



Safeguard Authentication Services 6.0.1

Basic Authentication Walkthrough Guide

Copyright 2025 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal/trademark-information.aspx. All other trademarks are the property of their respective owners.

Legend

 **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

Safeguard Authentication Services Basic Authentication Walkthrough Guide
Updated - 28 May 2025, 20:54

For the most recent documents and product information, see [Online product documentation](#).

Contents

Introduction	1
Authenticating a password	2
About us	8
Contacting us	8
Technical support resources	8
Glossary	9

Introduction

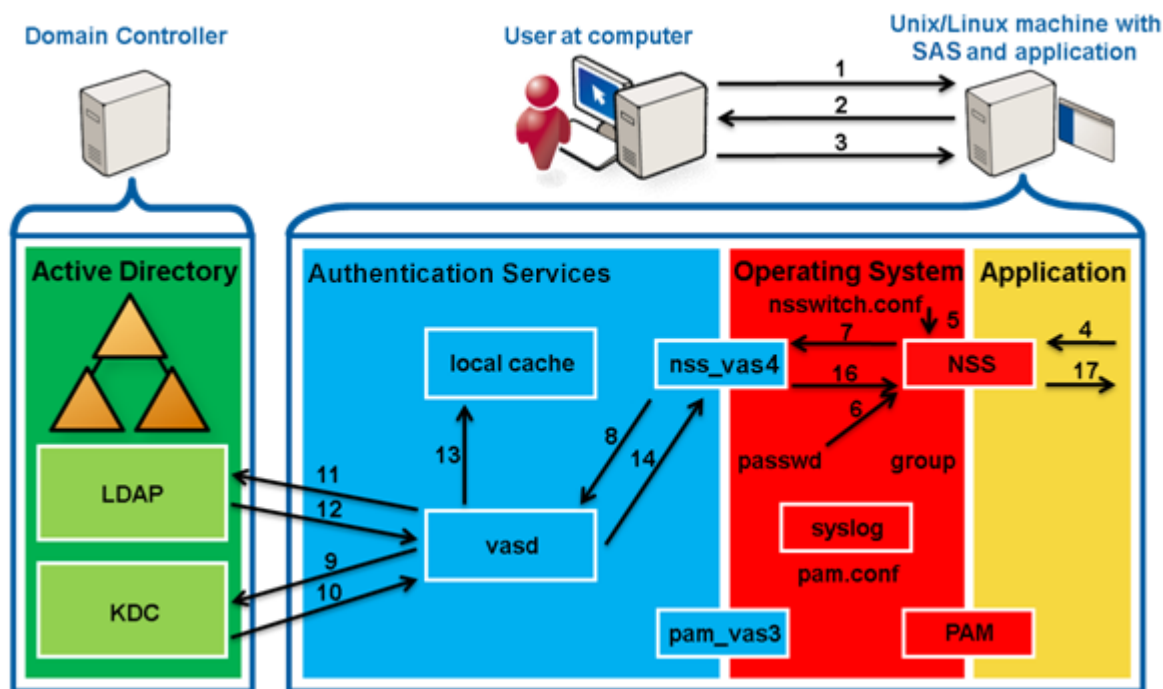
This document provides step-by-step instructions for authenticating a password for a normal Safeguard Authentication Services-enabled user through an ssh-like program onto a generic PAM/NSS using *nix system.

NOTE: This guide was last updated for Safeguard Authentication Services 6.0.1. Previous versions, as of version 3.5.2, work similarly with minor differences. For example, in very old versions, the Kerberos ticket request was done by the PAM module directly without involving the vasd process.

Authenticating a password

You can authenticate a password by performing the following steps.

