NAME

pam_sss − PAM module for SSSD

SYNOPSIS

pam_sss.so [*quiet*] [*forward_pass*] [*use_first_pass*] [*use_authtok*] [*retry=N*] [*ignore_unknown_user*] [*ignore_authinfo_unavail*] [*domains=X*] [*allow_missing_name*] [*prompt_always*] [*try_cert_auth*] [*require_cert_auth*]

DESCRIPTION

pam_sss.so is the PAM interface to the System Security Services daemon (SSSD). Errors and results are logged through **syslog(3)** with the LOG_AUTHPRIV facility.

OPTIONS

quiet

Suppress log messages for unknown users.

forward_pass

If **forward_pass** is set the entered password is put on the stack for other PAM modules to use.

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.

use_authtok

When password changing enforce the module to set the new password to the one provided by a previously stacked password module.

retry=N

If specified the user is asked another N times for a password if authentication fails. Default is 0.

Please note that this option might not work as expected if the application calling PAM handles the user dialog on its own. A typical example is **sshd** with **PasswordAuthentication**.

ignore_unknown_user

If this option is specified and the user does not exist, the PAM module will return PAM_IGNORE. This causes the PAM framework to ignore this module.

ignore_authinfo_unavail

Specifies that the PAM module should return PAM_IGNORE if it cannot contact the SSSD daemon. This causes the PAM framework to ignore this module.

domains

Allows the administrator to restrict the domains a particular PAM service is allowed to authenticate against. The format is a comma−separated list of SSSD domain names, as specified in the sssd.conf file.

NOTE: If this is used for a service not running as root user, e.g. a web−server, it must be used in conjunction with the “pam_trusted_users” and “pam_public_domains” options. Please see the **sssd.conf**(5) manual page for more information on these two PAM responder options.

allow_missing_name

The main purpose of this option is to let SSSD determine the user name based on additional information, e.g. the certificate from a Smartcard.

The current use case are login managers which can monitor a Smartcard reader for card events. In case a Smartcard is inserted the login manager will call a PAM stack which includes a line like

auth sufficient pam_sss.so allow_missing_name

In this case SSSD will try to determine the user name based on the content of the Smartcard, returns it to pam_sss which will finally put it on the PAM stack.

prompt_always
Always prompt the user for credentials. With this option credentials requested by other PAM modules, typically a password, will be ignored and pam_sss will prompt for credentials again. Based on the pre−auth reply by SSSD pam_sss might prompt for a password, a Smartcard PIN or other credentials.

try_cert_auth
Try to use certificate based authentication, i.e. authentication with a Smartcard or similar devices. If a Smartcard is available and the service is allowed for Smartcard authentication the user will be prompted for a PIN and the certificate based authentication will continue

If no Smartcard is available or certificate based authentication is not allowed for the current service PAM_AUTHINFO_UNAVAIL is returned.

require_cert_auth
Do certificate based authentication, i.e. authentication with a Smartcard or similar devices. If a Smartcard is not available the user will be prompted to insert one. SSSD will wait for a Smartcard until the timeout defined by p11_wait_for_card_timeout passed, please see **sssd.conf**(5) for details.

If no Smartcard is available after the timeout or certificate based authentication is not allowed for the current service PAM_AUTHINFO_UNAVAIL is returned.

MODULE TYPES PROVIDED

All module types (**account**, **auth**, **password** and **session**) are provided.

If SSSD's PAM responder is not running, e.g. if the PAM responder socket is not available, pam_sss will return PAM_USER_UNKNOWN when called as **account** module to avoid issues with users from other sources during access control.

RETURN VALUES

PAM_SUCCESS
The PAM operation finished successfully.

PAM_USER_UNKNOWN
The user is not known to the authentication service or the SSSD's PAM responder is not running.

PAM_AUTH_ERR
Authentication failure. Also, could be returned when there is a problem with getting the certificate.

PAM_PERM_DENIED
Permission denied. The SSSD log files may contain additional information about the error.

PAM_IGNORE
See options **ignore_unknown_user** and **ignore_authinfo_unavail**.

PAM_AUTHTOK_ERR
Unable to obtain the new authentication token. Also, could be returned when the user authenticates with certificates and multiple certificates are available, but the installed version of GDM does not support selection from multiple certificates.

PAM_AUTHINFO_UNAVAIL
Unable to access the authentication information. This might be due to a network or hardware failure.

PAM_BUF_ERR
A memory error occurred. Also, could be returned when options use_first_pass or use_authtok were set, but no password was found from the previously stacked PAM module.

PAM_SYSTEM_ERR
A system error occurred. The SSSD log files may contain additional information about the error.

PAM_CRED_ERR

Unable to set the credentials of the user.

PAM_CRED_INSUFFICIENT
The application does not have sufficient credentials to authenticate the user. For example, missing PIN during smartcard authentication or missing factor during two−factor authentication.

PAM_SERVICE_ERR
Error in service module.

PAM_NEW_AUTHTOK_REQD
The user's authentication token has expired.

PAM_ACCT_EXPIRED
The user account has expired.

PAM_SESSION_ERR
Unable to fetch IPA Desktop Profile rules or user info.

PAM_CRED_UNAVAIL
Unable to retrieve Kerberos user credentials.

PAM_NO_MODULE_DATA
No authentication method was found by Kerberos. This might happen if the user has a Smartcard assigned but the pkint plugin is not available on the client.

PAM_CONV_ERR
Conversation failure.

PAM_AUTHTOK_LOCK_BUSY
No KDC suitable for password change is available.

PAM_ABORT
Unknown PAM call.

PAM_MODULE_UNKNOWN
Unsupported PAM task or command.

PAM_BAD_ITEM
The authentication module cannot handle Smartcard credentials.

FILES

If a password reset by root fails, because the corresponding SSSD provider does not support password resets, an individual message can be displayed. This message can e.g. contain instructions about how to reset a password.

The message is read from the file pam_sss_pw_reset_message.LOC where LOC stands for a locale string returned by **setlocale**(3). If there is no matching file the content of pam_sss_pw_reset_message.txt is displayed. Root must be the owner of the files and only root may have read and write permissions while all other users must have only read permissions.

These files are searched in the directory /etc/sssd/customize/DOMAIN_NAME/. If no matching file is present a generic message is displayed.

SEE ALSO

sssd(8), **sssd.conf**(5), **sssd-ldap**(5), **sssd-krb5**(5), **sssd-simple**(5), **sssd-ipa**(5), **sssd-ad**(5), **sssd-files**(5), **sssd-sudo**(5), **sssd-session-recording**(5), **sss_cache**(8), **sss_debuglevel**(8), **sss_obfuscate**(8), **sss_seed**(8), **sssd_krb5_locator_plugin**(8), **sss_ssh_authorizedkeys**(8), **sss_ssh_knownhostsproxy**(8), **sssd-ifp**(5), **pam_sss**(8). **sss_rpcidmapd**(5) **sssd-systemtap**(5)

AUTHORS

The SSSD upstream − https://github.com/SSSD/sssd/