policy Director v3.8.

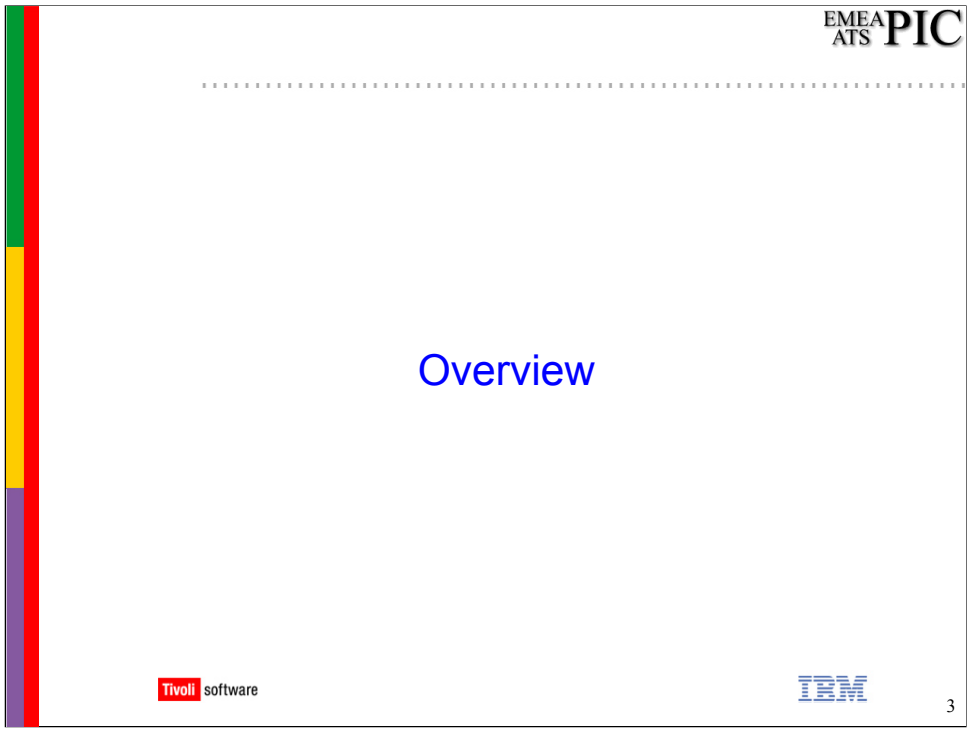
The support has now been re-introduced. This time there is fully automated install/config which makes it much easier to set up.

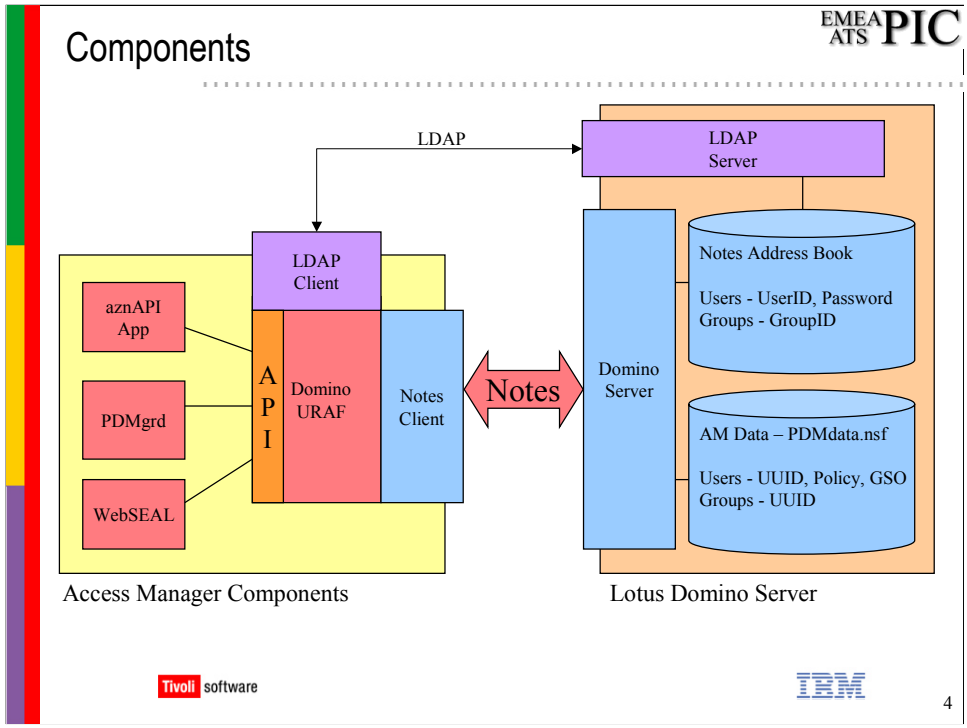


Using Lotus Domino as the Access Manager user registry means using the Domino domain Address Book (NAB) as the repository of user information rather than using LDAP.

The user definitions in the NAB are shared between Access Manager and Domino. This means that there are no user synchronisation problems for applications using user definitions in the NAB. Any user created by Access Manager (or created by Domino and imported into Access Manager) can access both Domino and Access Manager resources using the same identity.

The sharing of the user identity information (namely the users shortname and Internet password) means that achieving single sign-on is much simpler.


EMEA ATS PIC
Overview
Tivoli software
IBM
3



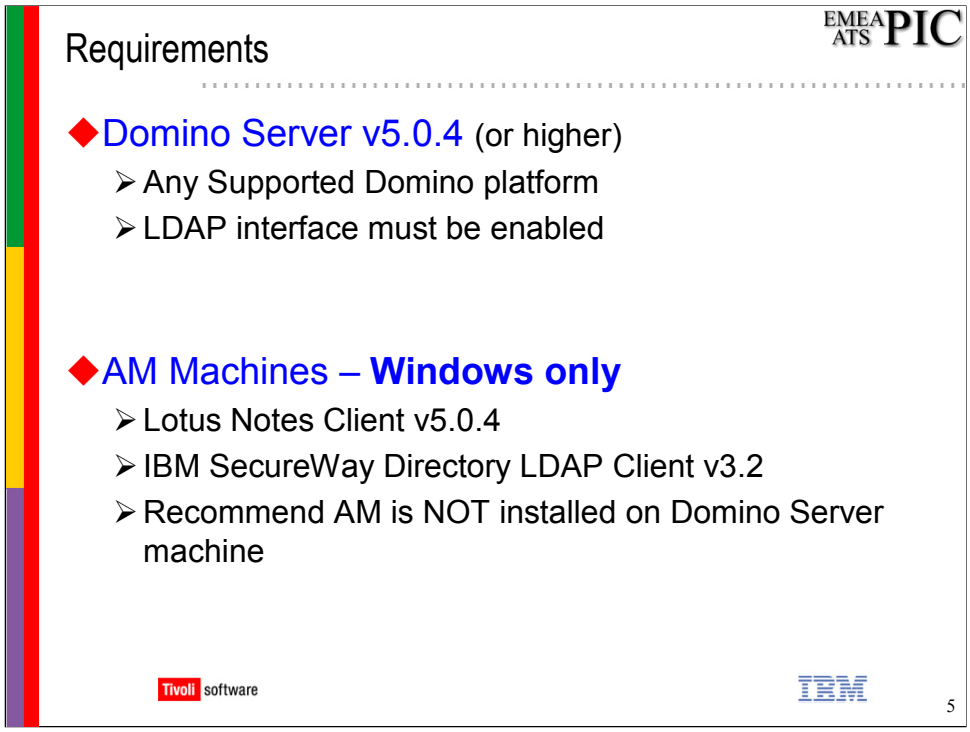
The diagram above shows how Access Manager communicates with Domino.

When Domino support is enabled, Access Manager components use a new AM interface (the URAF API) to make registry calls – rather than calling the original LDAP interface code. The domino implementation of the URAF interface then uses a local notes client and an IBM LDAP client to interact with a Domino server.

The LDAP client is used to perform remote authentication to the Domino LDAP server to verify username and password information. The Notes Client is used for direct access to the domain (using a pre-defined privileged account) for all other tasks (e.g. view/update user information)

User/Group information is split across two locations on the Domino Server. Information about a user that can already be expressed in Domino (such as name, description, group membership) is stored in the NAB. Access Manager specific information (such as GSO information,Policy information and UUID mapping) is stored in a special database called the PD Meta-data database.

Note: The URAF interface is an internal interface - it is described to assist understanding of how Domino is supported - it is NOT a published interface.

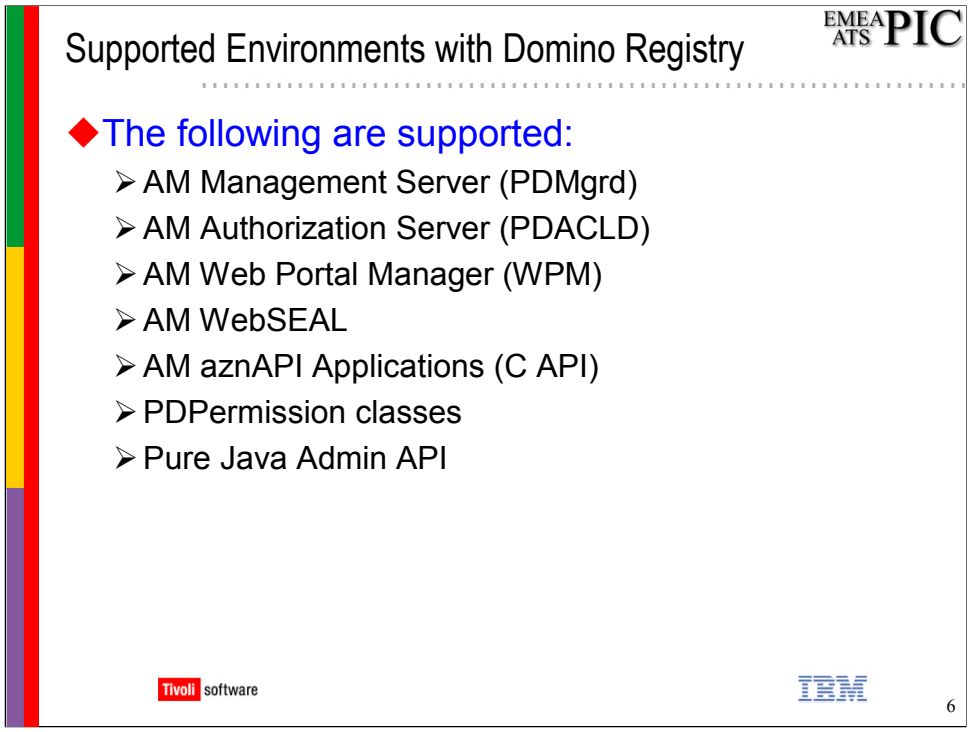


Lotus Domino server v5.0.4 is required for use with Access Manager. It can be running on any platform supported by Lotus.

