Lotus Developer Domain
The Technical Resource for Lotus software
LDD Today

All about AdminP Part 1

Level: Intermediate
Works with: Notes/Domino
Updated: 02-Jun-2003

by Timothy Speed
with Paul Raymond

It's 10 AM Monday morning, time for the IT department status meeting. The new director opens the meeting and asks each person for a status of the previous week's activities. Finally, it is your turn. "Last week we renamed 1,000 users, issued 800 Web certificates, created 200 replicas, and moved 650 users to a new server. We did that with one administrator and one operator." The director looks at you in total disbelief and asks, "You did all that with just *two* people?" You nod and reply, "Actually the operator did most of the work." Finally the perplexed director asks, "What magic did you use to make that happen?" Smiling, you respond with a single word, "AdminP!"

The preceding scenario is no fantasy—AdminP (also knows as the Administration Process) is indeed this powerful. AdminP is a program that automates many routine administrative tasks for a Domino environment. These tasks can include managing (among many other things):

- Mail files (moving and deleting mail files, delegating calendars without providing Manager access, and enabling the "Out of Office" agent without Designer access)
- Replicas (creating, moving, and deleting replicas)
- User names (person and group renaming, deleting servers, internal certificate management, moving users from one organization level certificate to another, and automatically updating ID recovery information)

This article is the first of a two-part series describing all the components of AdminP. We discuss how each component works, and how you can use these features to make your job much easier (and to impress your boss). This article assumes that you're an experienced Domino administrator, familiar with Notes and Domino terminology.

AdminP components

In this article, we define AdminP as a set of components, rather than a single element. These components include:

- AdminP server task
- Administrator client (Domino and/or Web)
- Notes client
- Domino Directory (names.nsf)
- Certification log database (certlog.nsf)
- Administration Request database (admin4.nsf)
- Administration server (assigned to each database in the domain)

The following sections briefly describe these components.

AdminP server task

The AdminP server task runs on all Domino servers. This task loads when the Domino server is first started and is controlled through the Notes.ini variable ServerTasks. The AdminP server task wakes up on periodic time intervals (specified in the Administration Process section of the Server document) and executes commands waiting in the Administration Request database. Each command placed in the Administration Request database has an assigned proxy action. These proxy actions are essentially the Op-code that runs the Administration Process.

Each command placed in the Administration Request database is represented by a document. Each document has a number of fields, including one called ProxyAction. After each action has completed on a server, a response document is created to indicate the status of that request.

AdminP requests are not limited to only one Notes domain. You can now set up cross domain documents to share some of the commands between domains.

Administrator client
The Administrator client has all of the tools needed to initiate the AdminP commands. These include renaming and deleting users, deleting a replica, moving a database, and moving a user from one hierarchy to another.

Notes client
With Notes/Domino 6, the Notes client has now become an active participant in the administration process. The client now can complete and initiate many different administration processes. For example, the client can accept user name changes and x509v3 certificates into the Notes.id file. The client can initiate calendar ACL delegation. The client is involved with the process to move a user to another server and can issue a request to change the user's password and/or synchronize his Notes.id and Web password. And the client now automatically accepts ID recovery information without user prompts.

Domino Directory
The Domino Directory provides part of the instructions used with AdminP. For instance, when a user is renamed, the certificate information is changed. This is stored in a Person document in the Domino Directory. When the renaming process is in progress, this is indicated in the Person document under the Change Request field. Each person's name is stored in various fields in the Person document. When a user is renamed, both the old name and new name are stored.

Also, every server has a Server document that controls how the server is managed. Every Server document has a section on AdminP parameters.

AdminP commands affect Domino Directory information, including:

- Resource names
- Clusters
- Person documents, including client information
- HTTP password synchronization
- Group updates and deletions
- Server information (protocol and version)
- Policies
- Certificate Authority (CA) configuration
- License tracking

