Global resource settings

This article describes how to make global settings for resources in Nexus Hybrid Access Gateway.

A number of settings can be specified globally to apply to all web resources as well as tunnel resources. Global resource settings cover, for example, internal proxy settings, mapped DNS names and filters.

They are configured in the Global Resource Settings section of Manage Resource Access.

The addresses for internal proxies are used when a resource is accessed via a cache or an ordinary proxy server. You can select to use NTLM v2 for HTTP and HTTPS proxies. If you experience authentication problems you may try to uncheck the use of NTLM v2.

Proxies available for configuration are:

- Internal HTTP proxy
- HTTPS proxy
- TCP proxy

The TCP proxy is used for the Access client.

You configure the DNS name pool for the purpose of improving link translation, and for using multiple DNS domains. Multiple DNS domains allow several customers to be hosted on the same Hybrid Access Gateway platform, and a single access point to serve multiple designs of logon pages as well as of the Application portal. This feature is mainly useful for ASP solutions.

The registered DNS names define the pool of available DNS names. To use multiple DNS domains, you define several DNS names for the access point.

All DNS names must also be registered in a public DNS server, or written to the hosts file on the client machine that uses the system.

When a user makes a request using a registered mapped DNS name, the access point looks up which server to connect to and which protocol to use and sends the request towards this server.

In Hybrid Access Gateway, three methods of DNS mapping are supported:

- URL mapping
  The resource is mapped to a path instead of using a mapped DNS name.
- Reserved DNS mapping
  The resource is mapped to a specific DNS name.
- Pooled DNS mapping
  The resource is assigned a DNS name on first access point request towards an internal server.

You specify which method of DNS mapping to use when adding or editing a resource.

You can add filters so that specific pages or requests are filtered when accessing a resource. For each filter you need to specify for which resource it applies. The filters are written using scripts in wasc format. Click the ?-sign for a more detailed description.

To find the scripts for the filters:

1. In the Hybrid Access Gateway administration interface, click Browse.
2. To find the scripts, go to access-point/built-in-files/scripts.
3. You can also create your own filter. The file script_syntax.txt contains information regarding how to create scripts for filters.

Here you enter the paths to the main page for the Portal and to the welcome page displayed after a successful logon.
Here, you define trusted IP addresses, for example an HTTP proxy.

Trusted in this context means that even though a client connecting to the Access Point may not have secure connection, incoming traffic from the specified IP address and the specified port is assumed to have a specified level of security (128 bit encryption) added.

Users are not redirected to HTTPS when coming from a trusted gateway.

Here, you select which type of information to add to internal requests. For example, the cookie names can be configured, and be extended with a prefix/suffix. Cookie names may need to be updated if you have several instances under the same domain, as you could have when running a Service Provider and an Identity Provider in the same location. In this case cookie of all instances would overwrite each other since they would have the same name.

The internal cookies are only visible to internal web resources. It is a fast way to do seamless integration as the cookies are in every single requires and are set by the Access Point. They are usually combined when you do backend user modification via the web services api.