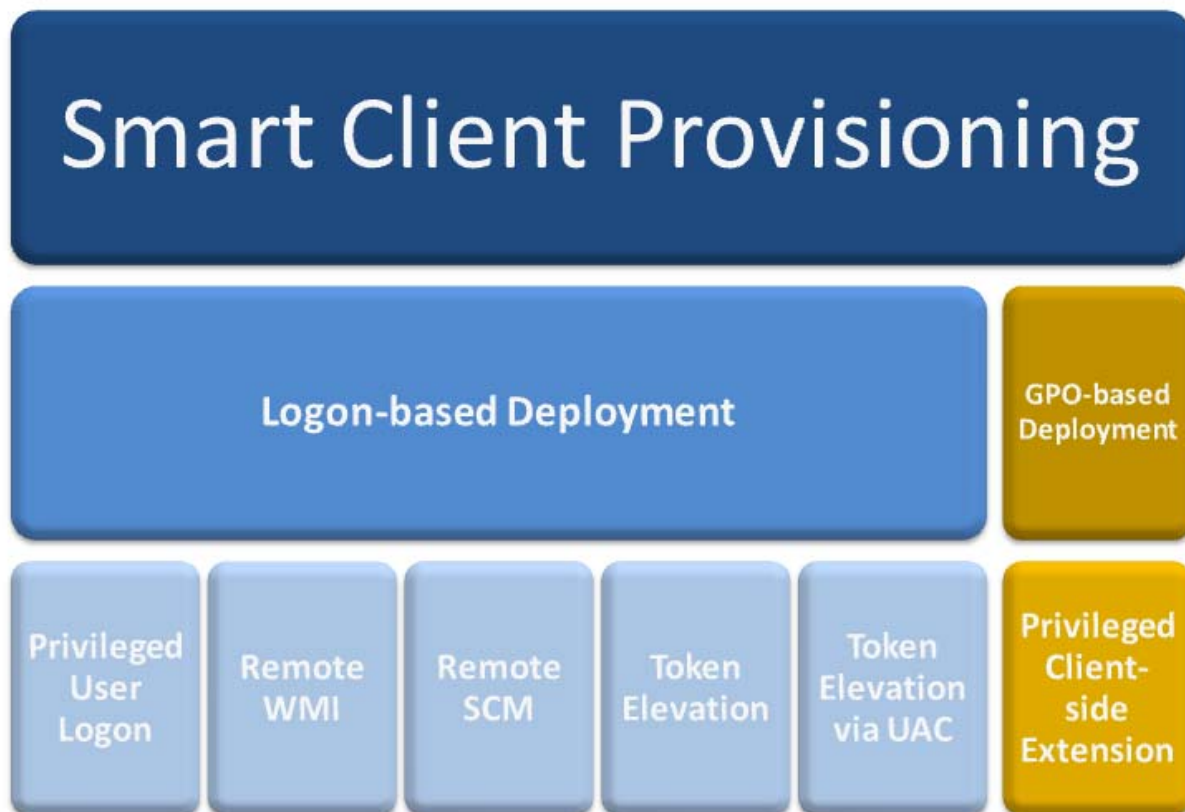


## SMART CLIENT PROVISIONING

Smart Client Provisioning is a new feature in Desktop Authority 8.1. Read on to learn more about this new client machine provisioning technique.

There are two ways in which Desktop Authority can deploy the necessary client files to machines that will be managed by Desktop Authority. Desktop Authority uses **Smart Client Provisioning** which encompasses both GPO-based Deployment and Logon-based Deployment. Smart Client Provisioning dynamically chooses from the best of several deployment approaches at runtime. The specific technique used depends on the client environment, and the obstacles present in that environment.



Desktop Authority GPO-based Deployment and Logon-based Deployment can both be used to deploy the Desktop Authority technology to client workstations and/or servers. They differ from each other in regard to the permission levels needed to accomplish the deployment. It is important to note that DA GPO does not require a user to login for the client files to be installed to the client, whereas the other methods used to deploy the client files will require a user login. This is important to consider when provisioning workstations or servers.