The Domino server must have the LDAP interface enabled. This is required so that Access Manager can authenticate users using their Internet password.

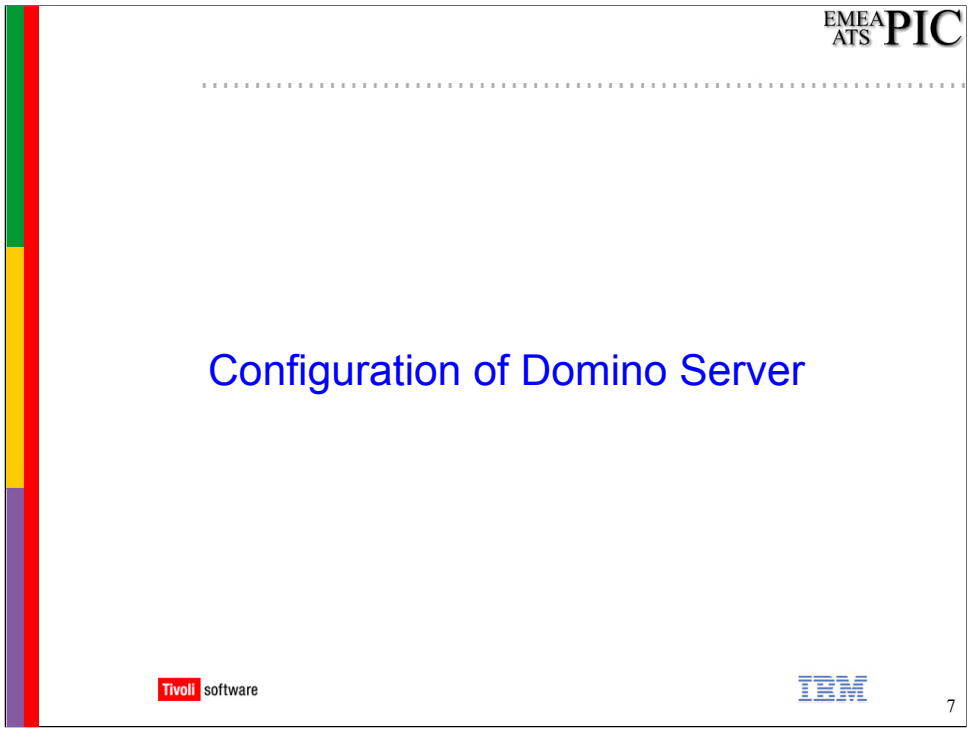
Access Manager components in an environment using a Domino user registry are **only supported on Windows**. This is because Access Manager requires the Notes client v5.0.4 which is only available on Windows. Since LDAP communication is required each AM machine also requires the IBM Secureway Directory client (v3.2) to be installed.

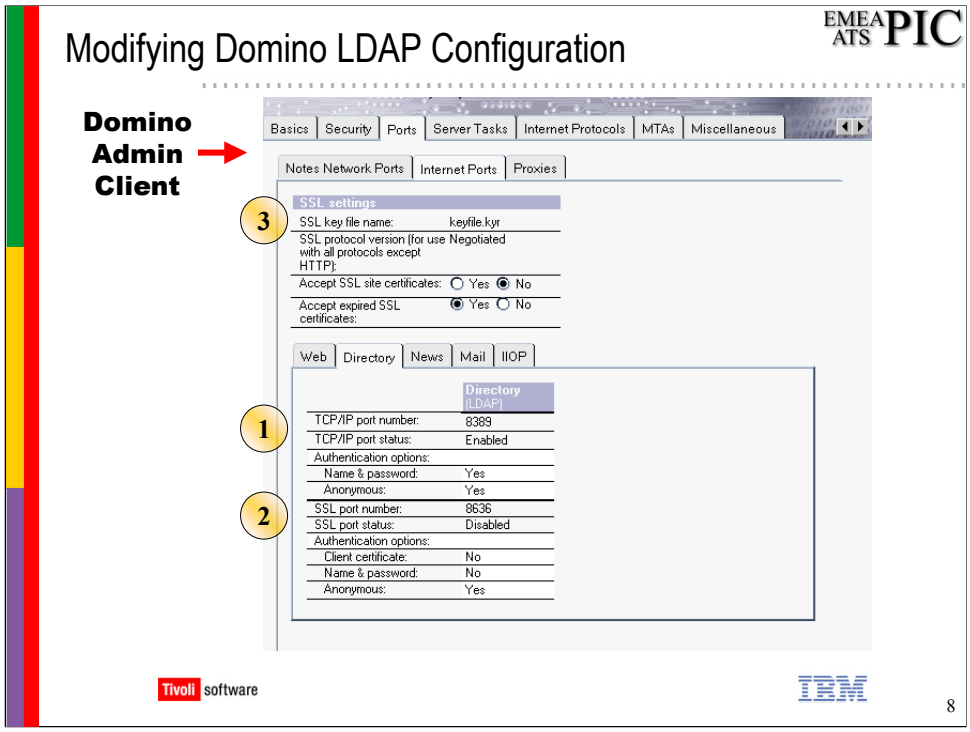
For performance reasons it is recommended to run the Domino Server on a machine that does not have any Access Manager components installed. However, this will work if a single machine installation is required (for testing or proof of concept for example).



Only the Access Manager components listed above are officially supported in an environment where Lotus Domino is being used as the user registry.

It may be possible to use other components (depending on their direct use of the registry) but their use is not officially supported.


EMEA ATS PIC
Configuration of Domino Server
Tivoli software
IBM
7

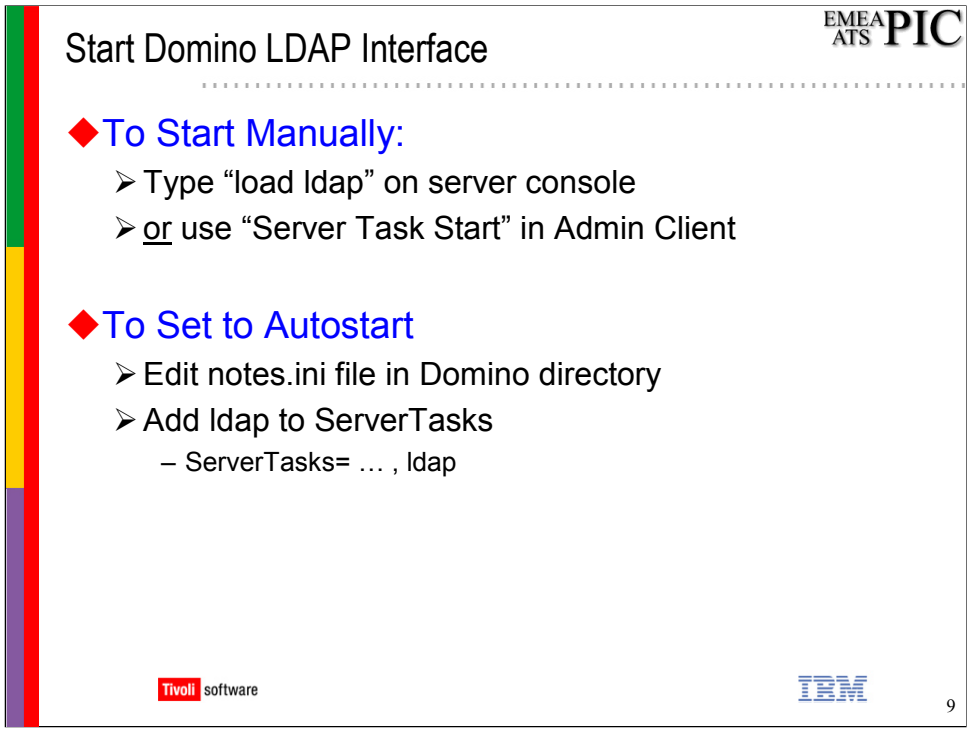


The screenshot above shows how the LDAP configuration of a Domino server can be modified. This panel is part of the Server Configuration in the Domino Administration Client.

-1- This is where the TCP port for the LDAP interface is set. By default this port is 389 but you may need to change this if another LDAP server is active on the same machine. The status indicates if the TCP port is enabled or not. This **does not mean that the port is active** – to activate the LDAP interface the LDAP task must be started (see later)

-2- This is where the SSL port for the LDAP interface is set. By default this is 636 but is disabled.

