NAME

pam_yubico − Module for YubiKey authentication

SYNOPSIS

pam_yubico [...]

DESCRIPTION

The module is for authentication of YubiKeys, either with online validation of OTP, or offline validation with HMAC−SHA1 challenge−response.

OPTIONS

debug
Turns on debugging.

debug_file=*file*
File name to write debug to, the file must exist and be a regular file. Defaults to stdout.

mode=[*client*|*challenge−response*]
Set the mode of operation, client for OTP validation and challenge−response for challenge−response validation, client is the default.

authfile=*file*
Set the location of the file that holds the mappings of Yubikey token IDs to user names. The format is username:first_public_id:second_public_id:... default location of the file is $HOME/.yubico/authorized_yubikeys.

id=*id*
Set to your client identity.

key=*key*
Set to your client key in base64 format. The client key is also known as API key, and provides integrity in the communication between the client (you) and the validation server. If you want to get one for use with the default YubiCloud service, please go to https://upgrade.yubico.com/getapikey/

alwaysok
Set to enable all authentication attempts to succeed (aka presentation mode).

try_first_pass
Before prompting the user for their password, the module first tries the previous stacked module´s password in case that satisfies this module as well.

use_first_pass
The argument use_first_pass forces the module to use a previous stacked modules password and will never prompt the user − if no password is available or the password is not appropriate, the user will be denied access.

nullok
If set, don’t fail when there are no tokens declared for the user in the authorization mapping files or in LDAP. This can be used to make YubiKey authentication optional unless the user has associated tokens.

urllist=*list*
List of URL templates to be used. This is set by calling ykclient_set_url_bases. The list should be in the format: https://api1.example.com/wsapi/2.0/verify;https://api2.example.com/wsapi/2.0/verify

url=*url*
This option should not be used, please use the urllist option instead. Set the URL template to use, this is set by calling ykclient_set_url_template. The URL should be set in the format https://api.example.com/wsapi/2.0/verify?id=%d&otp=%s

capath=*path*
Specify the path where X509 certificates are stored. This is required if *https* or *ldaps* are used in *url* and *ldap_uri* respectively.

proxy=*proxy*
Specify a proxy to connect to the validation server. Valid schemes are http://, https://, socks4://, socks4a://, socks5:// or socks5h://. Socks5h asks the proxy to do the dns resolving. If no scheme or port is specified HTTP proxy port 1080 will be used. E.g. socks5h://user:pass@10.10.0.1:1080

verbose_otp
This argument is used to show the OTP (One Time Password) when it is entered, i.e. to enable terminal echo of entered characters. You are advised to not use this, if you are using two factor authentication because that will display your password on the screen. This requires the service using the PAM module to display custom fields. This option can not be used with OpenSSH.

ldap_uri=*uri*
Specify the LDAP server URI (e.g. ldap://localhost).

ldap_server=*server*
Specify the LDAP server host (default LDAP port is used). **Deprecated. Use** *ldap_uri* **instead.**

ldapdn=*dn*
The dn where the users are stored (eg: ou=users,dc=domain,dc=com). If *ldap_filter* is used this is the base from which the subtree search will be performed.

user_attr=*attr*
The LDAP attribute used to store user names (eg:cn).

yubi_attr=*attr*
The LDAP attribute used to store the Yubikey id.

yubi_attr_prefix=*prefix*
The prefix of the LDAP attribute's value, in case of a generic attribute, used to store several types of ids.

token_id_length=*length*
Length of ID prefixing the OTP (this is 12 if using the YubiCloud).

ldap_bind_user=*user*
The user to attempt a LDAP bind as.

ldap_bind_password=*password*
The password to use on LDAP bind.

ldap_filter=*filter*
An ldap filter to use for attempting to find the correct object in LDAP. In this string %u will be replaced with the username.

ldap_cacertfile=*cacertfile*
Ca certfile for the LDAP connection.

chalresp_path=*path*
Path of a system wide directory where challenge response files can be found for users. Default location is $HOME/.yubico/

EXAMPLES

auth sufficient pam_yubico.so id=16 debug

auth required pam_yubico.so mode=challenge−response

auth required pam_yubico.so id=16 ldap_uri=ldaps://ldap.example.com ldap_filter=(uid=%u) yubi_attr=yubiKeyId

FILES

$HOME/.yubico/authorized_yubikeys
If **authfile** is not set this file is used for the mapping between YubiKey public id and in *client* mode.

$HOME/.yubico/challenge, **$HOME/.yubico/challenge**−*serial_number*
If **chalresp_path** is not set these files are used to hold next challenge and expected response for the

user in *challenge−response* mode. If **chalresp_path** is set the filename will be username instead of challenge.

BUGS

Report yubico−pam bugs in the issue tracker: https://github.com/Yubico/yubico−pam/issues

SEE ALSO

ykpamcfg(1), **pam**(7)

The yubico−pam home page: https://developers.yubico.com/yubico−pam/

YubiKeys can be obtained from Yubico: http://www.yubico.com/