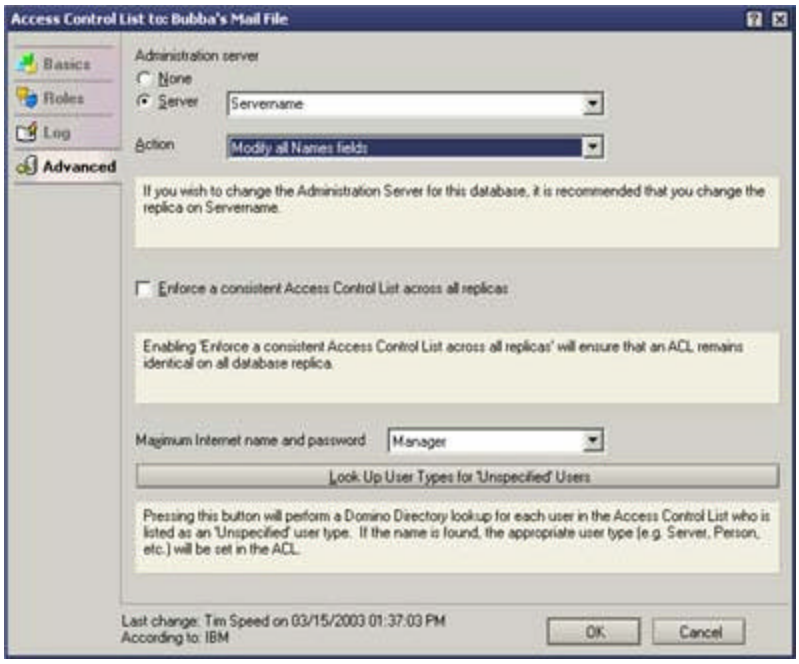
Certification log
The Certification log database (certlog.nsf) is created when you install the first server in a domain. The Certification log records certification-related activities from Domino, including new user and server registration, user recertifications and renames, and user moves from one organization level certifier to another. Each log entry tracks the data shown in the following illustration:

Certificate issued to:		Certificate issued by:	
Name:	Mike Admin/newfastcert	Name:	/newfastcert
License:	North American	License:	North American
ID Number:		ID Number:	80F4 F6D1 0599 41A5 21E7 D392 E500 07A9
Certificate not valid before:	12/26/2002 02:23:43 PM	Date logged:	12/27/2002 02:23:43 PM
Certificate not valid after:	12/26/2004 02:22:17 PM		

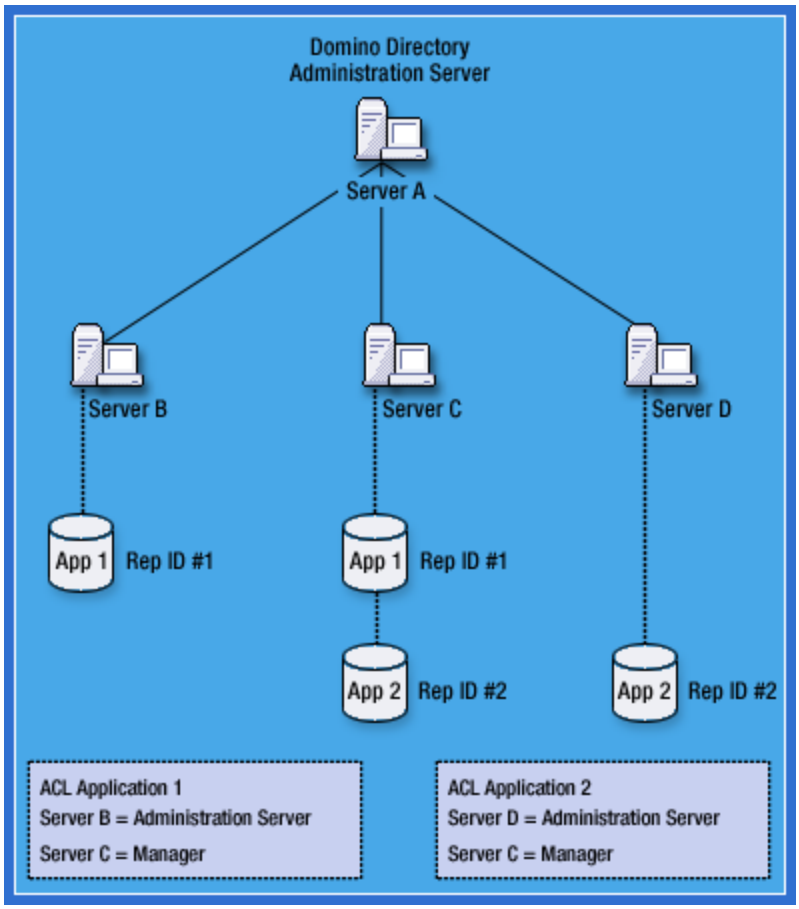
AdminP requires a Certification log on each server used to initiate administration requests. You can do this by creating a replica of the Certification log on every administration server and on every server used for user management.

Administration Request database
The Administration Request database (admin4.nsf) contains all the administrative requests from a single domain. Every request (via a proxy action) that is placed in the Administration Request database replicates to every server in the domain. This database is described in detail later in this article.

