



Set up SAML authentication

System Manager Classic

NetApp
December 09, 2021

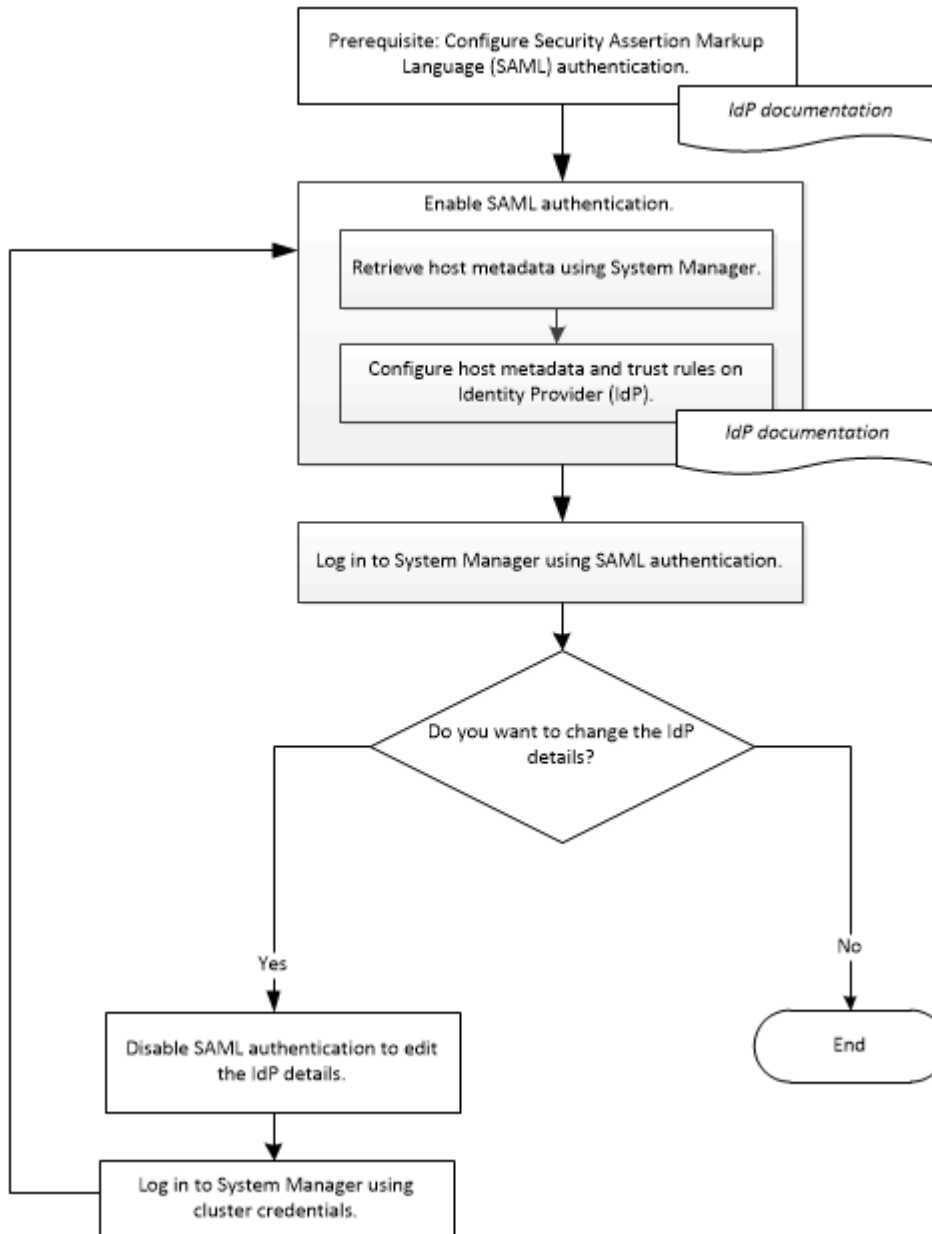
This PDF was generated from https://docs.netapp.com/us-en/ontap-sm-classic/online-help-96-97/task_enabling_saml_authentication.html on December 09, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Setting up SAML authentication 1
 - Enabling SAML authentication 1
 - Disabling SAML authentication 2

Setting up SAML authentication

You can set up Security Assertion Markup Language (SAML) authentication so that remote users are authenticated through a secure identity provider (IdP) before they log in to System Manager.



Enabling SAML authentication

You can use System Manager to configure Security Assertion Markup Language (SAML) authentication so that remote users can log in by using a secure identity provider (IdP).

Before you begin

- The IdP that you plan to use for remote authentication must be configured.



See the documentation that is provided by the IdP that you have configured.

- You must have the URI of the IdP.

About this task

The IdPs that have been validated with System Manager are Shibboleth and Active Directory Federation Services.



After SAML authentication is enabled, only remote users can access the System Manager GUI. Local users cannot access the System Manager GUI after SAML authentication is enabled.

Steps

1. Click **Configuration > Cluster > Authentication**.
2. Select the **Enable SAML authentication** check box.
3. Configure System Manager to use SAML authentication:
 - a. Enter the URI of the IdP.
 - b. Enter the IP address of the host system.
 - c. If required, change the host system certificate.
4. Click **Retrieve Host Metadata** to retrieve the host URI and host metadata information.
5. Copy the host URI or host metadata details, access your IdP, and then specify the host URI or host metadata details and the trust rules in the IdP window.



See the documentation that is provided by the IdP that you have configured.

6. Click **Save**.

The IdP login window is displayed.

7. Log in to System Manager by using the IdP login window.

After the IdP is configured, if the user tries to log in by using the fully qualified domain name (FQDN), IPv6, or a cluster management LIF, then the system automatically changes the IP address to the IP address of the host system that was specified during the IdP configuration.

Related information

[Accessing a cluster by using the ONTAP System Manager browser-based graphic interface](#)

Disabling SAML authentication

You can disable Security Assertion Markup Language (SAML) authentication if you want to disable remote access to System Manager, or to edit the SAML configuration.

About this task

Disabling SAML authentication does not delete SAML configuration.

Steps

1. Click **Configuration > Cluster > Authentication**.
2. Clear the **Enable SAML authentication** check box.
3. Click **Save**.

System Manager restarts.

4. Log in to System Manager by using the cluster credentials.

Related information

[Accessing a cluster by using the ONTAP System Manager browser-based graphic interface](#)

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.