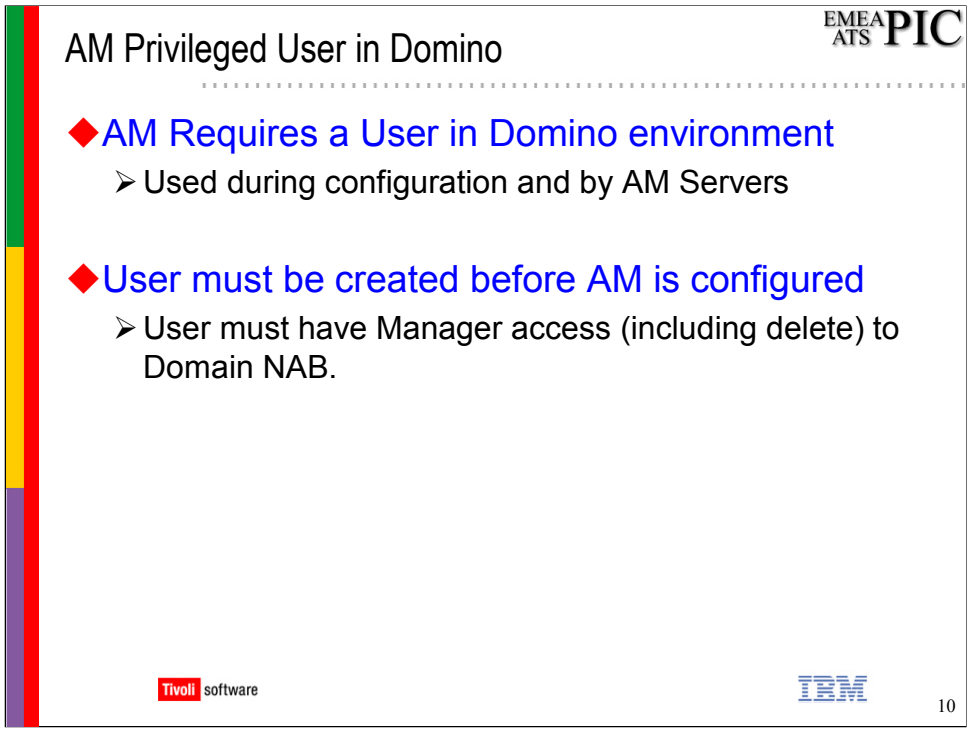
-3- If SSL is enabled for the LDAP interface then this information is used to locate the certificate and private key that will identify the LDAP server during SSL session negotiation.



Once the LDAP interface has been configured the LDAP task must be started. This can either be done directly from the Domino Console or by starting the LDAP task in the Administration client.

If the LDAP interface is always going to be needed then it is probably a good idea to add it to the tasks that are automatically started when the Domino Server is started. This list is configured in the notes.ini file for the Domino server. Add the keyword *ldap* to the end of the list for the *ServerTask* parameter.

Note: If you have a Notes Client installed on the same machine then there will be two notes.ini files. Be sure to select the correct one (The one in the Domino Server directory – C:\lotus\domino by default on windows)



In order to give Access Manager the authority it requires to configure itself in the Domino domain a user must be created in the Domino environment. This user must be configured before Access Manager configuration is started.

This user, that we will call the AM *Privileged User* requires Manager access (including delete) to the domain NAB.

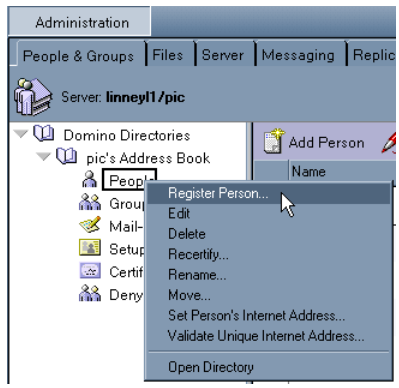
In addition to being used during configuration, the AM Privileged User identity is also used by all Access Manager servers to access the Domino environment – this is different from an LDAP environment where each server has its own identity to access the registry.

The name of the privileged user is not restricted – it can be anything that is valid in Domino.

Create AM Privileged User - 1

EMEA ATS PIC

- Navigate to “Register Person…” in Domino Administration Console
  - Do not use Add Person in NAB as this does not create a user



Tivoli software

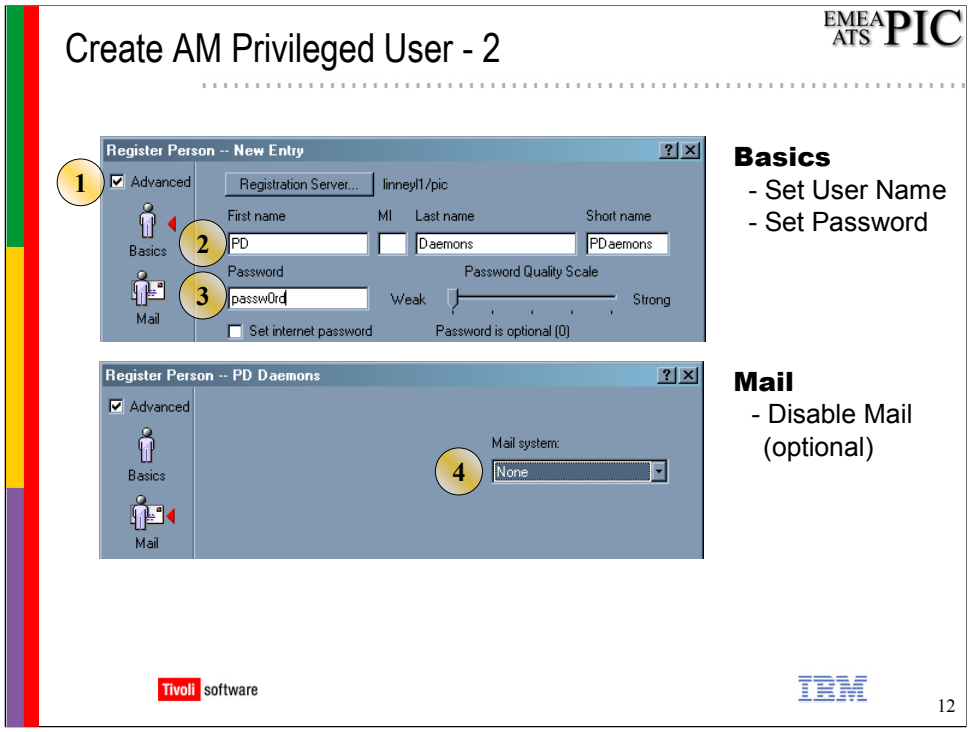
IBM

11

The screenshot above shows one way to access the user creation (registration) process in Domino. The screenshot is from the Domino Administration Client.

Go to the “People & Groups” tag and right-click on the People object in the domain address book. Select “Register Person…” from the pop-up menu.

Note: Do not use the “Add Person” button on the toolbar. This adds a user entry to the NAB but does not create a full Notes user (which is what is required for the AM Privileged User).



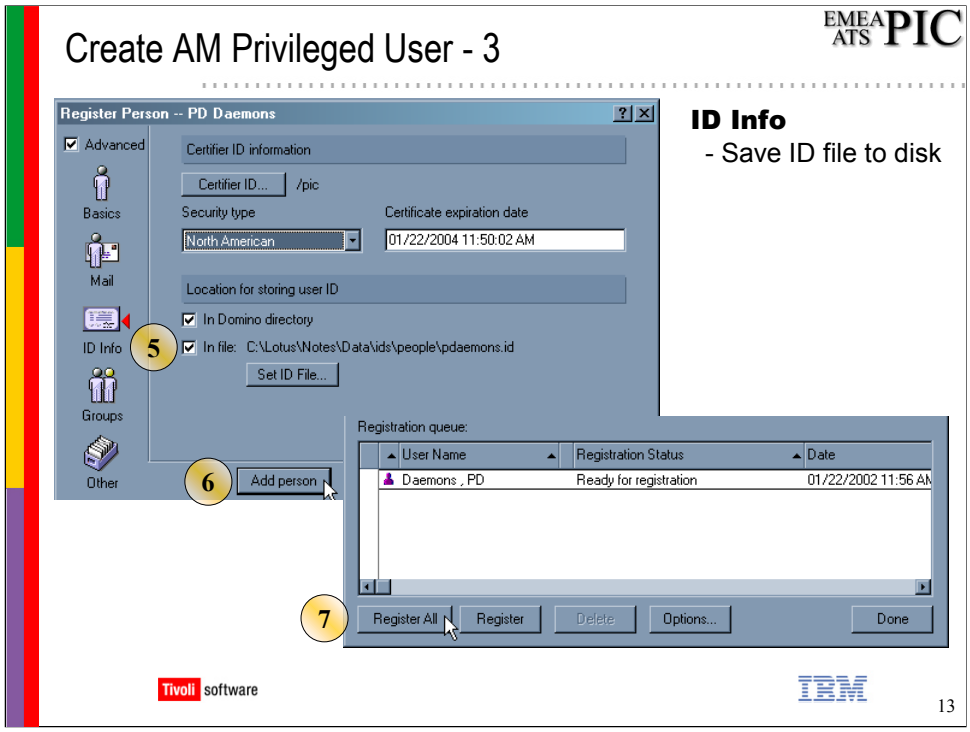
The screenshots above show the user registration dialog in the Domino Admin Client that is used to create the AM Privileged User.

-1- First, turn on the Advanced registration options. Some of these are needed to create the AM Privileged User

-2- Enter a name for the Privileged User. This can be whatever you like although something simple is probably better!

-3- Select a password for the user. You will need this password when configuring Access Manager. **Note:** This is a Lotus Notes password, NOT an internet password. The AM Privileged user does not require an internet password.

-4- In the Mail section change the Mail system to *None*. This is an optional step but it is not likely that this user will need to receive (or send) mail.

