

phibstest

<https://campus.barracuda.com/doc/73719755/>

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

In Barracuda Firewall 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 *phibscft* 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
<i>authscheme</i>	The authentication scheme, e.g., <i>msad</i>

<i>server</i>	The virtual server, e.g., <i>S1</i> (for logging only)
<i>service</i>	The configured Barracuda CloudGen Firewall service, e.g., <i>VPN</i>
<i>user</i>	The username
<i>password</i>	The password for the user
<i>metadirattr</i>	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 CloudGen Firewall, 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
<i>authscheme</i>	The authentication scheme, e.g., <i>msad</i>
<i>server</i>	The virtual server, e.g., <i>S1</i> (for logging only)
<i>service</i>	The configured Barracuda CloudGen Firewall service, e.g., <i>VPN</i>
<i>user</i>	The username
<i>password</i>	The password for the user

<i>metadirattr</i>	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
<i>server</i>	The virtual server, e.g. , <i>S1</i> (for logging only)
<i>service</i>	The configured Barracuda CloudGen Firewall service, e.g., <i>VPN</i>
<i>user</i>	The username (optional)
<i>mail</i>	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
<i>user</i>	The username
<i>uvpnuser</i>	The VPN username
<i>vpngroup</i>	The VPN group
<i>groups</i>	User groups
<i>peer</i>	The Peer-IP
<i>server</i>	The virtual server, e.g. , <i>S1</i>
<i>service</i>	The configured Barracuda CloudGen Firewall service, e.g., <i>VPN</i>
<i>box</i>	The Box name of the Barracuda unit
<i>origin</i>	Origin (one of HTTP, VPN, PROXY)
<i>x509subject</i>	The subject of the certificate
<i>x509issuer</i>	The certificate issuer
<i>x509altname</i>	The certificate subject altname

<i>x509policy</i>	The certificate policy
<i>policyroles</i>	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
<i>user</i>	Username
<i>peer</i>	Peer-IP
<i>server</i>	The virtual server, e.g. <i>S1</i>
<i>service</i>	The configured Barracuda CloudGen Firewall service, e.g., <i>VPN</i>
<i>origin</i>	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
<i>peer</i>	Peer IP
<i>origin</i>	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
<i>authscheme</i>	The authentication scheme (defaults to 'ocsp')
<i>ocspcert</i>	The certificate to check (filename PEM-format only!)
<i>ocspissuer</i>	The root certificate (filename PEM-format only!)
<i>ocspverifyexpl</i>	The server certificate of OCSP server (filename PEM-format only!)
<i>ocspverifyroot</i>	The root certificate of server certificate of OCSP server (filename PEM-format only!)
<i>ocspusessl</i>	0 or 1
<i>ocspghost</i>	The OCSP server IP address

<i>ocsport</i>	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.

phibstest 127.0.0.1 u

Clears the authentication cache.

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

Option	Description
<i>origin</i>	The origin pattern (one of HTTP, VPN, PROXY).
<i>peer</i>	The peer IP address pattern.
<i>server</i>	The virtual server name pattern, e.g. , <i>S1</i>
<i>service</i>	The configured Barracuda CloudGen Firewall service name pattern, e.g., <i>VPN</i>
<i>box</i>	The box name pattern.

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.