Table of contents

Objectives

The general idea is, users account information is stored and managed in the Microsoft Active Directory (AD). We do not want to create or manage users in Tiki.

The Tiki site is : https://tikisite.company.com
The AD realm (domain?) is: TEAM.COMPANY.LOCAL

Note:
We do have groups in Tiki and putting users into groups in Tiki is still done manually in Tiki.

Single Log On

SLO means that users will log into Tiki with their AD credentials. No automatic login will happen (this is SSO, see later).
This is done using LDAP as login mode.
(to be expanded with an example)

Single Sign On

SSO means that users don't need to enter their credentials when they browse https://tiki.company.com

This only works for users using browsers which are configured with the correct credentials. The others will still be able to log in.

Steps

1. Get SLO working (see above)
2. Prepare webserver environment
3. Prepare Active Directory
4. Enable kerberos in apache
5. Configure browsers
6. Debugging and setup

1.1.1. Get SLO working (see above)

1.1.2. Prepare webserver environment

1.1.3. Prepare Active Directory

1.1.4. Enable kerberos in apache

<Directory /var/www/virtual/tikisite> Options +Indexes +FollowSymLinks -IncludesNOExec AllowOverride All # Require all granted AuthType Kerberos AuthName "Login Kerberos" KrbAuthRealms TEAM.COMPANY.LOCAL KrbMethodNegotiate on KrbMethodK5Passwd on KrbServiceName Any Krb5Keytab /etc/httpd/conf.d/intranet-sso-user.http.keytab KrbSaveCredentials on KrbVerifyKDC on KrbLocalUserMapping On Require valid-user </Directory>

1.1.5. Configure browsers

1.1.6. Debugging and setup