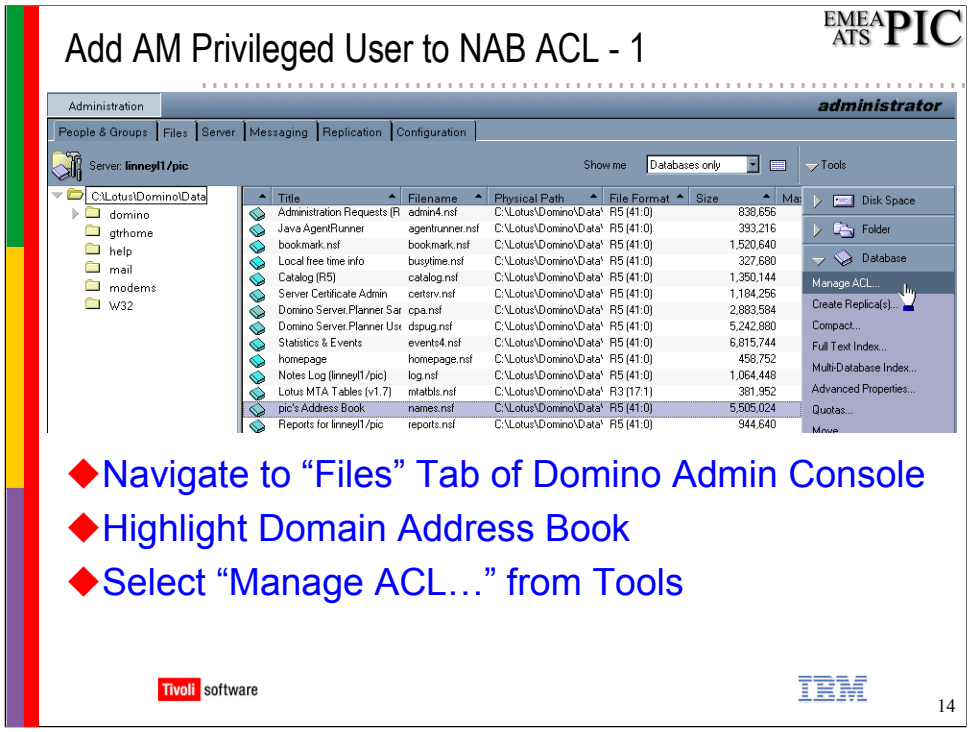


-5- In order to sign into Notes as the AM Privileged User, Access Manager will require the Domino ID file for the user. The easiest way to get this ID file is to have it saved as a file and then transfer it to the machines where AM components will be installed. In order to have Domino save the ID to a file select the "In File" option in the ID info section.

If you do not choose the "In File" option then you can find the ID file in the NAB attached to the users entry (as long as "In Domino Director" option is selected. The ID file can be detached to the local filesystem from there.

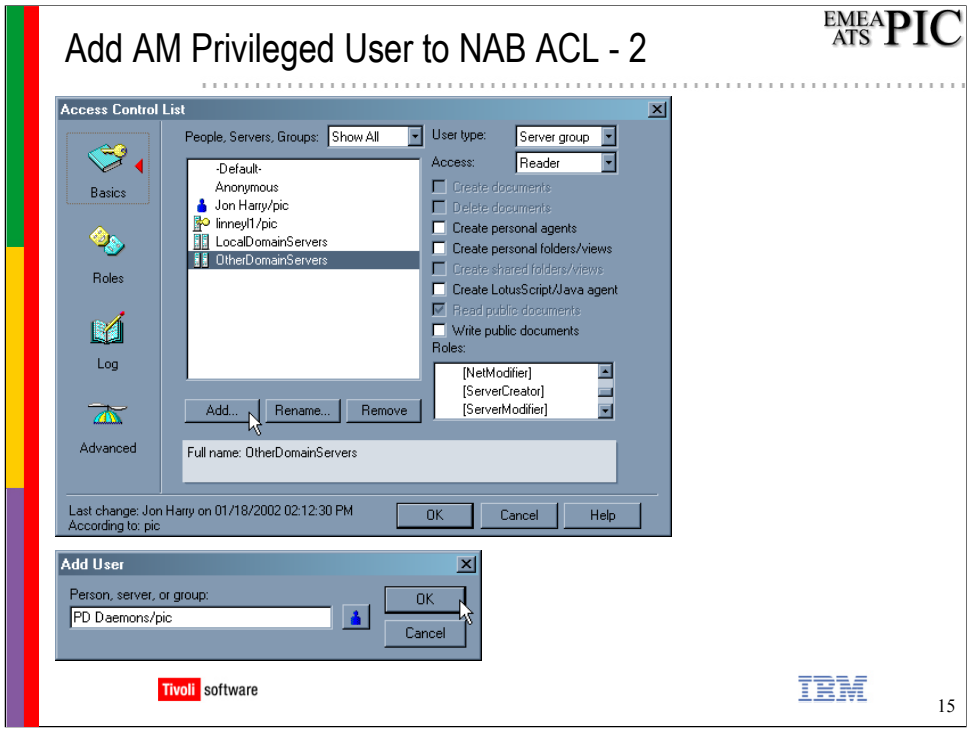
-6- To add the new user to the registration queue click the Add person button

-7- To register the AM Privileged User click the "Register All" button



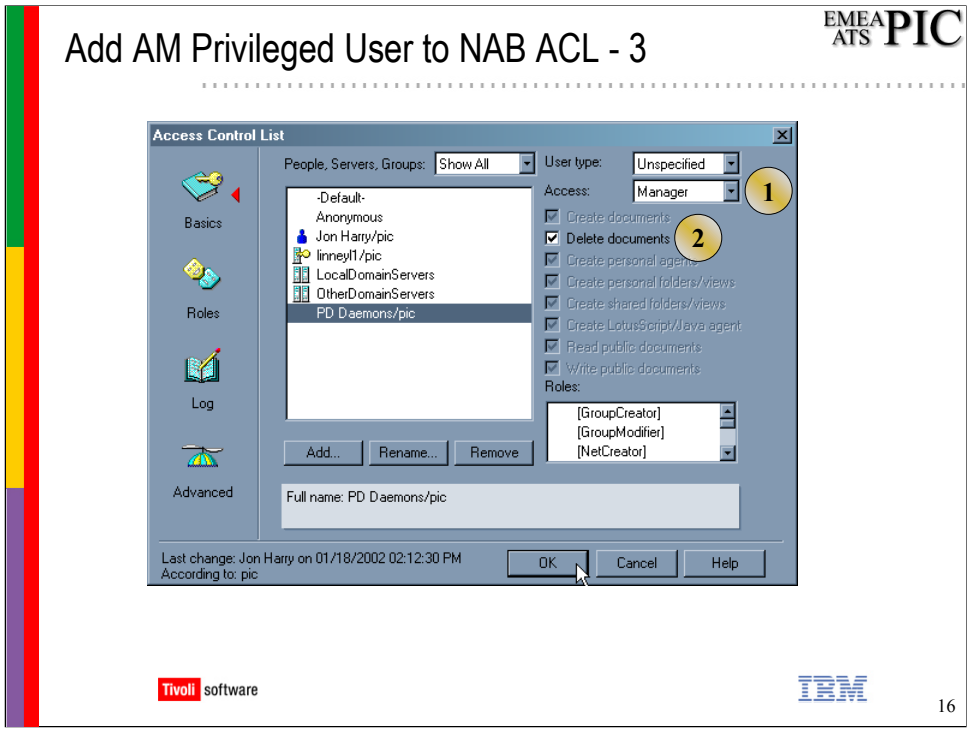
Once the AM Privileged User has been created the next task is to give it the required access to the domain address book.

The screenshot above shows the “Files” tab in the Domino Administration Client. Locate the domain address book (called <domain>’s Address Book) and select it. Go to the Tools bar, expand the Database section and select “Manage ACL…” as shown above.



In the Database ACL dialog click the add button to add an entry to the Access Control List.

In the pop-up window type the User name of the AM Privileged user and click OK. The User Name will have the form *Firstname Lastname/Domain*. If you don't know the exact username you can click on the person icon and use the address book pop-up that is displayed to choose the user from a list.



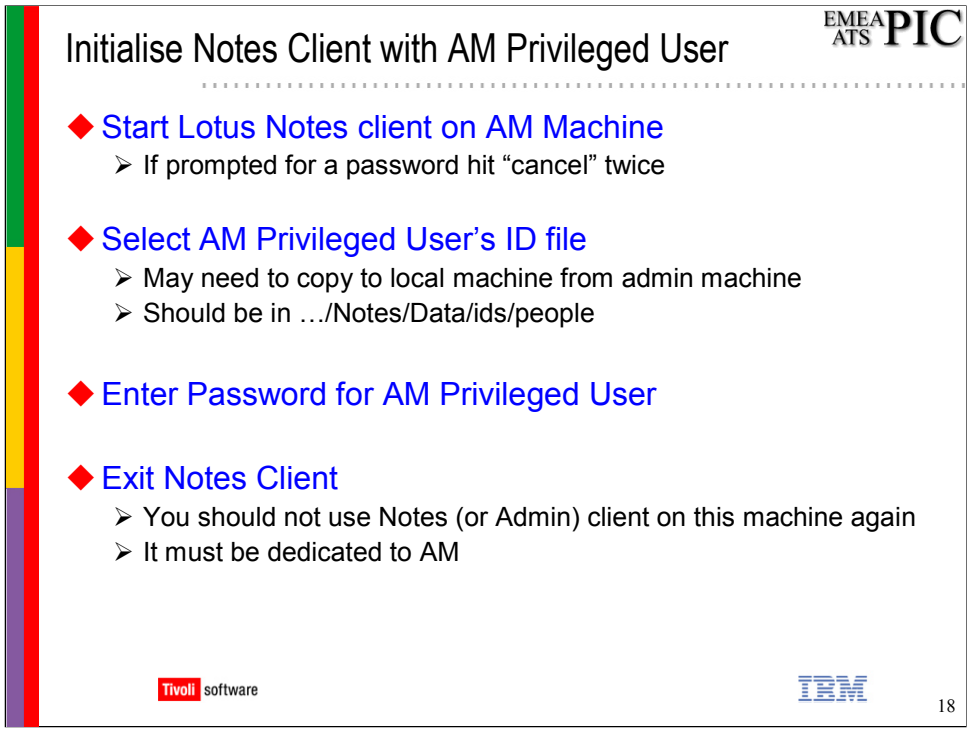
-1- Select the AM Privileged User in the ACL and change the Access to Manager. This gives the user all permissions except delete

-2- Check the Delete documents box to allow the user to delete documents from the domain address book.

Click OK to exit the ACL dialog.

Domino is now ready for AM to be configured.