Administration server
Every database must have an Administration server assigned to it, listed in the database's ACL. This includes the Domino Directory. The Administration server setting tells AdminP where to process each database. The Administration server appears in the ACL with a key icon next to its name. In each domain, there is a single Primary Administration server. The Primary Administration server is determined by the value in the ACL of the Domino Directory (names.nsf). To set the Administration server for a database (including the Primary Administration server), highlight the database and select File - Database - Access Control, then click Advanced:



For example, let's say you need to rename 1,000 users. Each user may have entries in Author, Reader, and Name fields in 100,000 documents in a single database. This means every document may need to be changed. Consider the following illustration:



In this example, there are four servers and two applications. Server A is the Administration server for the Domino Directory. This makes it the Primary Administration server for this domain. Server B has two applications, App 1 and App 2. The Administration server for App 1 is Server B and the Administration server for App 2 is Server D. Server C has a replica of each application. The command to change the values of the Name fields is issued on the Primary Administration server (Server A) and then sent to the other servers for processing. Each server receives the commands and processes them based on the time of arrival and the settings in the Server document.

Notice that the App 1 database is on both Server B and Server C. If the name change command ran on both servers, you would have 100,000 changes in both replicas, resulting in a big mess of replication conflicts. AdminP is designed to keep that from happening by looking at the ACL of each database on each server. If the ACL Administration server entry matches the name of that server, it processes the command. If the database ACL Administration server entry does not match that server, the command is ignored. In the case of Server B, the ACL entry for App 1 identifies Server B as the Administration server. Thus, commands that arrive on Server B are executed on App 1. The administration commands are also sent to Server C. But this server does not have any applications that list it as the Administration server. So no commands are processed on Server C. Finally, Server D is listed as the Administration server in the ACL for App 2. So any commands arriving on Server D are executed on App 2.

As you can see, this architecture allows only one server to update any single application (via replica ID). So now you ask, "Do I need to add an Administration server entry for every database in my Domino environment?" The answer is yes—but don't panic; there are several ways you can do this:

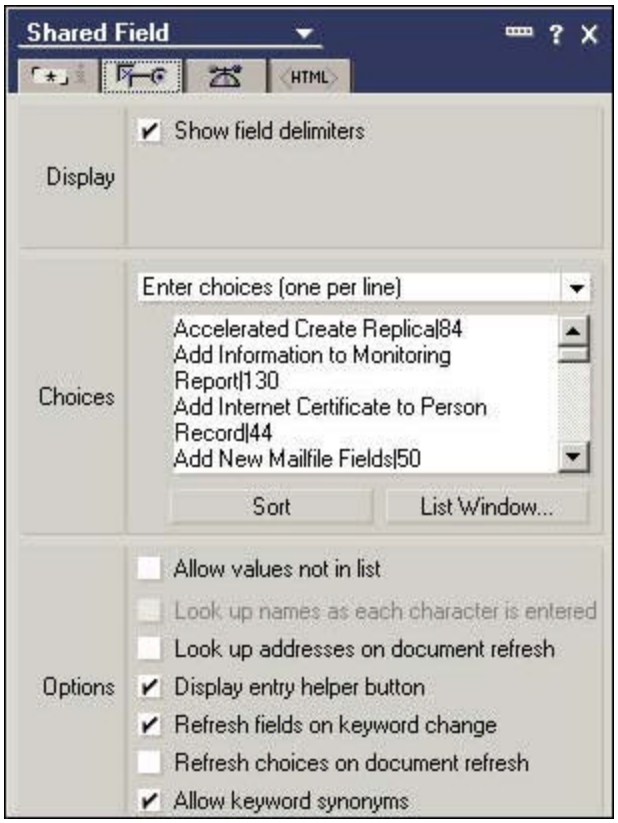
- *Manually*
  Open the Advanced section of the ACL dialog and edit the Administration Server field. This works fine for one or two databases, but in large environments, this obviously would take a very long time.
- *Via the Administrator client (Domino or Web)*

The Administrator client allows you to set individual databases or a large group of databases with a single operation. Open the Administrator client and select the databases that need to be updated. Right-click and select Access Control - Manage. This opens the standard ACL dialog box. Edit the ACLs as needed and save the entry. This updates the Administration server setting on all selected databases.

- *Via LotusScript*
  The NotesACLEntry Class has a Read/Write property that you can use in a LotusScript agent. Using the ISAdminServer property, you can create a simple agent that reads and/or sets the Administration server of an ACL entry.
- *Via the Lotus Notes API*
  You can create your own custom tools to edit and manage the Administration server name of a database. Two functions commonly used for this are ACLGetAdminServer and ACLSetAdminServer.
- *External vendor tools*
  There are many different vendor tools that include Administration server management features. Check with your vendor for details.

Proxy actions

Now let's look at AdminP commands. Each command is controlled by an individual document placed into the Administration Request database. Every document has a field named ProxyAction. You can see these proxy actions in two places: the field properties of a document in the Administration Request database or in the Administration Request document form. For the latter, open the ProxyAction shared field and look at the list of choices, for example:



Each proxy action has a number. R5 has 82 different proxy actions and Domino 6 has 165. Proxy action numbers are backward compatible. For example, proxy action 1 (which renames a user in an Access Control List) is the same in both R5 and Domino 6, and proxy action 119 (rename a Web user in an Access Control List) is new to Domino 6. See the **Proxy actions in R5 and Domino 6 sidebar** for a complete list.

