Recipe: Administration Process Gotchas and Hints, part 3

by Kendra Bowker

*[Editor's note: This article resides in "Notes Today", the technical Webzine located on the http://www.notes.net Web site produced by Iris Associates, the developers of Domino/Notes. This is the third article in a series of three on how to use the Domino Administration process. This third article provides tips and guidelines to help you use the Administration Process in Release 4.5 to its full advantage. Be sure to see the Lotus Notes Administrator's Guide for more information on the Administration Process in general and on each task the Administration Process can carry out. The **first article** focused on how to set up the Administration process in your domain. The **second article** provided a roadmap of common Administration process requests and described how Domino goes about completing some of its more extensive series of requests.]*

Introduction

The Administration Process is a valuable server administration tool that automates many routine administration tasks. You simply choose an action and the Administration Process takes charge of completing it. The Administration Process automates renaming people and servers, recertifying IDs, deleting references to people, servers, and groups, and moving and replicating databases--to name just a few of the tasks!

Getting started

Here's some information to help you get off to a good start with the Administration Process.

The Administration Process requires a hierarchical environment. The Administration Process is intended to be used in a hierarchical environment. The only tasks it can carry out in a flat environment is copying a server's public key to its Server document and copying a server's build number to the Server document.

The administration server for the Public Address Book must be able to populate wildcard replicas of the Administration Requests database.
A fully initialized Administration Requests database (ADMIN4.NSF) is only created on the administration server for the Public Address Book. For all other servers, if the Administration Requests database does not exist, a wildcard replica of it is created during server startup. A wildcard replica is essentially a database shell that is populated with documents through replication with another server. For these wildcard replicas of the Administration Requests database to be populated, you must give the administration server for the Public Address Book "Create replica databases" access to each server in the domain that has a wildcard replica.

You must have the correct level of access to databases the Administration Process uses.
You need the following access to the databases used by the Administration Process:

1. Administration Requests database--you should have at least Editor access--this allows you to approve requests and to perform requests again if errors occur.
2. Public Address Book--you should have Author access with the appropriate administration role or Editor access.
3. Certification Log-- you should have at least Author with "Create documents" access for renaming and recertification tasks.

Moving and creating replicas of databases have additional access requirements--see "Moving and creating replicas of databases" later in this article. For more information on the access requirements for each task, see Chapter 3 of the *Administrator's Guide*.

The Administration Process can only change or delete names in databases that are assigned administration servers.

You must assign a database an administration server in order for the Administration Process to update names in the database. You have to do this before you choose a rename or delete action.

There are several factors that affect how long a task takes to complete.
Completing a particular task often involves several requests carried out by various servers, and therefore, the task may not be completed immediately. For example, the following table shows where and when requests associated with changing a person's common name are posted and processed:

Table 1: Factors affecting time to complete task

Request	What it does	Where/when it's posted	Where/when it's processed
Initiate Rename in Address Book	Adds the new name and certificate and the change request to the Person document.	Immediately posted on the server where you choose the rename action	Processed on the administration server for the Public Address Book within 60 minutes (by default) after the server receives the request
Rename Person in Address Book	Changes the name in the Public Address Book except in Person documents	Posted on the first server the person accesses that the has the completed change request field in the Person document	Processed on the administration server for the Public Address Book within 60 minutes (by default) after the server receives the request
Rename in Person Documents	Changes the name in Person documents	Posted on the administration server for the Public Address Book after completion of the Rename Person in Address Book request	Processed at 12:00 A.M. (by default) on the administration server for the Public Address Book
Rename in Access Control List	Changes the name in database ACLs	Posted on the administration server for the Public Address Book after completion of the Rename Person in Address Book request	Processed on each server in the domain within 60 minutes (by default) after replicating to each server
Rename in Reader/Author Fields	Changes the name in database Reader and Author fields	Posted on the administration server for the Public Address Book after completion of the Rename in Person Documents request	Processed on each server in the domain Sunday at 12 A.M. (by default) after replicating to each server

As you can see there are several factors that affect how quickly the name change occurs throughout a domain:

- **When a person accepts the new name**. Once the change request is added to the Person document, the person is prompted to accept or reject the name change when he or she next authenticates with any of the servers in the domain. The person must accept the new name to trigger renaming throughout the domain. If the person is on vacation, this delays the renaming process.
- **Administration Process schedules**. The Administration Process on any server processes a request according to the schedule for that type of request. For example, by default servers update names in ACLs fairly quickly but update names in database Reader and Author fields only once a week**.** You can adjust these schedules by modifying the fields in the Administration Process section of the Server document. You can also override these schedules and process a specific group of requests immediately using the **tell adminp process** server command. For example, you can type **tell adminp process all** to process all outstanding requests on a server. Keep in mind that the processing of some of these requests can take some time, and so you might want to initiate an action and force the

request processing off-hours. For details on scheduling the Administration Process and on using the **tell adminp process** command, see Chapter 3 of the *Administrator's Guide.*

- **How frequently the Administration Requests database and Public Address Book replicate**. It's important that the Administration Requests database replicates frequently as some requests are posted on one server but carried out on another and the more quickly the request replicates the more quickly it can be processed. Also changes to the Public Address Book should replicate frequently too. Consider creating separate Connection documents to schedule frequent replication just of the Administration Requests database and the Public Address Book.

Using correct certifiers and public keys

The Administration Process makes renaming and recertifying Notes IDs easy. In the Public Address Book you just select the Server or Person documents associated with the IDs, choose a rename or recertify action, and the Administration Process takes care of the rest. You should understand the following about certifiers and public keys, since both are involved with recertification and renaming IDs.

You must select a valid certifier when you rename or recertify.
The following table indicates what is a valid certifier for each renaming and recertifications task.

Table 2: Valid certifiers for renaming and recertification task

Action	Acceptable certifier	Example
Rename Person - Change Common Name	Select the original hierarchical certifier	To change the name Alice Oakley/Newark/Acme to Alice Jacobs/Newark/Acme, use the certifier ID for/Newark/Acme.
Rename Person - Request Move to New Certifier (Step 1 of moving a person in hierarchy)	Select the original hierarchical certifier (or an ancestor of it) and also specify a hierarchical certifier as the target.	To submit a request to change the name Alice Oakley/Newark/Acme to Alice Oakley/Boston/Acme, select the certifier id for /Newark/Acme or /Acme as the original certifier and specify/Boston/Acme as the target certifier.
Complete Move for selected entries (Step 2 of moving a person in hierarchy)	Select the target hierarchical certifier specified in the original move request	To complete changing the name Alice Oakley/Newark/Acme to Alice Oakley/Boston/Acme, select the certifier ID for /Boston/Acme as the target certifier.
Rename Person - Upgrade to Hierarchical	Select any hierarchical certifier	To change the flat name Alice Oakley to the hierarchical name Alice Oakley/Newark/Acme, use the certifier ID for /Newark/Acme
Upgrade Server to Hierarchical	Select any hierarchical certifier	To change the flat name Newarkserv to the hierarchical name Newarkserv/Newark/Acme, use the certifier ID for /Newark/Acme.
Recertify Person	Select the original hierarchical certifier	To recertify Alice Oakley/Newark/Acme, use the certifier ID for /Newark/Acme.
Recertify Server	Select the original hierarchical certifier	To recertify Newarkserv/Newark/Acme, use the certifier ID for /Newark/Acme.

What happens when you select an invalid certifier.
The results of selecting an invalid certifier vary depending on the type of action you choose.

- **Upgrading a person or server to hierarchical or changing a person's common name:** You can't submit the request until you select a valid certifier ID.
- **Moving a person's name in a hierarchy:** If you don't specify the original certifier ID when you choose Actions - Request Move to New Certifier, you can submit the request but it isn't posted in the Administration Requests database and the Certification Log logs the error "The selected certifier is not an ancestor of the entity to be updated." To correct this, you'll need to choose "Request Move to New Certifier again," making sure to select the original certifier ID.

If you specify an invalid target certifier ID when you choose Action - Complete move for selected entries, the request is posted in the Administration Requests database with the error "The selected certifier is not the target certifier in the move request." The Certification Log also posts this error. If the target certifier ID you specified when completing the move is wrong, select the name entry in the Name Move Requests view of the Administration Requests database and choose the "Actions - Complete move for selected entries" again, specifying the correct target certifier ID. If you specified the wrong target certifier ID when you originally chose "Actions - Request Move to New Certifier, repeat that action again instead.