EMEA ATS PIC
Access Manager Configuration
Tivoli software
IBM
17



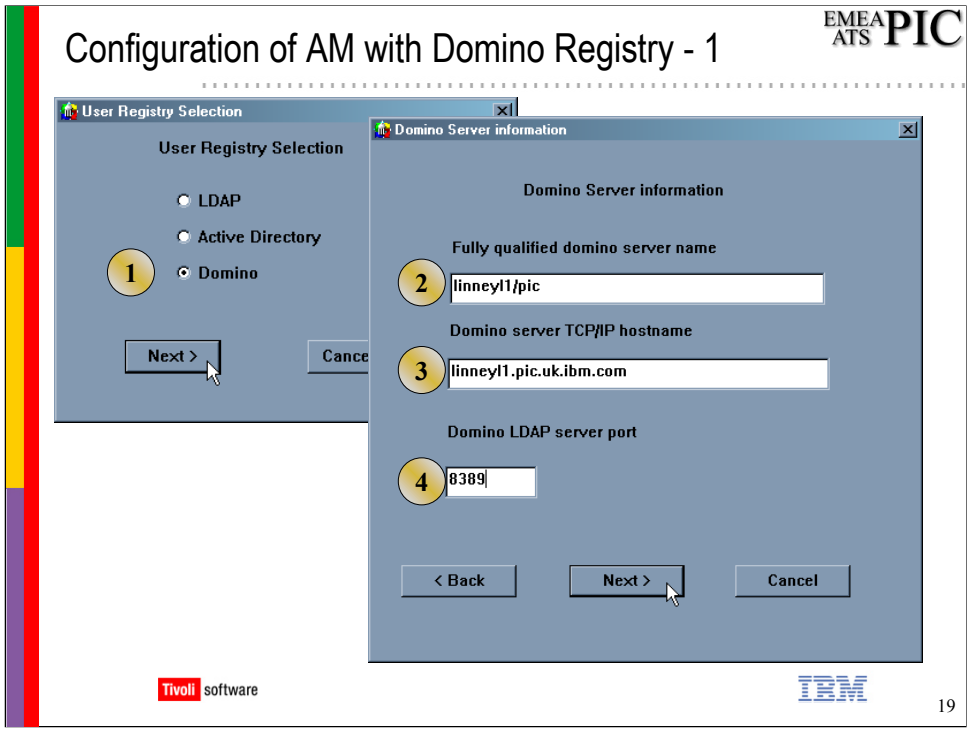
Each machine that will have Access Manager components installed requires a Notes Client. This client is used to access the data stored on the Domino Server and must have the AM Privileged User identity initialised on it.

First, assuming this is not the machine from which the AM Privileged user was created, copy the ID file of the AM Privileged User onto the local filesystem.

Start the Notes client on the machine and set it up for the AM Privileged User. You will need to select the ID file and enter the password you set for the user.

Once you have signed into the client you can exit it again. The user ID that last accessed the client is stored in the notes.ini file so when AM accesses the client it will now get the right user.

Note: Only one Notes user can be active on a machine at any time. Since Access Manager will be using the client as the AM Privileged User there can be no other use of the Notes client on the machine.



Once the Notes Client has been initialised then Access Manager can be configured. Use the PDCONFIG GUI as normal.

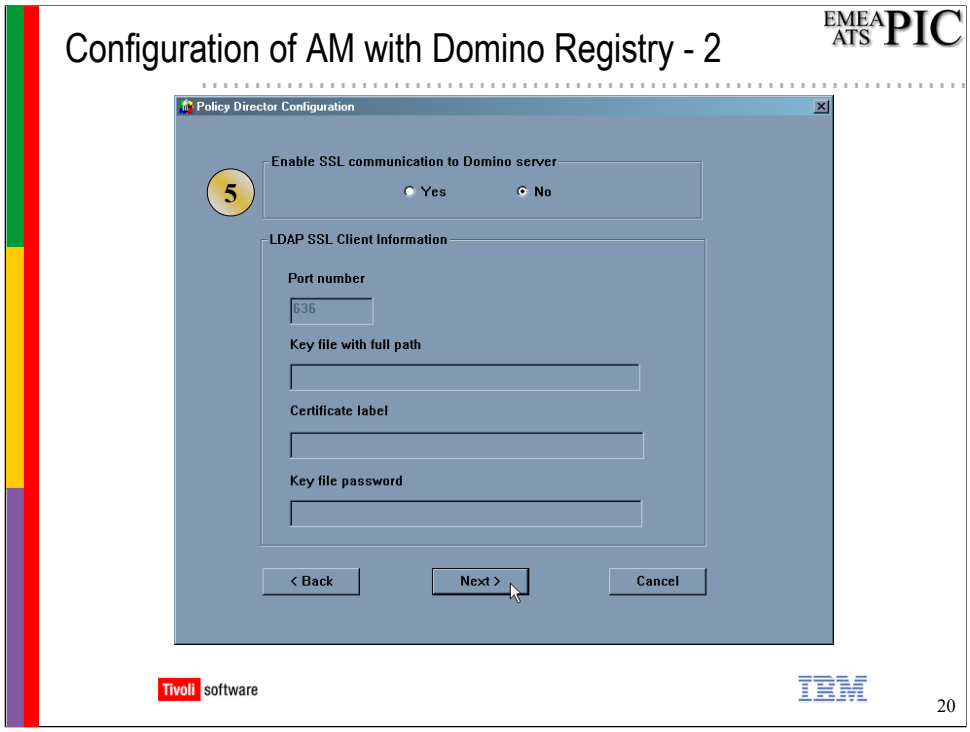
When configuring AMRTE the panels shown above are displayed.

-1- Select Domino as the User Registry

-2- Give the fully qualified Domino server name. This includes the name of the server and the Notes domain.

-3- Give the full DNS name of the Domino server.

-4- Give the port number that the Domino server TCP LDAP interface is listening on. This must match what was configured on the Domino server. This will be 389 if the default is used. In the example shown above the port was moved to 8389.

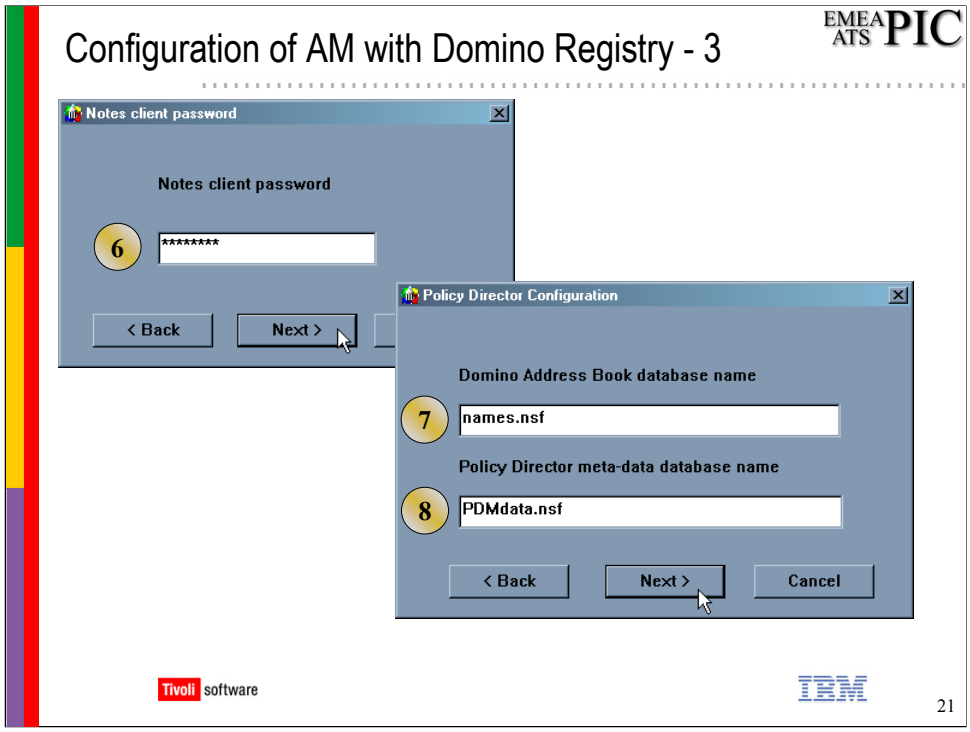


-5- Specify if SSL should be used for communication with the Domino LDAP interface. In the example above SSL has not been enabled.

If SSL is to be used to communicate with the LDAP server then the KDB file for the LDAP client must be specified. This file should contain the public certificate of the Certificate Authority that signed the LDAP servers certificate and also (optionally) a client certificate – with private key – for AM to use to identify itself to the LDAP server.

If a client certificate is going to be used then its label should be specified.

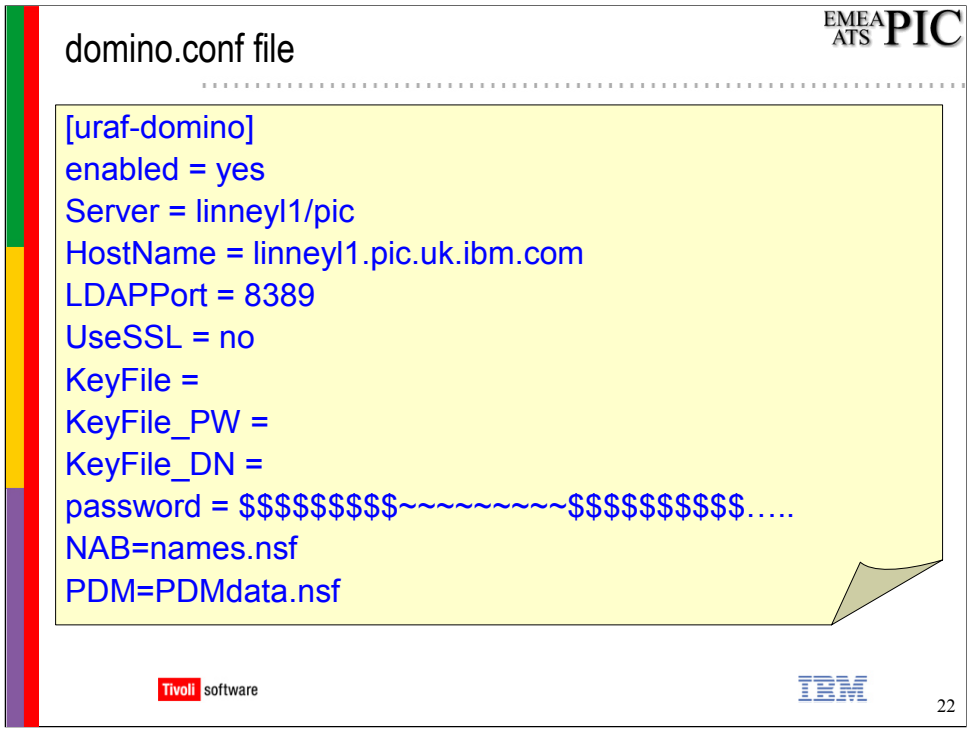
The password for access to the KDB file must also be given.