Each AdminP request can create a response document called the Process Log. The response document shows if an AdminP request completed successfully or failed with an error message. Most proxy actions are

created on the Primary Administration server. Some can be initiated on a spoke Administration server. For example, if you rename a user, the primary request is issued by AdminP at the Primary Administration server. In this example, a proxy action 6 (move person's name in hierarchy) is created on the Primary Administration server. You approve the name change and the Primary Administration server creates a proxy action 8 (initiate a rename in the Domino Directory). AdminP updates the public key and also updates the Certificate Request field in the Person document.

In the Person document Administration tab, there is a field titled Change Request. The internal name of this field is DisplaychangeRequest. The field formula is:

```
@If((ChangeRequest != "" | $AdminpOldWebNameExpires != ""); "Pending";"None")
```

If there is a value in the Change Request field, a value of Pending appears.

Types of proxy actions
There are three basic types of AdminP proxy actions:

- Operations that execute on the Primary Administration server
- Operations that execute on all spoke Administration servers
- Operations that execute on a targeted server

The following sections describe these proxy action types.

Operations that execute on the Primary Administration server
Most AdminP processes start on the Primary Administration server. However, the actual command (the document with a proxy action) can be created on virtually any server. Let's consider renaming the user's organization level. This is a proxy action 6 (move person's name in hierarchy). You start this process from the Domino Directory. A document is created in the Administration Request database that requires administrator approval. After this document is approved, another document is created. This is a proxy action 8 (initiate rename in Address book). This proxy action can only run on the Primary Administration server.

The Domino Directory is updated with the user's information after proxy action 8 executes successfully. This replicates to a spoke server. The user opens a database on this spoke server and a proxy action 5 (rename person in Address book) is created. Next, the Administration Request database replicates with the Primary Administration server, and this action is executed. In this example, proxy actions 6, 8, and 5 all ran on the Primary Administration server. Proxy action 5 was created on the spoke server, but this action was initiated when the Domino Directory was updated for that user. In each case, the actual execution of the proxy action was completed by the Primary Administration server, not on a spoke server.

The following table lists AdminP proxy actions that execute only on the Primary Administration Server (note this is not the complete list):

Delete in Domino Directory	Accelerate create replica
Place server's Notes build number into Server document	Store directory type in Server document
Rename server in Domino Directory	Replace roaming server's field in Person document
Rename person in Domino Directory	Modify user information stored in Domino Directory
Move person's name in hierarchy (actually this action can be approved on any server)	Modify CA configuration in Domino Directory
Delete statistic monitors in Domino Directory	Update license tracking information in Domino Directory
Initiate rename in Domino Directory	Re-initiate rename in Domino Directory
Recertify server in Domino Directory	Delete Policy document in Domino Directory
Recertify person in Domino Directory	Initiate Web user rename in Domino Directory

Delete in Person documents	Rename Web user in Domino Directory
Change user password in Domino Directory	Rename Web user in Person documents
Add Internet certificate to Person document	Delete Web user in Domino Directory
Delete person in Domino Directory	Change HTTP password in Domino Directory
Delete server in Domino Directory	Update roaming user state in Person document
Delete group in Domino Directory	Update roaming user information in Person document
Approve delete person in Domino Directory	Recertify cross certificate in Domino Directory
Approve delete server in Domino Directory	Recertify Certificate Authority in Domino Directory
Approve rename person in Domino Directory	Add or modify group in Domino Directory
Approve rename server in Domino Directory	Modify ID recovery information in Domino Directory
Modify room/resource in Domino Directory	

You may ask, "How will I know what type of command will operate on which server?" Open any Administration Request database and look at the AdminP request document. You see a field titled Server(s) to perform the action. In our example, this field is set to Administration server for the Domino Directory.

Operations that execute on all spoke servers

Let's continue with our example. The user has accepted the new name and a proxy action 8 (initiate rename in Address book) has been created on one of the spoke servers. This action now replicates to the Primary Administration server for the domain. After this proxy action executes, AdminP creates additional requests. One of these is a proxy action to update the ACLs in each database on every server in the domain. This is proxy action 1. Again, this is easy to determine by just looking at the Request document in the Administration Request database.