- **Recertifying a person or server:** If you don't select the original certifier ID, you can submit the request but it isn't posted in the Administration Requests database and the Certification Log logs the error "The certificate contained in the note was not issued by the selected certifier." To correct this, you'll need to choose the recertification action again, making sure to select the original certifier ID.

When you rename or recertify, the Public Address Book must contain the appropriate Certifier documents.
Any certifier you use for renaming or recertification, and any ancestor of the certifier, must have a Certifier document in the Certificates view of the Public Address Book. For example, if you're using the certifier /Newark/Acme to recertify a server, the Public Address Book must contain Certifier documents for /Acme and /Newark/Acme. One of the reasons a Certifier document might not be in the Public Address Book is if you registered the certifier in Release 3.

If a Certifier document for a certifier you specify isn't in the Public Address Book, the Administration Process posts the following error in the Administration Requests database when it attempts to carry out an "Initiate Rename in Address Book," "Recertify Server in Address Book," or "Recertify Person in Address Book" request:" "A required certifier was not found in the Address Book." To correct this:

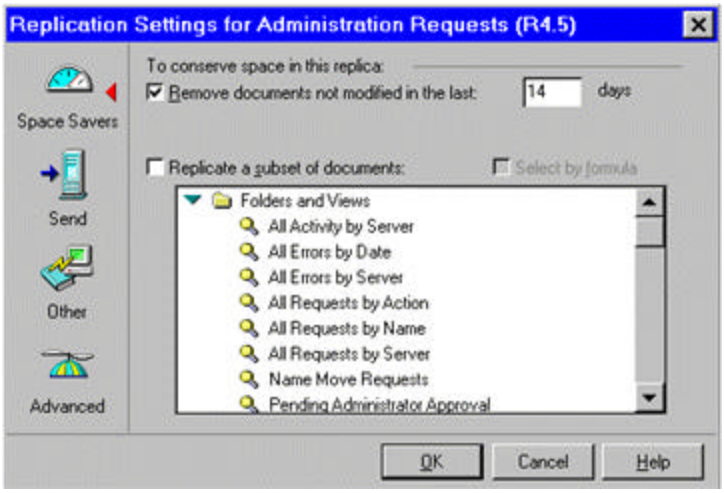
1. Create the necessary Certifier document(s) in the Public Address Book.
2. For each Certifier document you create, copy the certified public key from the certifier ID to the document:
   - Choose File - Tools - Server Administration then Administration - ID File.
   - Select the certifier ID.
   - Click More Options then Copy Public Key.
   - Paste the public key into the Certified public key field of the corresponding Certifier document.
3. At the server console enter the command load updall names.nsf -t $certifiers.
4. Select "Perform request again" in the response document for the request.

When you rename or recertify, the public key on an ID must match the one in the Public Address Book.
For recertification or renaming to work, the public key in the Person or Server document must match the one on the user or server ID. If a public key has been changed or corrupted in some way, you'll see this error in the Administration Requests database: "The name to act on was not found in the Address Book." If this happens, replace the public key in the Public Address Book with the key from the ID, rebuild the $Users or $Servers view, and select "Perform request again" in the response document in the Administration Requests database. For details on doing this, see the end of Chapter 14 in the *Administrator's Guide*.

Updating names in Reader and Author fields

Beginning in R4.5, when you delete or rename a person or server, the Administration Process can also update the name in the Reader and Author fields of documents in a database--it will do this as long you've assigned an administration server to the database and have selected the advanced ACL option "Modify Reader and Author fields."

The timing of automatic deletion of documents from the Administration Requests database may prevent Reader and Author fields from being updated.
To keep the size of the Administration Requests database to a minimum, unmodified documents are deleted from it by default every seven days--the replication setting "Remove documents not modified in the last 7 days" controls this. "Rename in Reader/Author Fields" and "Delete in Reader/Author Fields" requests are processed according to the "Delayed" settings in the Administration Process section of the Server document--by default each Sunday at 12:00 AM. If a server is down Sunday at 12:00, the outstanding requests will be deleted before the next opportunity to process them (next Sunday.) To prevent this from happening, you can either schedule delayed requests more frequently or extend the number of days unmodified documents remain in the Administration Requests database. For example, to allow unmodified documents to remain in the Administration Requests database for 14 days, select the Administration Requests database, choose File - Replication - Settings, then specify "Remove documents not modified in the last 14 days:"



Documents with updated Reader and Author fields are marked as unread.
After the Administration Process updates these fields in a database, Notes always marks the documents that contain them as unread, regardless if a particular person has read them or not.