-6- Give the password of the AM Privileged User. This will be used by Access Manager to log into the Notes client in order to communicate with the Domino Server. This password is the one given when creating the AM Privileged user

-7- Specify the filename of the Domain Address book on the Domino Server. By default this will be names.nsf (and is pre-filled with that value). This filename is relative to the server Data directory.

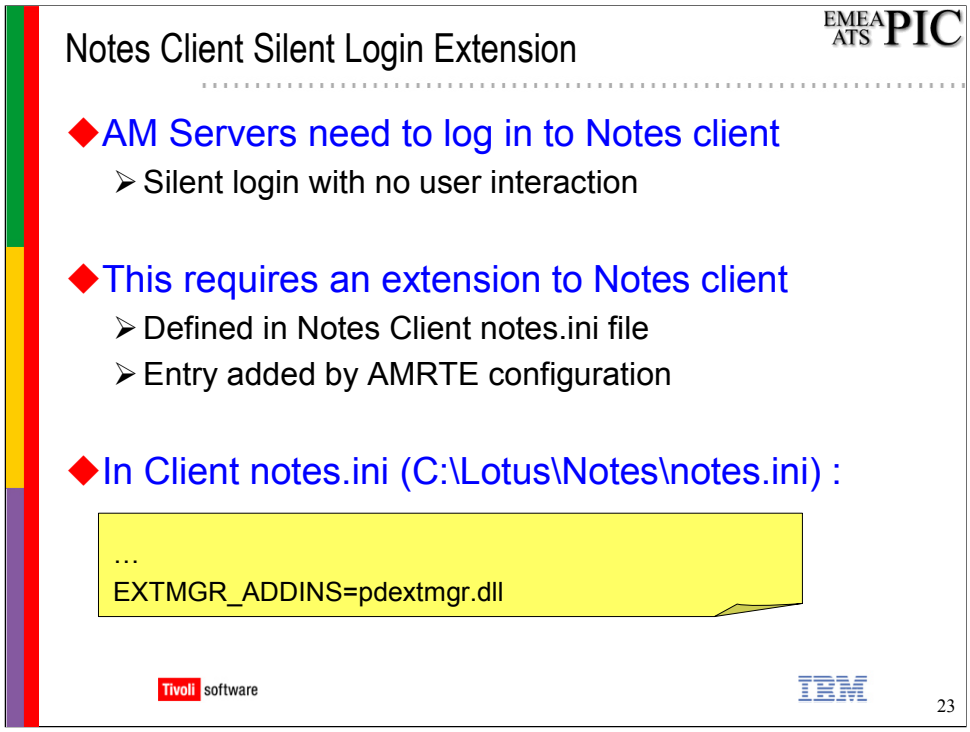
-8- Specify the filename of the AM Meta-data database on the domino server. By default this is PDMdata.nsf (and is pre-filled with that value). This filename is relative to the server Data directory. This filename will be used to create the AM Meta-data database when PDMgr is configured – on subsequent AM machines it is used to locate it.



The configuration of AMRTE performs two operations.

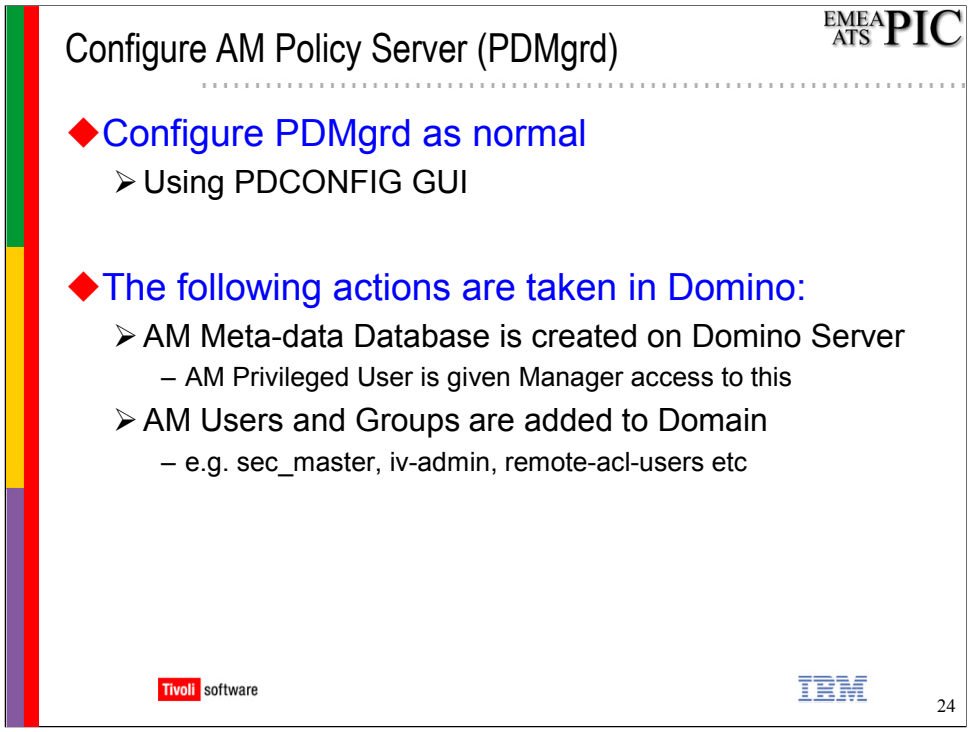
The first is to populate the domino.conf file (found in the Access Manager etc directory) with the configuration information entered by the administrator.

All of the information is visible in this file with the exception of the Notes client password which is obfuscated so that it cannot be read.



The second operation of AMRTE configuration is to modify the notes.ini file of the local Notes Client.

The line shown above is added and this allows Access Manager to silently log into the Notes client using the password stored in the domino.conf file.