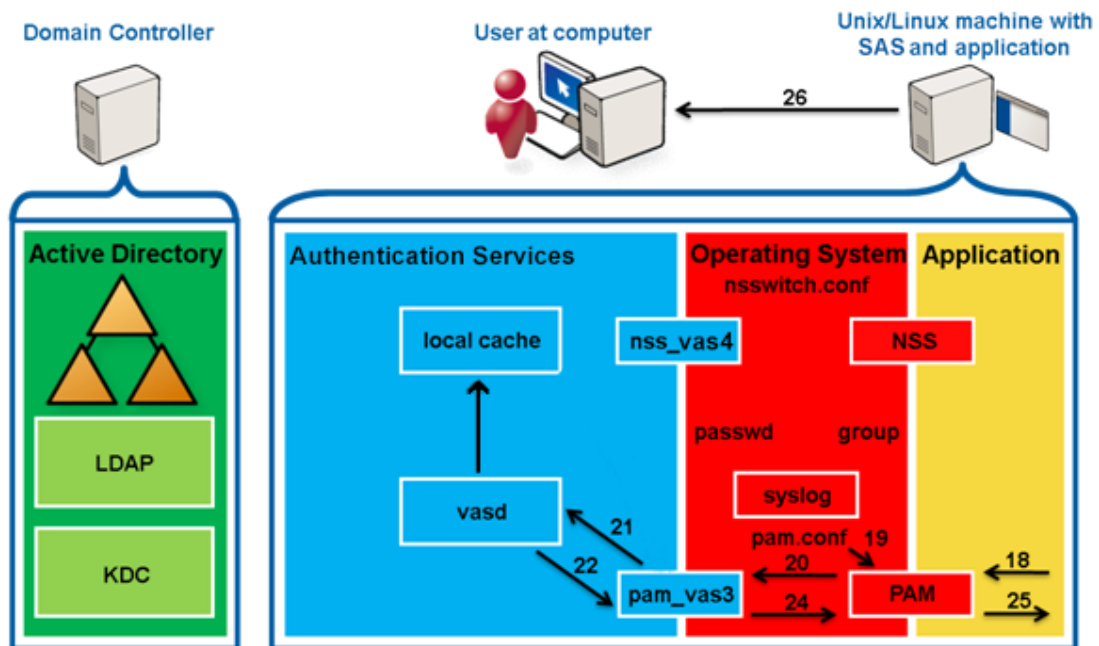
NOTE: This example assumes the system is configured using default settings, Safeguard Authentication Services is configured from a default install/join; and, the user is Safeguard Authentication Services-enabled with a password.



To authenticate a password

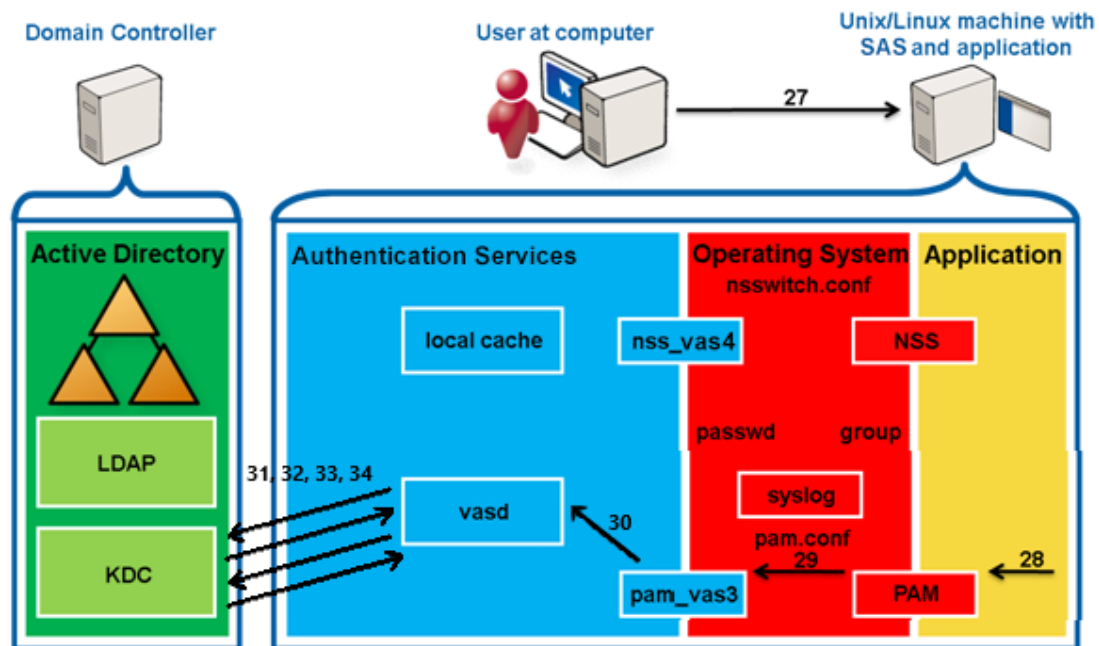
1. The user opens a secure connection with the application.
2. The application sends a prompt for the user name.
3. The user sends their user name to the application.
4. The application queries NSS (using `getpwnam`) about the user.
5. NSS reads `/etc/nsswitch.conf` and processes the `passwd: files vas4` entry.

6. NSS queries `nss_files`, which reads `/etc/passwd`, and returns `ENOENT` because no matching user entry is found.
 7. NSS queries `nss_vas4`.
 8. `nss_vas4` sends an IPC to `vasd` to update the user.
 9. `vasd` uses credentials from the keytab to request a ticket to talk to the LDAP/<DC> service in Active Directory.
 10. AD KDC returns the requested service ticket.
 11. `vasd` queries AD LDAP for the user information.
 12. The user's information is returned.
 13. `vasd` writes the user information into the local cache.
 14. `vasd` returns the information about the user to `vas_nss`.
 15. `nss_vas4` forms the data into a `passwd-stlye` response.
 16. `nss_vas4` returns the `passwd` info to NSS.
- NOTE:** There is no password hash since `vasd` does not have access to that unless you are using a legacy auth setup.
17. NSS returns the information to the application.



