DAP Security Model

Technical Note

Manual release date: May-31-13.

Please send comments or questions to info@geosoft.com

Geosoft Incorporated
Queen’s Quay Terminal
207 Queen’s Quay West
Suite 810, PO Box 131
Toronto, Ontario
M5J 1A7
Canada
Tel: (416) 369-0111
Fax: (416) 369-9599

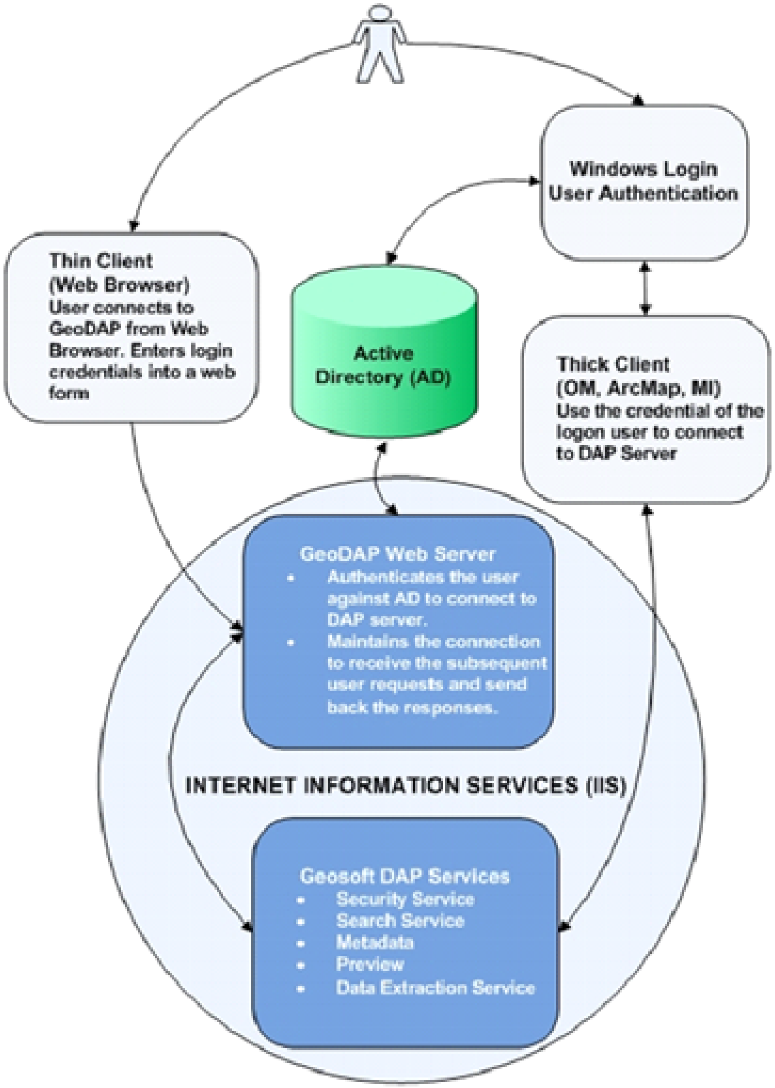
Website: www.geosoft.com
E-mail: info@geosoft.com

Support
For obtaining technical support, email support@geosoft.com

If you wish to speak to a technical support representative in your region, please visit the Geosoft Support page at: www.geosoft.com/about-geosoft/contact-us/world-offices for contact information.

DAP Security Model

The architecture of the DAP Security Model is illustrated below:


Windows Login
User Authentication
Thin Client
(Web Browser)
User connects to GeoDAP from Web Browser. Enters login credentials into a web form
Active Directory (AD)
Thick Client
(OM, ArcMap, MI)
Use the credential of the logon user to connect to DAP Server
GeoDAP Web Server
• Authenticates the user against AD to connect to DAP server.
• Maintains the connection to receive the subsequent user requests and send back the responses.
INTERNET INFORMATION SERVICES (IIS)
Geosoft DAP Services
• Security Service
• Search Service
• Metadata
• Preview
• Data Extraction Service

The DAP Server must be licensed for DAP Security in order to use this functionality.

DAP Server Access

How Seeker Accesses DAP Servers

1. A domain user launches a DAP client software application (Oasis montaj, ArcMap, or MapInfo).
2. Inside the client application, the **Seek Data > Seeker** command launches the DAP client plugin. The plugin sends the Active Directory ID of the logon user to the connected DAP Server to query the datasets available to the user.
3. The DAP Server returns - as a HTTP response via IIS - the list of datasets available to the user, along with the actions the user can perform on the datasets: view the metadata, preview the dataset and extract data from the selected dataset.