The Request document includes the field Server(s) to perform the action: See example figure below. If an asterisk appears in this field, this command attempts to execute on all servers in the domain. Here are a few examples of "asterisk" commands:

- Delete user in Access Control List
- Rename in Access Control List
- Move person's name in hierarchy
- Delete in Reader/Author fields
- Rename person in unread list

Operations that execute on a targeted server

AdminP is actually really smart. This is where the targeted server commands come in. Again, let's go on with our example of our renamed users. So far, you have run the rename process, the user has accepted the new name, and AdminP has issued a command to change the name in the ACL. Now AdminP analyzes the Person document of this user and determines if any targeted commands need to be created. If the user's Person document has a listing for a mail file, AdminP creates two commands:

- Rename person in calendar entries and profiles in mail file
- Rename person in Free Time database

The commands replicate to the targeted server and execute there. You can determine which commands are for a targeted server by opening the Request document and looking at the field Server(s) to perform the action. In this case, the value is NTMain, meaning the command executes only on that server.

Now for a little bad news—unless you create a selective replication formula, all commands in the Administration Request database are replicated to all servers, including targeted server commands. To avoid this, here's a sample selected replication formula:

ASDDList := "0":"2":"3":"4":"5":"7":"8":"9":"10":"11":"12":"16":"19":"26":"28":"29":"30":"34":"35":"36":"37":


```
"40":"41":"44":"46":"47":"50":"52":"54":"55":"56":"63":"64":"67":"70":"71":"73":"76":"77":
"80":"83":"85":"86":"89":"95":"96":"97":"98":"99":"103":"107":"109":"110":"113":"118":"120":"121":"127":
"133":"134":"136":"141":"144":"146":"157":"159";

SELECT @IsMember (@LowerCase
(@Name ([CN] ; ProxyServer));"*":@LowerCase(@Name([CN]; @UserName))) & Type != "AdminLog" &
!@IsMember (ProxyAction;ASDDList)
```

Caution: This is sample code only. We do not offer support for this, so use it at your own risk. Put this formula on your spoke servers only, not your hub or Primary Administration server. Also, you may need to update this formula with each release of Domino.

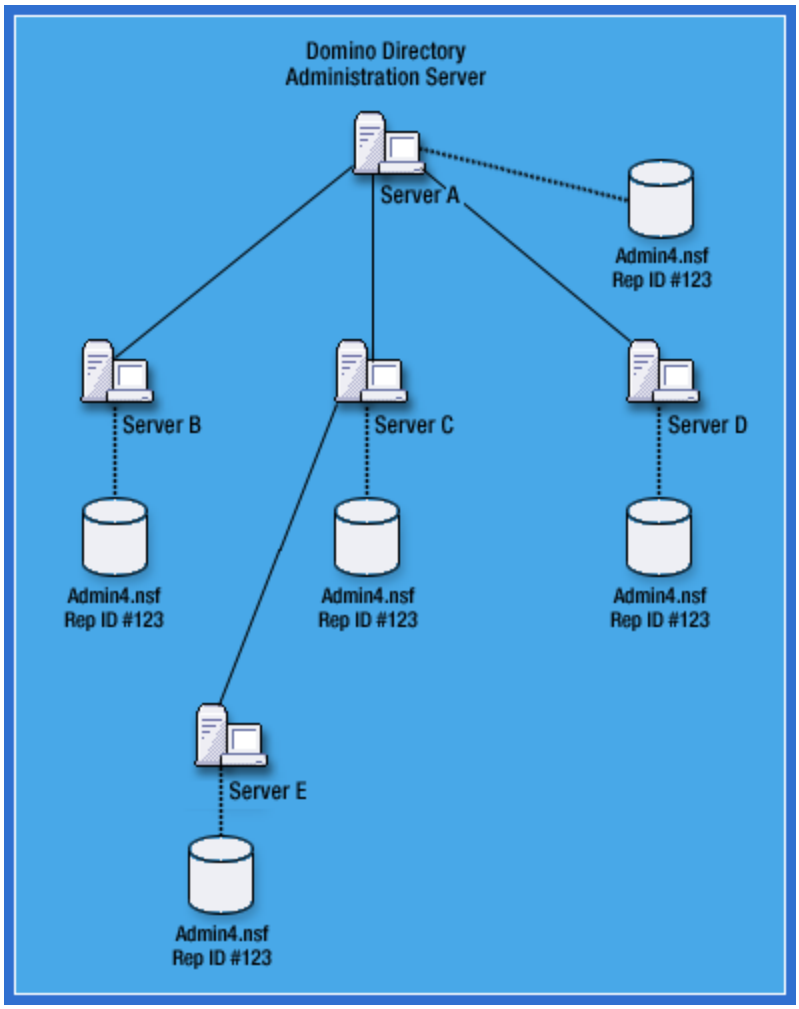
Proxy action execution timing

Proxy Actions are executed at different times, based on the type of proxy action. There are four different intervals:

- *Immediate*
  These requests typically execute within one minute. Examples include check mail server's access, promote new mail server's access, create new mail replica, add new mail file fields, replace mail file fields, and push changes to new mail server.
- *Daily*
  These requests are processed once a day as defined by a setting in the Server document. These requests include all new and modified daily requests to update the Person document in the Domino Directory, rename person in unread list, and delete obsolete change requests.
- *Timed*
  These are used by a recommended resource balancing plan. This process is generated by the **Tivoli Analyzer**. Time-based requests normally apply to move database or to create replica actions. Note that time-based execution requests let you specify the time that the AdminP request is executed. Examples of timed requests include check access for new replica creation, check access for move replica creation, check mail server's access, and check access for non-cluster move replica.
- *Delayed*
  Delayed requests are executed by the timing set in the Server document. Rename in Reader/Author fields is a delayed request.