18. The application calls PAM through `pam_start` then `pam_authenticate`.
19. PAM reads `/etc/pam.conf` or the config file relevant to the service from `/etc/pam.d` and processes the `pam_vas3` entry.
20. PAM queries `pam_vas3`.
21. `pam_vas3` asks `vasd` for the user info.

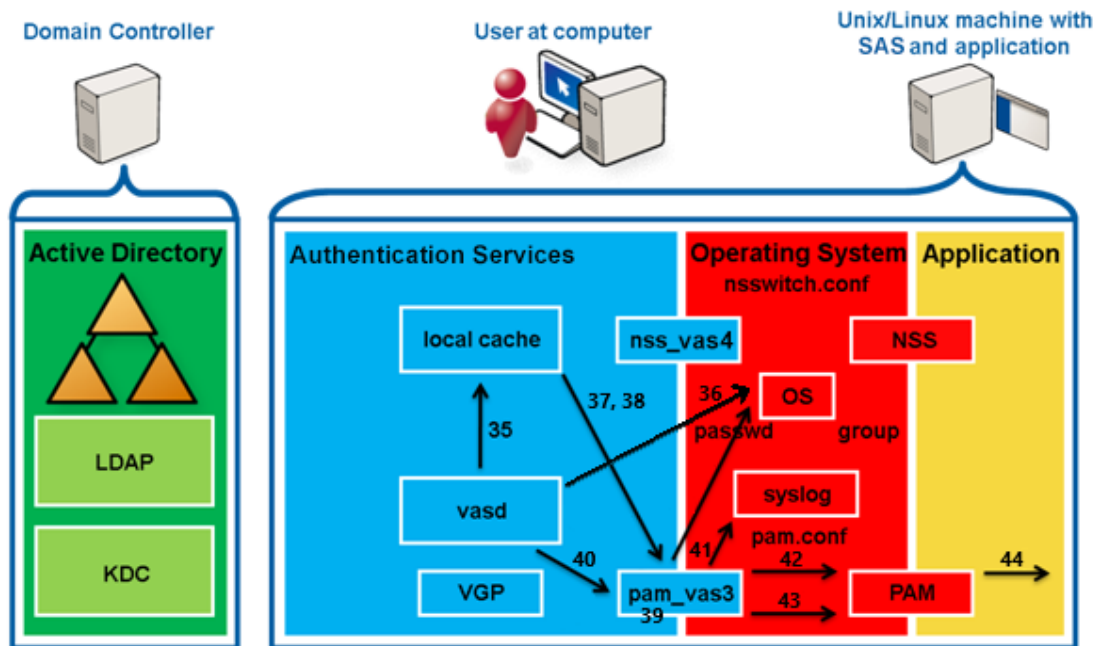
22. vasd returns the user info from the local cache.
23. The user is a Safeguard Authentication Services user, therefore pam_vas3 will continue to attempt to authenticate the user instead of ignoring and letting the PAM stack fall past pam_vas3.
24. pam_vas3 returns a request for credentials (password) using PAM conversations (including the prompt to use).
25. PAM returns the request to the requesting application.
26. The application presents the user with the prompt for their password. (If the application is PAM conversation-aware, it uses the prompt pam_vas3 set).



