documentum

Frequently Asked Questions for User Authentication

Documentum Support Services

January 2003

1. What are my options for setting up user authentication with Documentum?

a.) Default user authentication on UNIX - By default, the Content Server on UNIX uses the dm_check_password program to authenticate users. The installation procedure automatically creates a location object called user_validation_location and set the server config object attribute called validate_user to the name of the location object. By default, the user_validation_location points to the default dm_check_password program that comes with Documentum. In this authentication mode users must have an OS account.

b.) Default user authentication on Windows - By default, the Content Server on Windows uses an internal process for authenticating users against the OS and does not use the dm_check_password program. By default the validate_user attribute in the server config is blank. In this authentication mode users must have an OS account. (Refer to the Security chapter in the Server Admin Guide on Windows for more information on domain authentication on Windows.)

c.) Authentication using a custom dm_check_password program - If you've customized the dm_check_password program, Documentum can be set up to authenticate using it by creating a location object that points to the location of your custom dm_check_password & setting the validate_user attribute in the server config object to the name of that location object. ***NOTE:*** *Assistance with writing a custom dm_check_password program is provided by Developer Support and is not part of the Standard Support offering.*

d.) Lightweight Directory Access Protocol (LDAP) authentication - Docbase users can be set up to authenticate against an LDAP Server. In this authentication mode users must have LDAP account. (Refer to the chapter on "Using an LDAP Directory Server" in the Server Admin. Guide for more details.)

e.) Windows Unified Login - This is available for Windows Docbases only.
The Unified Log-in capability enables a user to login to a Docbase using DeskTop client without supplying a username and password. The "Unified Login" feature will work only if the domain that your username is validated in is the same as the default "user_auth_target" specified in the Docbase "server.ini" file.

To setup Unified Login set the a_silent_login attribute of the server config object to TRUE then run the following steps on the DeskTop client machine:

- Initialize the Desktop Client by selecting the Documentum icon in the Desktop Client Explorer interface.

- Find the Docbase name in the navigation pane of the Explorer. Highlight the Docbase and right click on the object.

- Select Connect As. The Connect to Docbase dialog appears with the "Use Windows Login" checkbox.

- Check the option, "Use Windows Login".

Once this is complete, each time you login to that specific Docbase, Documentum will use your Windows NT login and password.

2. Does Documentum support Microsoft Active Directory for user authentication?

Active Directory can be used as a "regular" Windows domain controller or as an LDAP Server.

Active Directory as a regular domain - This type of domain authentication configuration is described in the Security chapter of the Server Admin Guide for Windows under "User authentication". This mode of authentication doesn't require configuring LDAP Config object. This is supported for Servers 4.2 & 5.1 on Windows only.

Active Directory as an LDAP Server - LDAP authentication against Active Directory (uses LDAP config object). Server 5.1 on UNIX & Windows is supported when using Active Directory as an LDAP Server. On UNIX, Active Directory supports synchronization operations importing new users and groups into the Docbase, but rename and inactive synchronization operations are not supported*. **NOTE:** The fix for bug 36801 provides support for 4.2 to work with Active Directory as an LDAP server. Check the latest patch release notes for your platform to see if this bug fix is included in a 4.2 patch.*

3. Does Documentum support Kerberos for user authentication?

No, Documentum does not currently support Kerberos.

4. Can I use a Windows domain to authenticate my users who are in a UNIX Docbase?

Yes starting in Server 4.2 Documentum supports authenticating users in UNIX Docbase against a Windows domain. This can be achieved by rebuilding the dm_check_password program. Please see the Server Installation Guide for details on how to set this up or refer to Support Note 16592.

5. How do users change their passwords?

End Users- There are several options available that end users can use to change their Documentum password. Some Documentum Client products provide the ability for users to change their passwords (including DeskTop Client, WebTop and WebPublisher). Refer to the specific client product documentation to see if that client supports changing passwords. Also the changepassword API can be used or the dm_change_password utility can be run on the Content Server machine to change passwords. ***NOTE:*** *Passwords cannot be changed through Documentum when authenticating against LDAP or when using UNIX-Windows domain authentication. If using LDAP, the passwords must be changed in the Directory Server. If using UNIX-Windows domain authentication the passwords must be changed at the OS level.*

Docbase owner- Once the password has been changed in the Database (refer to your Database vendor for instructions on changing passwords in the Database), the $DOCUMENTUM/dba/config/<docbase_name>/dbpasswd.txt file needs to updated with the new password.

Installation owner- The password for the Installation owner account can be changed using any of the methods described above for End Users. In addition, on Windows the password needs to be changed for the Docbase service in Control Panel -> Services. Also the DocBroker can be configured to require a password for shutdown. If you are using this option, the password in the docbroker.ini feels needs to be changed as well.

NOTE: *If the password for the user that runs Object Replication, DistOperations, Federation, and/or Content Replication jobs changes, the password needs to be updated in the appropriate places for each job. (See below for details)*

Object Replication jobs – Passwords can be changed in the properties of the replication job using Documentum Administrator (DA).

Distributed Operations job – Passwords need to changed by manually editing the $Documentum/dba/config/<docbase name>/dm_operator.cnt and $Documentum/dba/config/<docbase name>/<remote_docbase_name>.cnt files.

Federation job – Passwords can be changed using DA under Federation Management.

Content Replication job – The passwords are stored inside the arguments of the Content Replication job and can be updated manually using DA in the properties of the Content Replication job for each site. Those same passwords are stored in the $DOCUMENTUM/dba/config/<Docbase name> SurrGet.txt file in order for the SurrogateGet method to run & must be updated manually on each site's Server machine.

6. How do I "undo" LDAP authentication?

To stop using LDAP authentication, set the user_source attribute in dm_user for the users that are authenticating against LDAP to blank.

7. **Why don't I need a password to connect to the Docbase if I'm connecting from the Content Server machine as the installation owner?**

If you're connecting to the Docbase from the Content Server machine & connecting as the Documentum installation owner you aren't required to enter a password. This is referred to as Documentum's "trusted login" capability, since the Server trusts that you know the password since you had to enter the password to login to the machine.

8. Why is the user authentication using the standard dm_check_password program producing different results than when connecting to the OS directly?

When dm_check_password produces different results than connecting to the OS directly, this is almost always due to a bug in the dm_check_password program. (For example, if dm_check_password is saying that the account is disabled, but the same user can login directly to the OS, this would be a bug with dm_check_password.) If you are experiencing problems with dm_check_password returning different results than the OS, refer to the latest patch release notes for your Content Server release to see if any bugs have been fixed that match the behavior that you're seeing.

9. What special characters aren't allowed in a password?

Commas aren't allowed in a password. Other special characters that can't be used in a password are currently under investigation by Documentum engineering.