Administration Request database

All roads lead to Rome or, in our case, all AdminP actions end up in the Administration Request database. This database contains all requests for a single domain. (We will discuss cross domain functions in Part 2 of this article series.) Every request (via a proxy action) placed in the Administration Request database replicates to every server in the domain:



Each Administration Request database in a domain has the same replica ID and must replicate to all other servers in the domain that run AdminP. This allows one server to post a request and another to respond to it. When an additional server in your domain is set up, the Administration Request database is copied from the registration server to the new server.

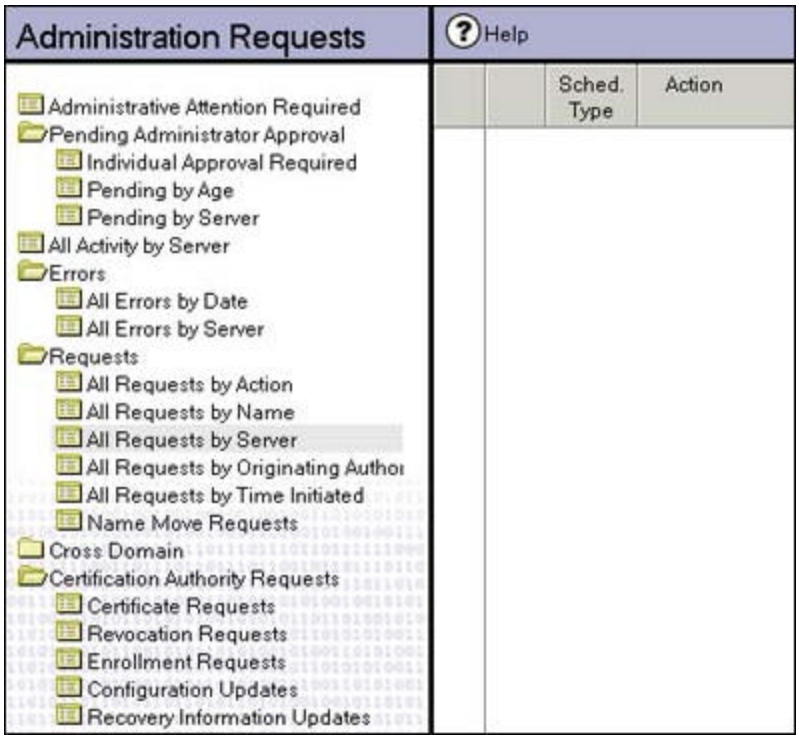
For instance, let's say you want to recertify a user. The command to recertify a user in the Domino Directory (proxy action 10) can be issued to any server in the domain. The command replicates to the Primary Administration server (Server A in the preceding chart), where it executes. The process is started in the Administrator client when you request that a user be recertified. The proxy action is created in the Administration Request database.

After the request is placed into the database, AdminP on the Primary Administration server processes the command. This command does the following:

- Updates the Domino Directory's Person document for this user. The public key for the user is replaced by the value in the Administration Request document.
- Creates an AdminLog response document with status information.

When the user authenticates, the ID is updated with a new public key and possibly with a new expiration date.

The Administration Request database has a number of views. Each view provides reporting information or access to approve certain actions. (Many actions require approval from an administrator.) The following illustration shows the basic views in the Domino 6 Administration Request database:



The following sections describe these views.

Administrative Attention Required
If an error is detected, ErrorFlag = "2". One example is when AdminP attempts to update Reader fields and fails. In this case, an error document is created and placed in this view. AdminP creates a doclink to each document it was unable to update.

Individual Approval Required
Documents appear in this view if the ApprovalFlag field is missing and if one of the following requests are issued:

- Cross domain requests, including approve delete person in Domino Directory, approve delete server in Domino Directory, approve rename person in Domino Directory, and approve rename server in Domino Directory
- Approve deletion of moved replica
- Approve refused name change
- Approve deletion of hosted organization storage

Pending Administrator Approval\By Age, Pending Administrator Approval\By Server
Documents show up in these views (sorted by age or server) if the ApprovalFlag field is missing and if one of the following requests are issued:

- Cross domain requests, including approve delete person in Domino Directory, approve delete server in Domino Directory, approve rename person in Domino Directory, and approve rename server in Domino Directory
- Approve resource deletion
- Approve deletion of private design elements
- Approve replica deletion
- Approve revert name change
- Approve certificate request
- Approve person's name change request
- Approve new public key request

All Activity by Server

This view organizes the Administration Log documents, so you can see the type of Administration Requests that have been performed on a person, group, or server.