Recertifying IDs

The Administration Process makes recertifying IDs easy. You choose Actions - Recertify Person or Actions - Recertify Server and the Administration Process takes care of recertifying the ID. The Administration Process posts the new certificate in the Person or Server document in the Public Address Book. When a client detects the new certificate during authentication the new certificate is automatically copied to the ID file--so the recertification occurs without any involvement on the part of the ID owner.

The Administration process lets you be proactive about recertification--you can recertify a group of IDs due to expire at the same time--this way people don't have to remember to notify you when their IDs are about to expire.

Use only the original certifier.
When you choose the Recertify Server or Recertify Person actions you have to recertify using the original certifier--you can't use these actions to move the person or server to a different part of a name hierarchy.

People should make backups of recertified IDs.
Once an ID is recertified, backup copies of the original ID become obsolete after the certificate expires on them. So be sure to tell people to make new backup copies of recertified IDs.

Renaming people and upgrading servers to hierarchical

The Administration Process makes changing a name in your organization easy--once you initiate a rename action, it takes care of updating that name throughout the databases in a domain.

The only way you can change a server name using the Administration Process is to upgrade it to hierarchical.

You can use the Administration Process to change a person's common name, move the person's name to a different branch of the name hierarchy or to a different hierarchy, and convert the name from flat to hierarchical. However, the only way you can change a server name using the Administration Process is to change it from flat to hierarchical--you must do any other server name change manually.

You can't change a common name at the same time you change the name in another way.

When you convert a person's or server's name from flat to hierarchical, you can't change the common name at the same time. For example, you can't convert the flat name Alice Oakley to the hierarchical name Alice Jacobs/Acme. You also can't change a hierarchical person's common name when you move the name to a different hierarchy--you have to change the common name before or after the "move."

A person or server has to accept a new name while the change request still exists in the Person or Server document.

Choosing a rename action causes the Administration Process to create a request called "Initiate Rename in Address Book." When this request is carried out (according to the Interval setting for the Administration Process) the Administration Process makes an entry in the Change request field in the Person or Server document and also adds the new name and certificate to the document. (In Person documents, the word "Pending" appears in the Change request field; in Server documents, an encoded change request appears in the field.)

Once the Change request field is filled in, the Administration Process waits for the person or server to accept the new name. Renaming doesn't begin to occur throughout the domain until the name is accepted.

A person or server can only accept a new name while the change request remains posted in the Change request field. The change request remains for 21 days by default. (You can use the NOTES.INI setting Name_Change_Expiration_Days to change this expiration period.) So if you find a person's new name appears only in the Person document and nowhere else, this can indicate that the change request expired before the person authenticated with a server and accepted the new name. If this happens, replace the new name in the "User name" field in the Person document with the original name and then choose "Actions - Rename Person" again. (Although this problem can also occur with servers, it's less likely to occur).

The change request remains even after a person or server accepts a new name.

A change request remains in the Change request field even after a person or server accepts a new name. So, if a person accepts a new name within 2 days, "Pending" still remains in the Person document by default for another 19 days. This extra period of time serves two purposes: 1) it gives a person with additional IDs the opportunity to change the name on them too and 2) it lets people continue to access databases whose ACLs haven't yet been updated with the new name.

"New Qualifying Org. Unit" doesn't mean an existing organizational unit certifier.

When you rename a person or server, the rename dialog box displays the field "New Qualifying Org. Unit." The purpose of this field is to let you add an extra component to a specific name, for example, to distinguish one person from another with the same name in the same branch of the name hierarchy. Don't enter an existing organizational unit certifier name here. If you do, the new name will include the organizational unit certifier name twice. For example, if you're renaming Alice Oakley/Newark/Acme to Alice Jacobs/Newark/Acme and you specify Newark in the "New Qualifying Org. Unit" field, her new name actually becomes Alice Jacobs/Newark/Newark/Acme.

A person's original name remains in the Person document.
When the Administration Process changes a person's name, it keeps the original name along with the new one in the User name field so the person can continue to receive mail addressed to the original name.