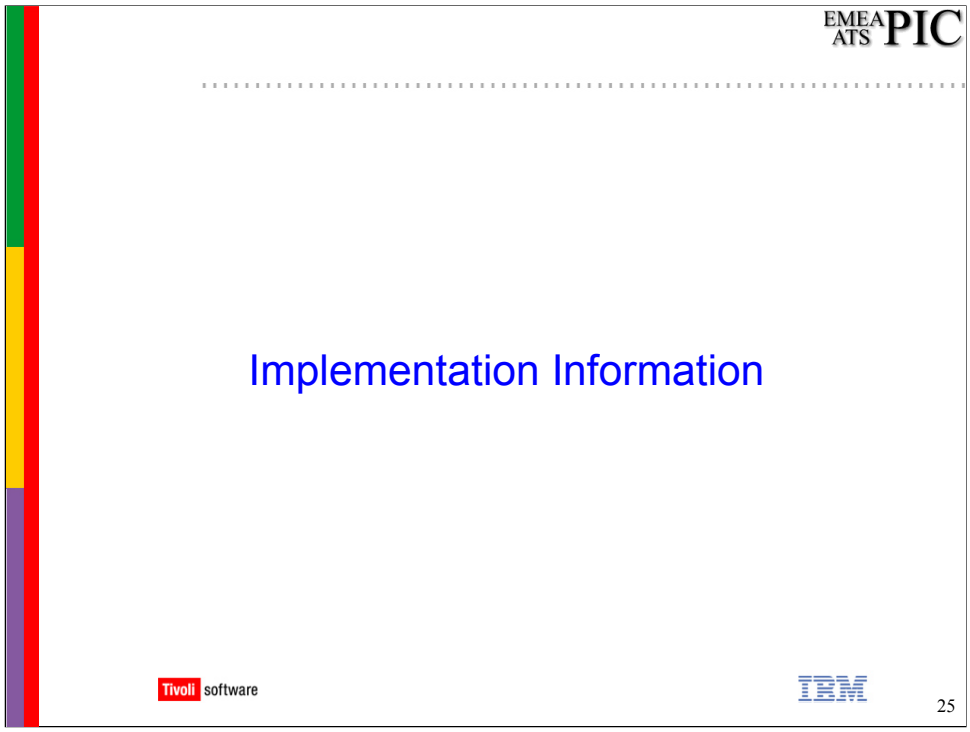


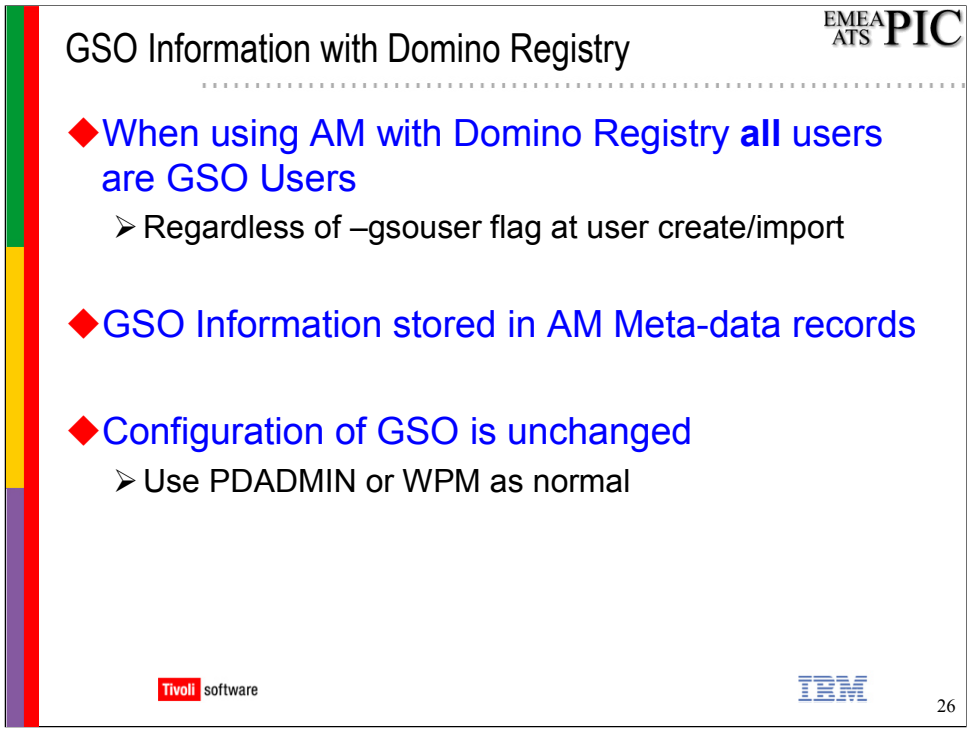
Once AMRTE has been configured PDMgrd can be configured.

PDMgrd configuration with a Domino registry is externally no different than when using LDAP. Under the covers it is significantly different.

PDCONFIG logs into the domino server through the local notes client using the password that was given during AMRTE configuration. It then performs the actions shown above.

Note: If configuration of PDMgrd fails then check the config.log file for details. It is well worth unconfiguring AMRTE and starting again because any typing mistakes made during AMRTE configuration will only show up when PDMGRD is configured.

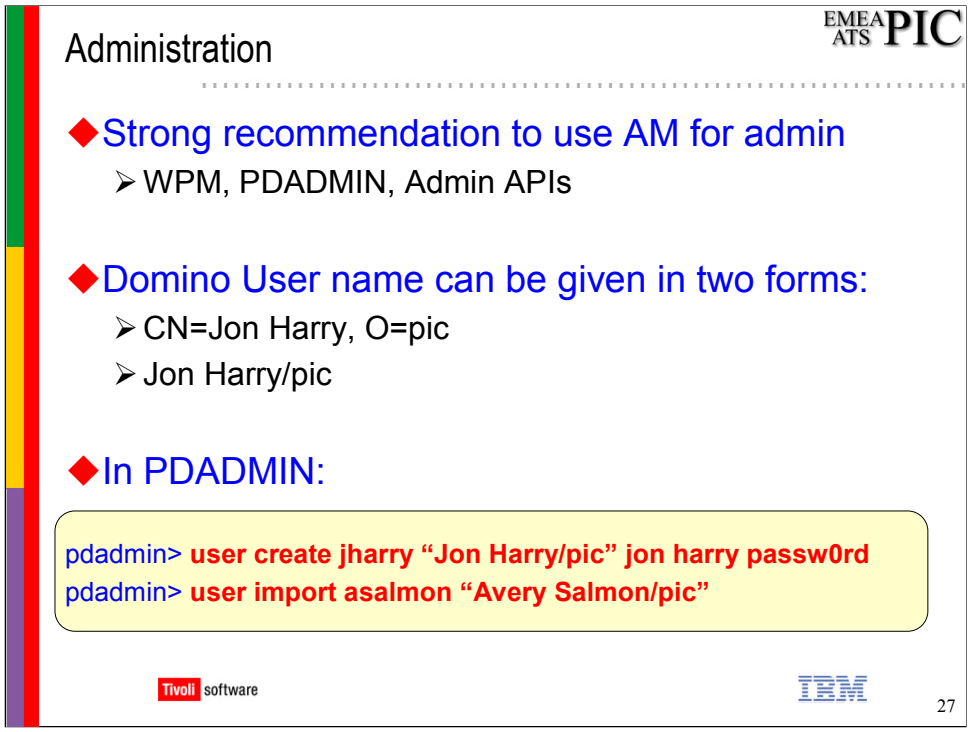

EMEA ATS PIC
Implementation Information
Tivoli software
IBM
25



When using AM with a Domino Registry there is no distinction made between GSO users and non-GSO users. Every user created will be a "GSO user" regardless of whether the *gsouser* flag is given.

Apart from the above, there are no changes to the configuration of GSO as a result of using a Domino registry.

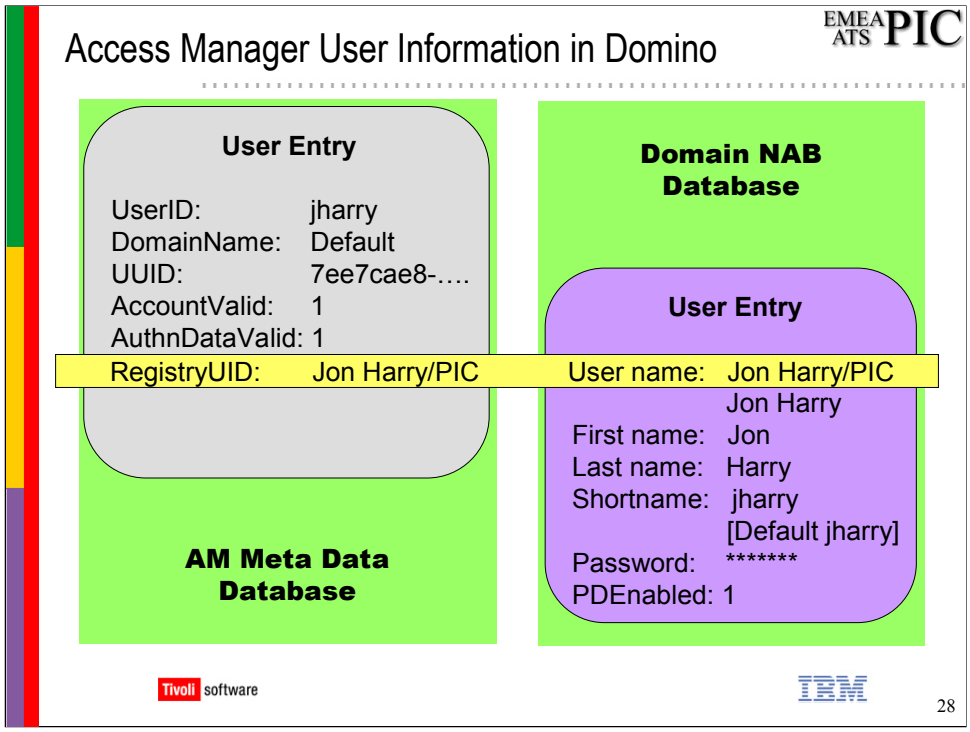
GSO information (ie GSO targets, GSO groups and UserID/passwords) is stored in the AM Meta-data database.



When AM is configured into the Domino registry it is strongly recommended that Access Manager tools be used to create and modify users that will be used with Access Manager. This ensures that the AM information about the user remains synchronised.

Domino can recognise a user in its registry using two forms of the User name. The first is the native Notes format (which is User name qualified with the Domino domain) and the second is the pseudo-Distinguished Name of the user which is CN=<*user name*>,O=<*domino domain*>.

In PDADMIN, the WPM and the Admin APIs either form can be used when a group or user DN is required. In places where DN syntax is checked the pseudo-DN can always be used.

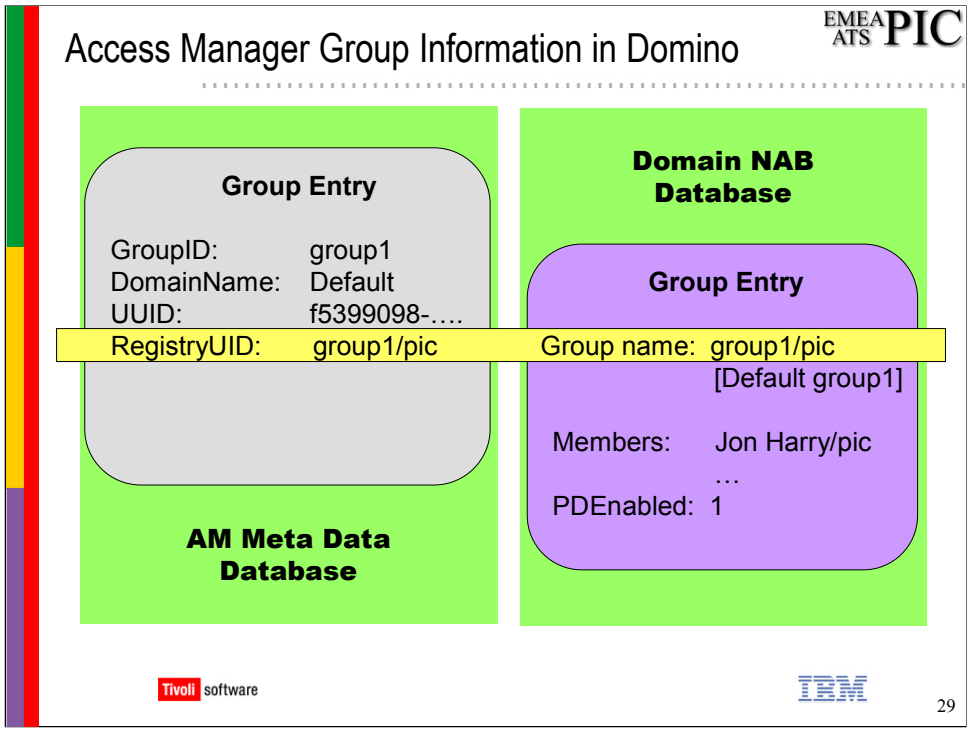


The diagram above shows how user information is stored when using a Domino registry.