All Errors by Date, All Errors by Server
All Errors by Date displays the Administration Log documents, so you can see all errors encountered by the servers performing Administration Requests. All Errors by Server displays the Administration Log documents, so you can see the errors each server encountered performing Administration Requests.

All Requests by Action, All Requests by Name, All Requests by Server
All Requests by Action shows the Administration Request documents, so you can see each request to be performed followed by the Administration Log response documents. All Requests by Name is one of the most useful views in the Administration Request database. This view shows you the name of the person, or server, that is being operated on. All Requests by Server is the default view in the database. This view shows the Administration Request documents so you can see all requests to be performed by a particular server followed by the Administration Log response documents.

All Requests by Originating Author
This view shows who has been issuing AdminP requests. This view when expanded also shows the person being processed.

All Requests by Time Initiated
This view displays each entry and response document, based on the sorting of when the proxy actions was first entered into the Administration Request database.

Name Move Requests
This view shows documents created when a person is moved within the hierarchical name tree. You select documents in this view and then choose Actions - Complete move for each selected entry. This is processed by AdminP and a proxy action 8 (initiate rename in Domino Directory) is created for each user.

Cross Domain Configuration
This view shows the configuration documents that control how the Cross Domain administration functions operate.

Cross Domain Delivery Failures
The Cross Domain administration function uses the Notes mailer (router) to send administration messages between domains. This shows NDR (non-delivery reports), showing failed attempts to send an update from one domain to another.

Certificate Requests
This view shows requests to create an Internet or Notes certificate. This view is monitored by the person assigned by the Certification Authority (CA) or Registration Authority (RA).

Recovery Information Update
This view is used with the CA process only. This view shows how AdminP updated the ID and password recovery information for any Notes ID that is stored in a CA database.

Conclusion

This article introduced you to AdminP. We took a quick tour of its components and explained how proxy actions and the Administration Request database work. In Part 2 of this series, we'll explore AdminP further, looking at cross domain administration requests and how to control AdminP functions through Server document settings, server console commands, the Notes.ini file, and database purge intervals.

ABOUT THE AUTHORS
Timothy Speed is an infrastructure and security architect for IBM Software Services for Lotus (ISSL). Tim has been involved in Internet and messaging security since 1992. He also participated with the Domino infrastructure at the Nagano Olympics and assisted with the Lotus Notes systems for the Sydney Olympics. His certifications include MCSE©, VCA (VeriSign Certified

Administrator), Lotus Domino CLP Principal Administrator, and Lotus Domino CLP Principal Developer. Tim has also co-authored four books: *The Internet Security Guidebook* , ISBN: 0122374711, February, 2001; *The Personal Internet Security Guidebook* , ISBN: 0126565619, October, 2001; *Enterprise Directory and Security Implementation Guide: Designing and Implementing Directories in Your Organization* , ISBN:0121604527; and *Internet Security: A Jumpstart for Systems Administrators and IT Managers, ISBN* 1555582982. You can reach Tim at **Tim_Speed@us.ibm.com**.

Paul Raymond is a Development Relations Manager within the Product Introduction organization. He was involved with the early deployment Design Partner Beta program for Notes/Domino 6.0 and continues to be the lead for the Notes/Domino 6.5 Beta programs. Paul joined Lotus in 1992 and worked in various parts of the organization ranging from Desktop Support and Field Support Services before joining the newly formed Development Relations team.

Proxy actions in R5 and Domino 6

The following tables list proxy actions in R5 and Domino 6.

Domino 5 and 6 proxy actions

These proxy actions apply to both Domino 5 and 6:

Number	Description
0	Delete in Address Book
1	Rename in Access Control List
2	Copy server's certified public key
3	Place server's Notes build number into Server document
4	Rename server in Address Book
5	Rename person in Address Book
6	Move person's name in hierarchy
7	Delete statistic monitors in Address Book
8	Initiate rename in Address Book
9	Recertify server in Address Book
10	Recertify person in Address Book
11	Add server to cluster
12	Remove server from cluster
13	Create replica
14	Move replica
15	Delete original replica after move
16	Delete in Person documents
17	Delete in Access Control List
18	Delete in Reader/Author fields
19	Rename in Person documents
20	Rename in Reader/Author fields
21	Delete mail file
22	Approve file deletion
23	Delete unlinked mail file
24	Create mail file
25	Monitor replica stub
26	Delete obsolete change requests
27	Get file information for deletion
28	Request file deletion
29	Add resource
30	Delete resource
31	Approve resource deletion
32	Check access for new replica creation

