

Endpoint Example

The screenshot below shows an example of an endpoint document for a user:

Endpoint: [Amilia Admin/DemoData](#) 

Server:	Server1/DemoData	Last Modified:	11/21/17, 3:41:58 PM
Type:	person	Open Change Map	

Database Access (4) **Group Membership (20)**

Total databases found:4

[▶ limit results](#)

TIPS: Click on column headers to sort. Use CTRL+F to quickly find items in the table.

Filepath	Access Level	Granted Through	Roles	Actions (legend)
anexample\circref.nsf	Editor	Circular Group Nested Group 1		CrDoc DiDoc -- -- -- -- RdPub WrPub
anexample\muchoadmin.nsf	Manager	Administrator Group	[Admin]	CrDoc DiDoc PerAg PerFld ShrFld LscAg RdPub WrPub
marketing\survey.nsf	Author	Survey Group 3		CrDoc -- -- -- -- -- RdPub WrPub
secure\dbpwd.nsf	Editor	Administrator Group Database Administrators	[CreatePasswords], [DeletePasswords], [ReadPasswords]	CrDoc -- -- -- -- -- RdPub WrPub

results in table:4

At the top of the document, you can see:

- the user's name (Amilia Admin)
- the server this information is relevant for
- the type of user it is (which can be person, server, or unknown).

The first tab on the bottom part of the document shows all the databases that the user has access to on this server, along with:

- what their access level is
- what groups gave them this access
- all the roles and actions (like create documents, delete documents, etc.) they have.

The database names and group names are hyperlinks, so you can click on them to get more information about the specific databases or groups in the list.

The second tab shows all the groups the user is in, and all the ways they are members of those groups:

Endpoint: Amilia Admin/DemoData



Server: Server1/DemoData Last Modified: 11/21/17, 3:41:58 PM
Type: person [Open Change Map](#)

Database Access (4)

Group Membership (20)

Total group paths found:20

▶ [limit results](#)

TIPS: Click on column headers to sort. Use CTRL+F to quickly find items in the table.

member of group...	type	...through the following path
*/DemoData	security-only	<named directly>
Administrator Group	security-only	Database Administrators
Administrator Group	security-only	Server Administrators
Administrator Group	mail & security	Web Administrators
Administrator Group	security-only	Database Administrators << Server Administrators
Administrator Group	security-only	Web Administrators << Server Administrators
Circular Group	mail & security	<named directly>
Database Administrators	security-only	<named directly>
Database Administrators	security-only	Server Administrators

In this example, you can see there are five different ways that they are members of the Administrator Group:

- through the Database Administrators group
- through the Server Administrators group
- through the Web Administrators group
- and also because the Server Administrators group is a member of the Database Administrators and Web Administrators group

It also shows what kind of group access they have: security, mail, or both. Security groups are used for ACL access to databases, and mail groups are used for sending email to the group.

Group membership can be tricky. In the example above, if you just remove the user from the Database Administrators group, they will still be members of the Administrator Group through membership in other subgroups. In fact, if you remove them directly from the Database Administrators group, they will still be members of that group because they are members of the Security Administrators group, which is a subgroup of Database Administrators.

Without endpoint processing, it's very hard to see the web of relationships that are involved with group membership and, ultimately, database access.