Configure simpleSAMLphp to Request Multi-Factor Authentication (Duo MFA)

Introduction

The University of California, San Francisco uses Duo MFA to implement multi-factor authentication for certain applications and users. Multi-factor authentication improves the security of a resource by requiring more than just a username and password in order to gain access to a resource. Check out this article to learn more about Duo MFA.

The MyAccess single-sign-on system is integrated with the Duo MFA system. However, it does not require users to use multi-factor authentication unless an application requests it. Applications can request that the MyAccess SSO system require the additional security layer of a MFA login by changing parts of the SAML Request it sends to the MyAccess Identity Provider (IdP). More specifically, the SAML Request must include an "AuthnContextClassRef" element with a value of "https://refeds.org/profile/mfa", which is defined by the REFEDS (Research and Education FEDerationS) group. Read up on the REFEDS MFA assurance profile and the associated specifications and assumptions for more details.

This article is only intended for the simpleSAMLphp software version 1.6 or later when used as a SAML SP.

Before You Begin

Before you begin, you must have a working simpleSAMLphp configuration that is already integrated with the MyAccess single-sign-on login system. See the installation and configuration instructions for more setup details.

Edit the simpleSAMLphp Configuration

See the most up-to-date simpleSAMLphp configuration guide for details on how to change the "AuthnContextClassRef" that is sent to the MyAccess Identity Provider in the SAML Request. The value of the "AuthnContextClassRef" must be "https://refeds.org/profile/mfa".

Important Notes

- **If an application requests multi-factor authentication, then ALL users who use MyAccess to login to that application must use Duo MFA** to gain access to that application. It's not possible to exempt some users from using MFA while requiring MFA for other users.
- **Duo MFA uses the username that the user typed into the MyAccess login page to process multi-factor authentication.** If users use a username to login to MyAccess that is not already enrolled into Duo MFA, they'll be denied access to your application.

  EXAMPLE: Let's say you're enrolled in the Duo MFA system with the "jdoe" Active Directory username, but you usually login to MyAccess with your old SF ID of "SF123456". If you login to MyAccess using your SF123456 username and associated password, then attempt to access the above application protected by the simpleSAMLphp software that requests multi-factor authentication, you'll be denied access at during the Duo authentication process, even though you are already enrolled into Duo with your "jdoe" AD account. If you want to use Duo MFA with your AD account, you must login to MyAccess with the same "jdoe" username and password before going to a MFA protected SSO application.