A person shouldn't accept a new name using the administration client on a server.
If you start an administration client before the server and then accept a new name while at the client, the name is immediately updated in access control lists on the server rather than waiting for the "Rename in Access Control List" to be processed.

There are some occurrences of names that the Administration Process doesn't change.
The Administration Process doesn't update the name of an ID file, the name and title of a mail file, or a short name in a Person document.

If you move a person to another organization, the Public Address Book must contain the appropriate cross-certificates.
Before you move a person to another organization, make sure that each organization has cross-certified the other and that both cross certificates are in the Public Address Book. For example, to change the name Alice Oakley/Newark/Acme to Alice Oakley/Anotherorg, the Public Address Book must contain the following cross-certificates:

- A cross certificate from /Anotherorg issued to /Newark/Acme or /Acme
- A cross certificate from /Newark/Acme or /Acme issued to /Anotherorg

Remember that the Administration Process only operates within one domain, so both cross-certificates must be in the same Public Address Book.

When you attempt to move a person's name to another organization without the required cross certificates in the Public Address Book, processing of the "Initiate Rename in Address Book" request generates the following error as a response in the Administration Requests database: "The Address Book does not contain a cross certificate capable of validating the public key." To correct this:

1. Issue a cross certificate from organization A to B, if one doesn't exist.
2. Issue a cross certificate from organization B to A, if one doesn't exist.
3. At the server console enter the command load updall names.nsf -t $certifiers.
4. Select "Perform request again" in the response document for the "Initiate Rename in Address Book" request.

People should make backups of renamed IDs.
Once an ID is renamed, backup copies of the original ID become obsolete. So be sure to tell people to make new backup copies of renamed IDs.

Deleting references to a person, server, or group

If you need to delete the name of a person, server, or group use the Administration Process because it can automatically remove the name from databases throughout a domain.

You can't press a delete key on the keyboard to initiate Administration Process deletions.
For example, if you select a Person document and click DEL, the document is deleted but the Administration Process isn't involved and so the person's name isn't removed anywhere else.

You can delete a name from the Public Address Book immediately or delay the deletion.
When you choose a delete action and you have at least Editor access to the Public Address Book you also must choose whether to immediately delete occurrences of the name from the Public Address Book or to

delay the deletion. When you delay the deletion, the server deletes names from Person documents in the Public Address Book by default at 12:00 A.M. and other occurrences of the name in the Public Address Book by default after 60 minutes. If you delete names immediately, the deletions occur immediately in the foreground and so you can't use the workstation until they are done. We therefore don't recommend deleting immediately, especially if you're deleting several names at once.

If you choose a deletion action but have only Author access to the Public Address Book, then deletion of the name from the Public Address Book is automatically delayed--you're not given the option to delete the name immediately.

Deleting names from Author fields can result in uncategorized documents.
When the Administration Process deletes the last name from an Authors field in a document, the document becomes uncategorized in a view that categorizes by author.

Enabling and using password checking

You can use the Administration Process to require that people provide passwords each time they authenticate with a server. If you do this, you can also require that people periodically change their passwords to help prevent someone with an unauthorized copy of an ID from continuing to use it after the password change.

Only enable password checking for people and servers that run Release 4.5 or higher.
Password checking during authentication requires that workstations and servers run R4.5. If you enable password checking on a server running a previous release, authentication occurs without password checking. If you enable password checking for a workstation running a previous release, authentication fails when the workstation attempts to connect to a server that requires password checking.

It's also necessary to enable password checking in Server documents.
For password checking to work, you must enable the feature in Server documents as well as in Person documents. To enable password checking for a server, select "Enabled" in the Check password field in the Security section of the Server document of each server you want to require password checking. You do this manually, rather than through the Administration Process.

You can optionally require people to periodically change their passwords.
Doing this helps prevent an unauthorized user of an ID from continuing to use it after a password change. To require password changes, enter a "Required change interval" in days when you enable password checking in a Person document. If you don't want to require password changes, enter 0 as the required change interval. A person is prompted to change the password as the required change interval approaches**.** If the required change interval expires without the person changing the password, the person can't authenticate with servers that check passwords until providing the new password.