Information that AM shares with Notes (shown above) is stored in the Domain NAB database. The shortname and internet password fields are used for AM userID/password authentication through the LDAP interface. Notice the special formatting of the second shortname entry – this is discussed later.

The PDEnabled flag indicates that the user is known to Access Manager. It is not visible in the NAB by default but, if required, the design of the domain NAB can be altered so that it can be seen.

If a user defined in the domain NAB is known to AM then there will be an entry for the user in the AM Meta-data Database. This is linked to the users NAB entry by the User name (as shown above). The Meta-data Database stores AM specific information such as accountValid flag, password valid flag (AuthnDataValid) and a UUID mapping. (which identifies the user in the AM ACL database).

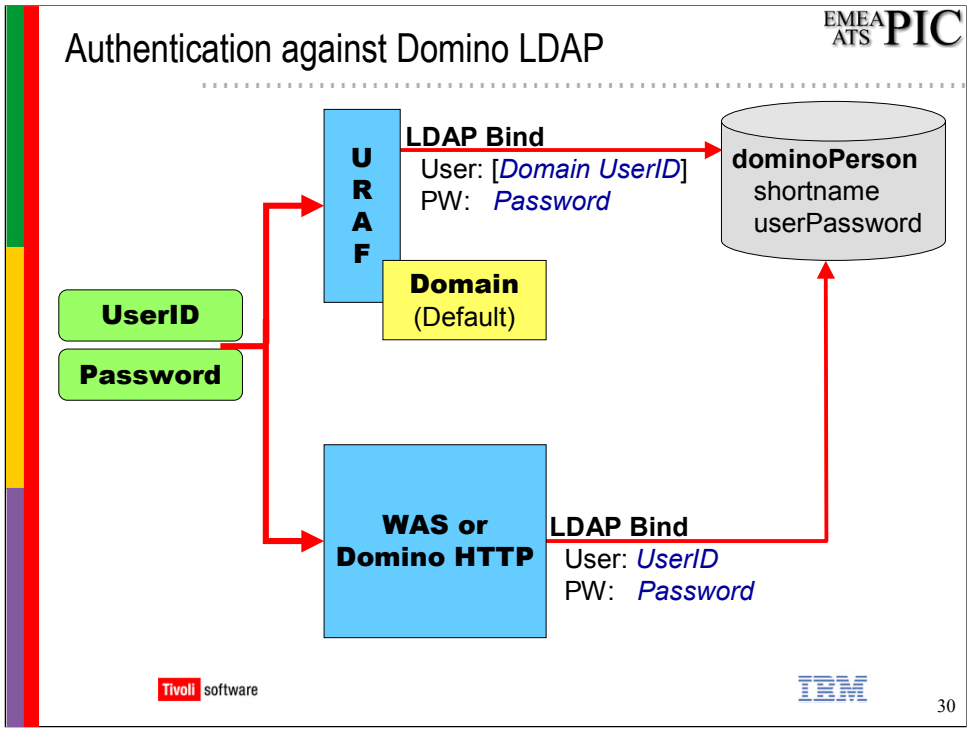


The diagram above shows how group information is stored when using a Domino registry.

Information that AM shares with Notes (shown above) is stored in the Domain NAB database.

The PDEnabled flag indicates that the group is known to Access Manager. It is not visible in the NAB by default but, if required, the design of the domain NAB can be altered so that it can be seen.

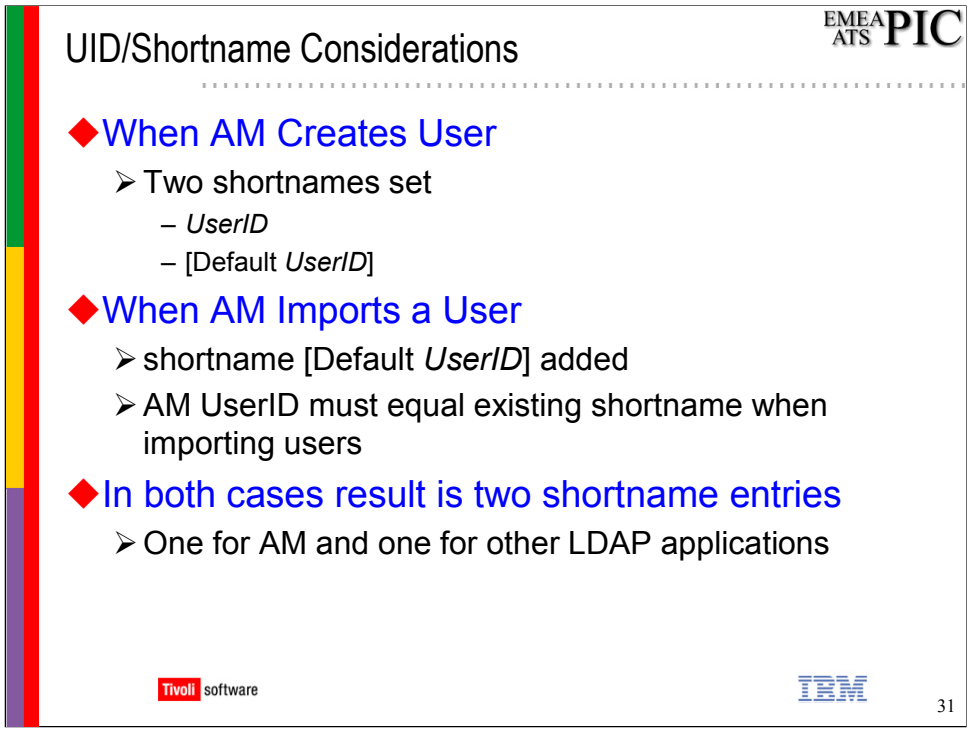
If a group defined in the domain NAB is known to AM then there will be an entry for the group in the AM Meta-data Database. This is linked to the group's NAB entry by the Group name (as shown above). The Meta-data Database stores the UUID of the group which identifies it in the AM ACL database.



The diagram above shows how AM user authentication differs from that of other applications.

AM has always left open the option of having multiple *secure domains* configured against single registry - although currently only a single domain (called Default) is supported. When a user is authenticated (against the LDAP interface of the domino server) AM needs to be able to ensure they are in the correct domain so it takes the UserID provided by the user and formats it to include the domain name (as shown above). This is why the *shortname* of a AM user includes an entry that has Default in it.

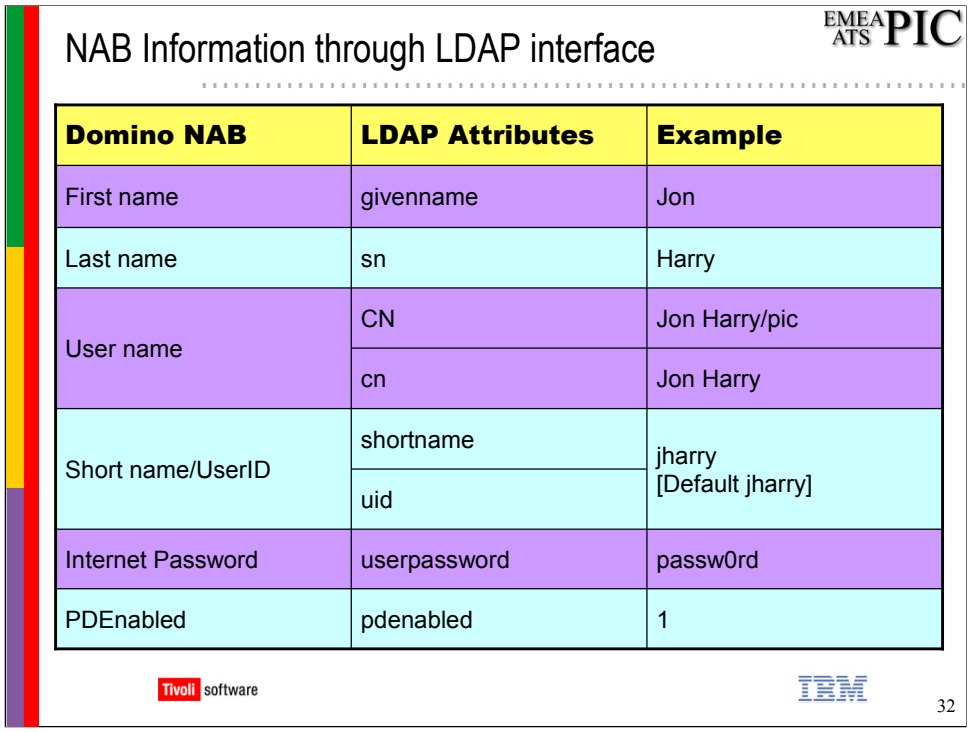
Since other applications may be sharing the user entry with AM the shortname also includes a “normal” version of the users shortname. This should match the users AM UserID so that the user has the same UserID across the systems.



When AM creates a user it adds two shortnames to Domino. One is the standard shortname, the users UserID, and the other is one of the format [Default UserID] that is used by AM when authenticating users.

When AM imports a user from the registry it checks that the AM UserID matches the users existing shortname. An error is returned if this is not the case. AM then adds the [Default UserID] shortname to the user.

In either case the result is that every user in the Domino directory that is defined to Access Manager has two shortnames.



The chart above shows how user information in the Domino domain address book is represented through the LDAP interface.

When AM needs to authenticate a user it attempts a BIND to LDAP. The LDAP server checks this against the shortname (or uid – they're both the same) and the userpassword.

The shortname and uid both come from the Shortname/UserID field of the NAB. This field can have multiple entries and the BIND will be successful as long as one of the entries matches what is in the BIND and the password is correct.

The userPassword comes from the users Internet Password in the NAB.

Note: If an ldapsearch is performed against the Domino LDAP then only one shortname entry will be shown in the output. However, all values can be searched.