```
# Increase buffer size for large headers
# This is needed only if you get 'upstream sent too big header while reading response
# header from upstream' error when trying to access an application protected by goauthentik
proxy_buffers 8 16k;
proxy_buffer_size 32k;

# Make sure not to redirect traffic to a port 4443
port_in_redirect off;

location / {
    # Put your proxy_pass to your application here
    proxy_pass          $forward_scheme://$server:$port;
    # Set any other headers your application might need
    # proxy_set_header Host $host;
    # proxy_set_header ...

    ##############################
    # authentik-specific config
    ##############################
    auth_request      /outpost.goauthentik.io/auth/nginx;
    error_page        401 = @goauthentik_proxy_signin;
    auth_request_set $auth_cookie $upstream_http_set_cookie;
    add_header        Set-Cookie $auth_cookie;

    # translate headers from the outposts back to the actual upstream
    auth_request_set $authentik_username $upstream_http_x_authentik_username;
    auth_request_set $authentik_groups $upstream_http_x_authentik_groups;
    auth_request_set $authentik_email $upstream_http_x_authentik_email;
    auth_request_set $authentik_name $upstream_http_x_authentik_name;
    auth_request_set $authentik_uid $upstream_http_x_authentik_uid;

    proxy_set_header X-authentik-username $authentik_username;
    proxy_set_header X-authentik-groups $authentik_groups;
    proxy_set_header X-authentik-email $authentik_email;
    proxy_set_header X-authentik-name $authentik_name;
    proxy_set_header X-authentik-uid $authentik_uid;
}

# all requests to /outpost.goauthentik.io must be accessible without authentication
location /outpost.goauthentik.io {
    proxy_pass              http://0.0.0.0:3001/outpost.goauthentik.io;
    # ensure the host of this vserver matches your external URL you've configured
    # in authentik
    proxy_set_header        Host $host;
    proxy_set_header        X-Original-URL $scheme://$http_host$request_uri;
    add_header              Set-Cookie $auth_cookie;
    auth_request_set        $auth_cookie $upstream_http_set_cookie;
    proxy_pass_request_body off;
    proxy_set_header        Content-Length "";
}

# Special location for when the /auth endpoint returns a 401,
# redirect to the /start URL which initiates SSO
location @goauthentik_proxy_signin {
    internal;
    add_header Set-Cookie $auth_cookie;
    return 302 /outpost.goauthentik.io/start?rd=$request_uri;
    # For domain level, use the below error_page to redirect to your authentik server with the full redirect path
    # return 302 https://authentik.company/outpost.goauthentik.io/start?rd=$scheme://$http_host$request_uri;
}
```

Konfiguration der Puffergrößen für den Header mit der Fehlermeldung zu verhindern

Portkonfiguration: Portweiterleitung in URLs ist deaktiviert

Standortkonfiguration mit **/location**: mit **proxy_pass** wird auf die zu schützende Anwendung gesetzt

Authentifizierungsanfrage an den Standort stellen

extrahiert Informationen aus den Antwort-Headern, die vom Authentik-Server erhalten wurden

setzt HTTP-Anfrageheader, die die aus Authentik erhaltenen Informationen enthalten und werden an die Anwendung übergeben

Standortblock für Anfragen an **/outpost.goauthentik.io**, die direkt zur Authentik Outputs umgeleitet werden und demonstrationsweise unter der ip **0.0.0.0.3001** läuft

wenn eine 401 (unbefugt)-Antwort vom Endpunkt empfangen wird, erfolgt eine Weiterleitung zur **/start**-URL