33	Check access for move replica creation
34	Set Password fields
35	Change user password in Address Book
37	Set Directory Assistance field
38	Rename person in Free Time Database
39	Rename person in calendar entries and profiles in mail file
40	Rename group in Address Book
41	Rename group in Person documents
42	Rename group in Access Control List
43	Rename group in Reader/Author fields
44	Add Internet certificate to Person document
45	Check mail server's access
46	Update client type in Person document
47	Update external domain information
48	Promote new mail server's access
49	Create new mail file replica
50	Add new mail file fields
51	Monitor new mail file fields
52	Replace mail file fields
53	Push changes to new mail server
54	Delete person in Address Book
55	Delete server in Address Book
56	Delete group in Address Book
57	Delegate mail file
58	Approve delete person in Directory
59	Approve delete server in Directory
60	Approve rename person in Directory
61	Approve rename server in Directory
62	Modify room/resource in Directory
63	Update server's protocol infomation
64	Create ISPY mail in database
65	Check access for non-cluster move replica
66	Non-cluster move replica
67	Store server's CPU count
68	Rename person in unread list
69	Delete replica after move
70	Store server's DNS Hostname in Server document
71	Store server's platform in Server document
72	Approve deletion of private design elements
73	Request to delete private design elements
74	Delete private design elements
75	Approve deletion of moved replica
76	Request to delete moved replica
77	Configure Domain Catalog
78	Delegate Web mail file

83	Set Web Admin fields
101	Sign database with server's ID file
999	Unrecognized request

Domino 6 proxy actions
These proxy actions apply only to Domino 6:

Number	Description
84	Accelerate create replica
85	Store Directory type in Server document
86	Set Directory filename
87	Create roaming user's roaming files
88	Promote new roaming server's access
89	Replace roaming server's field in Person document
90	Monitor roaming server's field in Person document
91	Create roaming user's replica stubs
92	Remove roaming user's roaming files
93	Check roaming server's access
94	Create roaming user's replicas
95	Store certificate in Domino or LDAP Directory
96	Store Certificate Revocation List in Domino or LDAP Directory
97	Modify user information stored in Domino Directory
98	Remove certificate from Domino or LDAP Directory
99	Modify CA configuration in Domino Directory
100	Push changes to new roaming server
102	Configure Certificate Authority publication
103	Remove Certificate Revocation List from Domino or LDAP Directory
104	Update delegated user's mail file list
105	Sign Certificate Authority configuration
106	Approve refused name change
107	Retract person's name change
108	Set user name and enable scheduled agent
109	Update license tracking information in Domino Directory
110	Re-initiate rename in Domino Directory
111	Delete server in Domain Catalog
112	Maintain trends Database document
113	Delete Policy document in Domino Directory
114	Approve revert name change
115	Approve certificate request
116	Approve person's name change request
117	Approve new public key request
118	Initiate Web user rename in Domino Directory
119	Rename Web user in Access Control List
120	Rename Web user in Domino Directory
121	Rename Web user in Person documents
122	Rename Web user in Reader/Author fields

123	Rename Web user in Free Time Database
124	Rename Web user in calendar entries and profiles in mail file
125	Rename Web user in unread list
126	Delete Web user in Domino Directory
127	Change HTTP password in Domino Directory
128	Create Monitoring Report
129	Collect Monitoring Report information
130	Add information to Monitoring Report
131	Create IMAP delegation requests
132	Delete hosted organization
133	Update roaming user state in Person document
134	Update roaming user information in Person document
135	Create hosted organization storage
136	Recertify cross certificate in Domino Directory
137	Create object store
138	Get hosted organization storage information for deletion
139	Approve deletion of hosted organization storage
140	Delete hosted organization storage
141	Recertify Certificate Authority in Domino Directory
142	Find name in domain
143	Verify hosted organization storage
144	Add or modify group in Domino Directory
146	Modify ID recovery information in Domino Directory
148	Monitor roaming user's replica stubs
149	Delegate mail file on Administration server
150	Check access for new replica creation (time-based execution)
151	Check access for move replica creation (time-based execution)
152	Check mail server's access (time-based execution)
153	Check access for non-cluster move replica (time-based execution)
156	Create SSL certificate and keyring file
157	Enable server's SSL ports in Domino Directory
158	Change the server on which the agent runs
159	Store cross certificate in Domino or LDAP Directory
160	Set Web user name and enable scheduled agent
161	Update replica settings
162	Rename in shared agents
163	Web set soft deletion expire time
164	Rename in agent's Readers field
165	Delete in agent's Readers field
166	Monitor server's SSL status in Domino Directory
167	Delegate mail file on home server