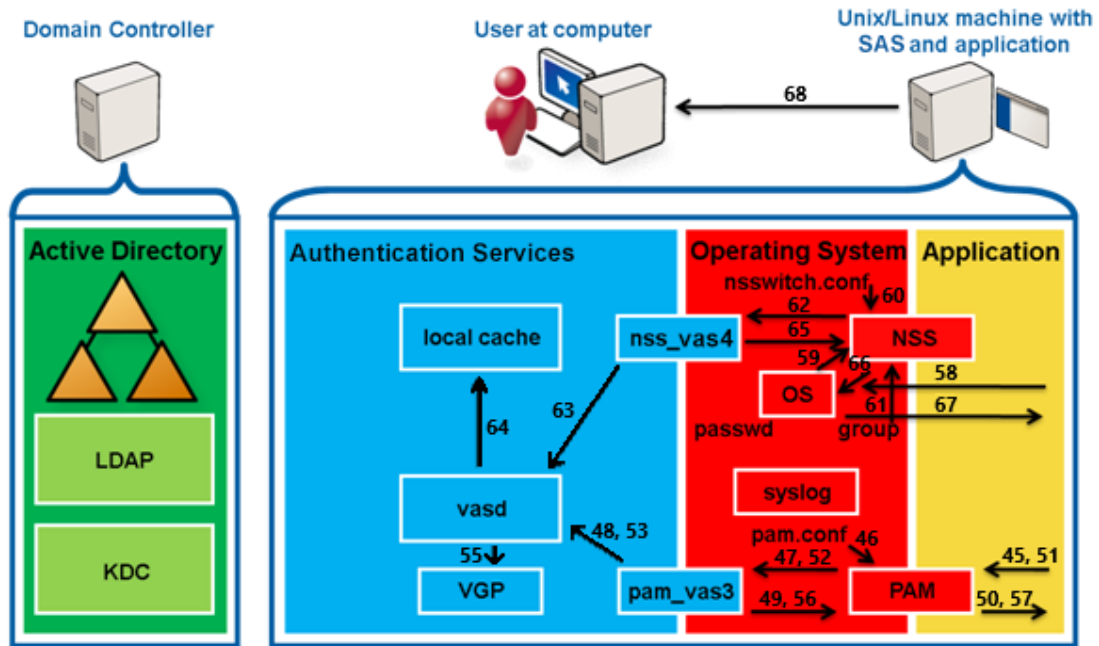
27. The user enters their password.
28. The application passes the password to PAM.
29. The password is passed back to pam_vas3 through the conversation mechanism.
30. pam_vas3 sends the password to vasd through a secure IPC asking for authorization.
31. vasd requests a Kerberos TGT (Ticket Granting Ticket) for the user using a user key derived from the user's samaccountname@realm and the supplied password.

NOTE: Kerberos does not actually use passwords; it uses keys derived from them for security.
32. AD KDC returns the TGT (AS-REP).
33. vasd decrypts the response using the user key, obtaining a TGT and Session key. TGT and Session key are used to request a service ticket (TGS-REQ) from the AD KDC for the user to authenticate against the host/ (local machine) service.

34. The AD KDC returns the service ticket (TGS-REP), which is decrypted using both the Session key (user portion) and the host/ key (service portion) that is stored in the host.keytab file.



35. vasd processes the payload of the service portion of the service ticket, which is the PAC (Privileged Access Certificate), a list of SIDs of groups of which the user is a member and modifies the local cache to set the current group memberships.
36. vasd creates the user's home directory if needed.
37. vasd reads the user account information from the local cache. It verifies the user is within any configured logon hours and has a valid shell (not /bin/false in AD).
38. vasd verifies the user's group membership information and confirms that the user has access based on any configured access control.
39. vasd performs UID and GID conflict checking.
40. vasd returns success to pam_vas3.
41. pam_vas3 writes a syslog entry that the authentication succeeded.
42. pam_vas3 sets a PAM stack variable to note that it has already processed the above.
43. pam_vas3 pam_authenticate returns PAM_SUCCESS.
44. Because the pam_vas3 entry is configured with sufficient, PAM_SUCCESS is returned to the querying application, ignoring the rest of the PAM stack.



45. The application calls PAM through `pam_setcred` and `PAM_ESTABLISHED_CRED`.
46. PAM reads `/etc/pam.conf` and processes the `pam_vas3` entry.
47. PAM queries `pam_vas3` for `pam_sm_setcred`.
48. `pam_vas3` asks `vasd` to store the user's TGT and host/service ticket a local file-based cache for the user to use again if desired.
49. `pam_vas3` returns `PAM_SUCCESS`.
50. PAM returns `PAM_SUCCESS` to the application for both calls.
51. Similarly, the application calls PAM through `pam_open_session`.
52. PAM queries `pam_vas3`.
53. `pam_vas3` asks `vasd` through the IPC to create a login session for the user.
54. `vasd` fills the `~<user>/.vas_logon_server` file with the server name.
55. `vasd` runs VGP to apply any user policies if configured so.
56. `pam_vas3` returns `PAM_SUCCESS` to PAM.
57. PAM returns `PAM_SUCCESS` to the application.
58. The application starts the user's shell, which then sets up their environment.
59. The OS/shell calls NSS `getgroups` for the user's group memberships.
60. NSS reads `/etc/nsswitch.conf` and processes the `group: files vas4` entry.
61. NSS queries `nss_files`, which reads `etc/group` and adds no groups if no local groups contain the user.
62. NSS queries `nss_vas4`.
63. `nss_vas4` queries `vasd` to compute the user's group memberships.

64. vasd reads the group memberships from the local cache and returns them.
65. nss_vas4 returns the memberships to NSS.
66. The shell uses the groups to set the process space group memberships.
67. The OS presents the shell to the application.
68. The application presents the shell to the user, and they are now logged in.

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Glossary
