{%- from "apache/map.jinja" import server with context %}

{%- if auth.engine == 'basic' %}

AuthType Basic

{%- if auth.htpasswd is defined %}

AuthUserFile {{ server.htpasswd\_dir }}/{{ auth.htpasswd }}

{%- else %}

AuthUserFile {{ server.htpasswd\_dir }}/htpasswd

{%- endif %}

{%- elif auth.engine == 'kerberos' %}

AuthType Kerberos

KrbMethodNegotiate {% if auth.kerberos.get("method", {}).get("negotiate", True) %}on{% else %}off{% endif %}

KrbMethodK5Passwd {% if auth.kerberos.get("method", {}).get("k5passwd", True) %}on{% else %}off{% endif %}

KrbServiceName {{ auth.kerberos.get("service", "HTTP") }}

KrbAuthRealms {{ auth.kerberos.realms|join(' ') }}

Krb5KeyTab {{ auth.kerberos.get("keytab", "/etc/apache2/ipa.keytab") }}

KrbSaveCredentials on

#KrbConstrainedDelegation on

# Ensure X-Forwarded-User is correctly set

RequestHeader unset X-Forwarded-User

RewriteEngine On

RewriteCond %{LA-U:REMOTE\_USER} (.+)@(.+)

RewriteRule .\* - [E=RU:%1,NS]

RequestHeader set X-Forwarded-User %{RU}e

{%- if auth.ldap is defined %}

{%- if auth.ldap.get("mech", "basic") == "GSSAPI" %}

# Not supported without patching, see:

# https://bz.apache.org/bugzilla/show\_bug.cgi?id=55178

AuthLDAPBindSASLMech {{ auth.ldap.get("mech", "GSSAPI") }}

{%- if auth.ldap.interact is defined %}

AuthLDAPBindSASLInteract "{{ auth.ldap.interact }}"

{%- else %}

AuthLDAPBindSASLInteract "/usr/bin/kinit -k -t {{ auth.kerberos.get("keytab", "/etc/apache2/ipa.keytab") }} {{ auth.kerberos.get("service", "HTTP") }}/{{ site.host.name }}"

{%- endif %}

{%- else %}

AuthLDAPBindDN "{{ auth.ldap.binddn }}

AuthLDAPBindPassword "{{ auth.ldap.password }}

{%- endif %}

AuthLDAPURL "{{ auth.ldap.url }}"

{%- endif %}

{%- endif %}

{%- if auth.engine == "none" %}

AuthType None

{%- else %}

AuthName "{{ auth.get("name", "Authentication required") }}"

{%- endif %}

{%- if auth.require is defined %}

{%- for require in auth.require %}

Require {{ require }}

{%- endfor %}

{%- else %}

Require valid-user

{%- endif %}