How Web Clients Access DAP Servers

Flamingo is the Geosoft DAP web client.

1. A user connects to Flamingo from a web browser and enters login credentials. The user is logged into the same domain as the IIS server.
2. Flamingo verifies login credentials. The cached user list and / or Active Directory is queried by DAP server.
3. The DAP Server determines the list of datasets that the user is allowed to access by querying against the Active Directory ID of the user. The DAP Server also indicates the actions the user can perform on the datasets: view the metadata, preview the dataset and extract data from the selected dataset. The DAP server sends the results to Flamingo.
4. Flamingo builds a results web page and sends an HTTP response to the user via IIS.
5. The Active Directory ID of the user is used for all subsequent queries of and requests to the DAP Server.

Enabling DAP Security

To enable the DAP security, do the following in the order listed:

1. Create an IDAP domain account.
2. Configure the IDAP account on the DAP Server computer.
3. Update IIS security through IIS Manager.
4. Apply the IDAP appropriate security permissions to all DAP related folders in Windows Explorer.
5. Plan and create DAP security groups in DAP Administrator.
6. Assign user permissions to DAP datasets in DAP Administrator. Publish the datasets; if the datasets are already published, refresh the security by running **Update DAP Server** in DAP Administrator.
7. Enable DAP security for Flamingo, if used.
8. Test the secured DAP Server in a DAP thick client (Seeker) and Flamingo.

Creating an IDAP Domain Account

DAP Server installation program creates an IDAP account on the local computer. To enable the DAP security, a domain IDAP in the internal network system needs to be created.

Set up the domain IDAP account to *No logon* to limit its security permissions and to *Password never expire*.

Configuring the IDAP Account on DAP Server Computer

On the DAP Server computer, use the **Control Panel |Administrative Tools | Computer Management | System Tools | Local User and Groups | Groups** and add the IDAP domain account to the *Users* group.

Updating the IIS Security through IIS Manager 7.5

1. Open the *Internet Information Services Manager* and select **<Server_Name>\Web Sites\Default Web Site\DAP**.
2. Right-click on the DAP website and from the popup menu, select **Properties**.
3. On the *DAP Properties* dialog, select the **Directory Security** tab.
4. Click the **Edit** button under *Authentication and access control*.
5. Ensure that *Enable anonymous access* is enabled. Enter the following information:
   - User Name: IDAP (use the Browse button to find the domain IDAP account)
   - Password: Password for the IDAP account
6. Your *Application Pool* should also be set to run as your IDAP_#### account.

   Save the changes and close all the dialogs.
7. Recycle the Application Pool or open a Command Prompt window and type the following at the DOS prompt: **IISRESET**

Applying IDAP Security Permissions to DAP Folders

1. On the DAP server computer, grant the IDAP domain account the same permission as the local IDAP_DAPServer account created by the DAP server setup program.

   ⚠ *It is important that you traverse the DAP software directory and its sub-directories to complete this process.*

   The following permissions are required on the DAP server computer and should be applied recursively.

   a. ..\Program Files (x86)\Geosoft\DAP Server\dap (modify)

   b. ..\dap\storage (read, write)

   c. ..\daptemp (modify)

Planning and Creating DAP Security Groups

Use DAP data security groups. The DAP security groups created should be easy to manage and make sense to your company’s workflow and business operations. One model to create DAP security groups is based on exploration projects. Use the DAP Administrator web application Security Settings to create DAP security groups.

Setting DAP Securities to DAP Data Folders/Files

In DAP Administrator, select a dataset(s), assign **Security** under *Dataset Properties*, and **Update DAP Server** to update access permissions.

Testing DAP Security

Use the Seeker client to test the change of access permissions.

Active Directory User Caching for Secured Servers

The first time a DAP client user makes a connection, they will be added to a cached user list called *guids.cache*. All users that have connected are stored in a new cache file. The next time the user connects, in a day, a month, or several months, they will have a faster connection experience.

The SID cache is stored in the root of the Managed Exploration Data Repository / Data Folder. It contains a list of active users. The DAP12.2 Server keeps an extra thread that watches the in-memory cache and automatically refreshes the list. The list is updated with new users when they connect to the DAP Server.

The file is an ASCII file, so new users can be added manually. There is no fixed limit on the number of users in the cache file. The in memory cache will be rebuilt if IISRESET is run. The combination of deleting the *guids* file and running IISRESET would delete the cache completely.