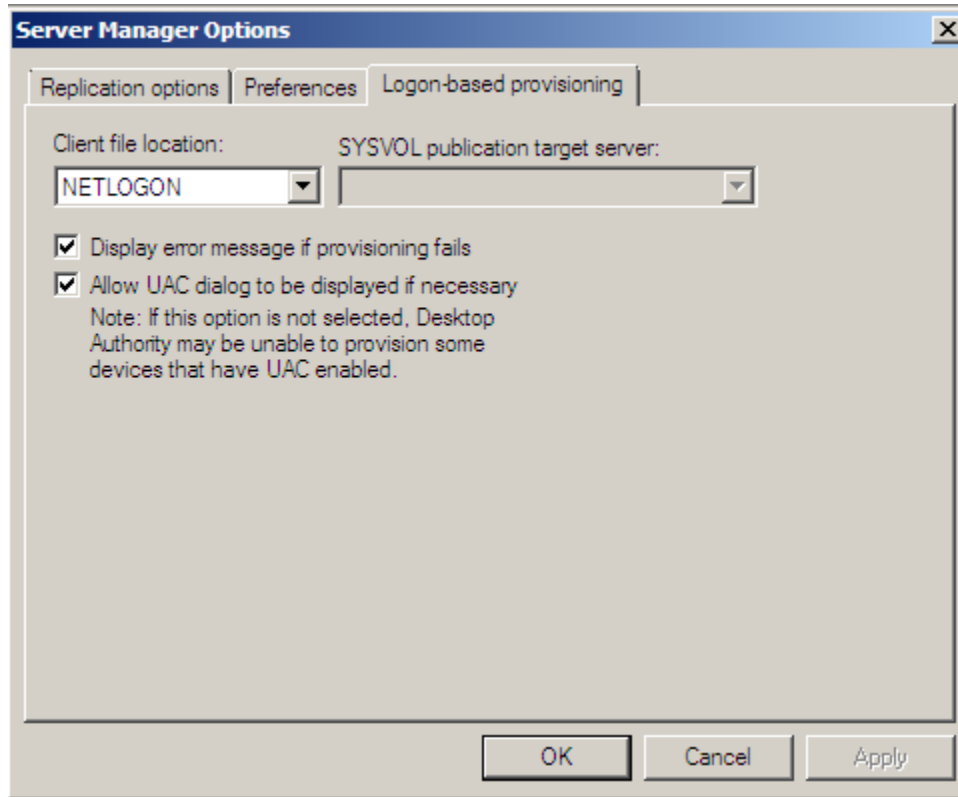
Deploying the Privileged Client-side Extension with GPO-based Deployment requires higher permission levels than non-domain admins, such as an OU Admin would typically have. Therefore, in some cases an OU Admin would not be able to configure the client file deployment without assistance from a Domain Admin, which defeats the purpose of having an OU Admin.

It is due to this privilege level issue, that Smart Client Provisioning has been implemented. Smart Client Provisioning will go through the following series of steps to get the DAClientInstall.MSI deployed or installed on a machine.

1. Attempt to install the client files (DAClientInstall.MSI) with the user's credentials. This will be successful only if the user is a local admin.
2. If using the user credentials does not successfully install the client files, then an attempt to install the files using a process that is launched administratively via WMI. It is possible that a firewall may block WMI communications. TCP ports 135 or 445 may be opened to allow a remote WMI connect.
3. If using WMI does not successfully install the file, then an attempt is made to use a process installed as a service via SCM (Service Control Manager). It is possible that the firewall may block remote SCM calls.
4. If the above fails, an attempt to install the MSI will be made using a process, run administratively, that uses token elevation. This method may require an UAC prompt to the user.
5. If the above fails, then display the UAC prompt and install the MSI using a process, run administratively, using token elevation
6. Otherwise, GPOs must be used to install the MSI. The use of GPO's is still required if you want no-touch provisioning of machines.

**It is important to note that if WMI fails to allow a remote connection, TCP ports 135 or 445 may be opened to allow this connection to be successful and thereby allow the installation of the client files. Opening these ports may be easier to configure than to configure the GPO-based Deployment throughout the enterprise.**

## Smart Client Provisioning Settings



### Client file location

With Logon-based Deployment, client files can be delegated to client machines via NETLOGON, a custom NETLOGON or SYSVOL. This makes the Logon-based Deployment very flexible.

Select either NETLOGON or SYSVOL from the drop down menu. Client files will be replicated to the specified location and applied to each client computer when a user logs into the computer with the Desktop Authority logon-script (slogic.bat).

Select NETLOGON to use any NETLOGON share to store the client files. Using NETLOGON allows the NETLOGON share (or any custom share hosting the user files) to be used.

Selecting SYSVOL will allow client files to be stored in a single place, to be shared between GPO and logon-based provisioning.

**When using both Logon-based Deployment and GPO-based Deployment, using the SYSVOL location is the most efficient. The file location is shared for both GPO-based and Logon-based Deployments. This is most useful in large environments. Using SYSVOL requires domain admin privileges.**

### SYSVOL publication target server

If the client file location is set to SYSVOL, select a server from the drop list as the target for the logon-based provisioning files. A server may also be manually entered into the entry field.

### Display error message if provisioning fails

Select this box to display an error message if the login provisioning fails for some reason. This error will be displayed on the client.

### Allow UAC dialog to be displayed if necessary

Select this box to ensure that the logon-based provisioning completes successfully on the client if UAC is enabled on the computer. During the provisioning process, a Windows UAC dialog will be displayed, if necessary. This may be required if the client-side firewall is unusually restrictive. The user must accept the request. If the permission is not granted or this box is not selected, Desktop Authority may not be able to provision the computer properly.