phibstest

The *phibstest* command is used to check authentication, certificate validation, and Online Certificate Status Protocol (OCSP) information on the command line of the Barracuda NextGen Firewall F-Series and NextGen Control Center.

In Barracuda NextGen Admin, you can view the log for the *phibstest* utility in:

Logs > **Box** > **Control** > **AuthService**.

Type the command *phibstest -h* to display the help text that describes all possible options. Use *127.0.0.1* as the IP address if you are logged in directly to the firewall or Control Center.

Options

You can use the following options with *phibstest*:

phibstest 127.0.0.1 s

Displays the current status of the *phibsclt* components to verify the working status of authentication schemes, and to perform login and certificate validation checks.

phibstest 127.0.0.1 x

Checks certificate working state and displays certificate details.

phibstest 127.0.0.1 a

Checks the working state of configured authentication schemes against server, service, and user.

You can use the following options with *phibstest 127.0.0.1 a* :

Option	Description
authscheme	The authentication scheme, e.g., *msad*
server	The virtual server, e.g., *S1* (for logging only)
service	The configured Barracuda NextGen Firewall F-Series service, e.g., *VPN*
user	The username
password	The password for the user
metadirattr	MSAD/LDAP attributes to retrieve. Pipe-separated.

Example:

To test authentication, enter *phibstest 127.0.0.1 a*, followed by the authentication scheme, your virtual server, a service configured on the Barracuda NextGen Firewall F-Series, and the user, e.g.: *phibstest 127.0.0.1 a authscheme=msad server=S1 service=VPN user=tom password=tom123*

After a successful authentication check, the SSH console displays the details, e.g., as follows:

type=userauth sub=1098246068 id=2 ver=1 res=Success timeout=5: Authentication Ok

challengeid =
user = tom

If the authentication test fails, check the following log file for error messages: Box\Control\AuthService.

phibstest 127.0.0.1 p

This command is used for password management.

Note that executing this may change the passwords.

phibstest 127.0.0.1 e

Provides extended features for authentication checks, such as AD lookup.

You can use the following options with *phibstest 127.0.0.1 e* :

Option	Description
authscheme	The authentication scheme, e.g., *msad*
server	The virtual server, e.g., *S1* (for logging only)
service	The configured Barracuda NextGen Firewall F-Series service, e.g., *VPN*
user	The username
password	The password for the user
metadirattr	MSAD/LDAP attributes to retrieve. Pipe-separated.

phibstest 127.0.0.1 i

Provides user group information independent from authentication.

You can use the following options with *phibstest 127.0.0.1 i* :

Option	Description
server	The virtual server, e.g. , *S1* (for logging only)
service	The configured Barracuda NextGen Firewall F-Series service, e.g., *VPN*
user	The username (optional)
mail	The mail address (optional)

Example:

To get user group information without authentication, enter *phibstest 127.0.0.1 i* , followed by the authentication scheme, your virtual server, a service, and the user, e.g.: *phibstest 127.0.0.1 i authscheme=msad server=S1 service=VPN user=tom*

phibstest 127.0.0.1 l

Checks the working state of authentication against extended firewall login information.

You can use the following options with *phibstest 127.0.0.1 l* :

Option	Description
user	The username
uvpnuser	The VPN username

vpngroup	The VPN group
groups	User groups
peer	The Peer-IP
server	The virtual server, e.g. , *S1*
service	The configured Barracuda NextGen Firewall F-Series service, e.g., *VPN*
box	The Box name of the Barracuda unit
origin	Origin (one of HTTP, VPN, PROXY)
x509subject	The subject of the certificate
x509issuer	The certificate issuer
x509altname	The certificate subject altname
x509policy	The certificate policy
policyroles	Policy Roles

phibstest 127.0.0.1 o

Checks the working state of authentication against extended firewall logout information.

You can use the following options with *phibstest 127.0.0.1 o* :

Option	Description
user	Username
peer	Peer-IP
server	The virtual server, e.g. *S1*
service	The configured Barracuda NextGen Firewall F-Series service, e.g., *VPN*
origin	The origin (one of HTTP, VPN, PROXY)

phibstest 127.0.0.1 n

Checks the working state of authentication against firewall login information.

You can use the following options with *phibstest 127.0.0.1 n* :

Option	Description
peer	Peer IP
origin	The preferred origin (optional)

phibstest 127.0.0.1 f

Checks the working state of authentication against OCPF information.

You can use the following options with *phibstest 127.0.0.1 f* :

Option	Description
authscheme	The authentication scheme (defaults to 'ocsp')
ocspcert	The certificate to check (filename PEM-format only!)
ocspissuer	The root certificate (filename PEM-format only!)
ocspverifyexpl	The server certificate of OCSP server (filename PEM-format only!)
ocspverifyroot	The root certificate of server certificate of OCSP server (filename PEM-format only!)
ocspusessl	*0* or *1*
ocsphost	The OCSP server IP address
ocspport	The port of OCSP server

phibstest 127.0.0.1 v

Displays information about the certificate validation chain.

Type *phibstest 127.0.0.1 v certvalidatechain* to display a list of PEM encoded certificate files, delimited by commas, ordered from subcertificate to issuer.