If you specify a required change interval, you can also set a grace period that determines the amount of time after expiration of a required change interval a person has to provide a new password. The default is an unlimited amount of time. If you set a grace period and the person doesn't change the password within it, the person is then locked out from servers that check passwords. Using a grace period is a way to automatically deny server access to inactive people, for example people who have left the organization. To allow someone who is locked out of servers because of an expired grace period to access them again, manually delete the data in the Password digest field from the Person document then have the person access a server and provide a new password.

Don't enable password checking for a person whose ID uses multiple passwords.
If you do this the person won't be able to authenticate with servers enabled for password checking.

People whose Person documents have password checking enabled can't use their IDs with Notes Release 3.
The first time a person for which password checking is enabled authenticates with a server that requires password checking, the user ID is altered and can only be used with Release 4.0 or later.

If a person has multiple copies of an ID, only one password is valid for all of them.
If a person has multiple copies of an ID, the password on the ID first used to log on to a server after password checking is enabled is the only one that is valid for that person. If the person tries to authenticate using a copy of the ID with a different password, authentication fails unless the person changes the password on the ID to match the one the server recognizes.

You can enable password checking in Person documents without using the Administration Process.
To do this, select "Check password" in a Person document while in edit mode. However use the Administration Process instead if you are enabling password checking for several people at once as this saves you time. If your organization replicates the Public Address Book using a hub and spoke topology for security purposes and you change the Person document manually, make sure to do this from the hub replica of the Public Address Book so the change replicates.

Adding and deleting resources for scheduling

A Resource Reservations database stores information about resources, for example rooms and equipment, so that people can schedule them for meetings. When you create a resource in a Resource Reservations database, the Administration Process posts a "Resource Add" request that duplicates the resource in the Mail-In Database and Resources view of the Public Address Book -- duplicating the resource in the Public Address Book lets people do free time queries when they are creating a Calendar Entry in their mail files to see when a resource is available. Resources are created (and deleted) in the Resource Reservations rather than the Public Address Book so that people can add and delete resources without having create and delete access directly to the Public Address Book.

You must have the necessary access to create a resource.
You must be included in the [CreateResource] role in the Resource Reservations database to create a resource in the database.

To delete a resource, an administrator must approve the deletion.
When somebody initiates a resource deletion from the Resource Reservations database, the resource isn't deleted immediately. Instead, the Administration Process posts an "Approve Resource Delete" request in the Administration Requests database. Somebody with Editor access to the Administration Requests database must then approve the deletion before it can occur.

Moving and creating replicas of databases

You can save yourself time by using the Administration Process to do the following database tasks:

- Move databases from a cluster server to another server
- Create replicas of databases

You can only move or replicate databases between servers in the same domain using the Administration Process.
Although you can select source and target servers that are in different domains, databases aren't created on the target server because it can't respond to requests from a different domain.

To move a database, the source server must be a member of a cluster.
Moving a database using the Administration Process requires that the source server, the server you're moving the database off of, is a member of a cluster. This is because after a database is moved to a target

server, a cluster server deletes the original database only after ensuring that no one is still accessing it--a feature not supported by non-cluster servers.

The source and target servers must have the necessary access.
Before you create a replica of a database or move a database, it's important to set up the necessary server access. The source server (or some other server in the domain that stores the database and replicates with the target server) must have "Create replica databases" access to the target server--this allows the source server to create a wildcard replica of the database on the target server and to populate the wildcard replica with documents. You must also give the target server at least Reader access to the database being moved or replicated.

Creating mail files during setup

If you choose the option "Create files during setup" when you register someone in Notes, the Administration Process automatically creates the mail file on the person's home server if the person hasn't yet created the mail file by running setup. This feature is particularly useful for people who set up Notes over dial-up connections, as creating mail files during remote setup can take some time.

A home server must have the access necessary to create the mail file.
In order for the Administration Process on a home server to create a mail file, the server must have "Create new databases" access to itself. Check the "Create new databases" field in the Restrictions section of the Server document for the home server--if there are entries in the field, be sure to include the home server as well. (If there are no entries in this field, the home server already has this access.)

ABOUT THE AUTHOR

Kendra Bowker earned a certificate in technical writing from Middlesex Community College in Bedford, Massachusetts. She has worked as a software technical writer for six years, the last four at Lotus. Kendra joined Lotus originally as a release notes writer and now contributes to the *Lotus Domino Administrator's Guide*.