# EnterpriseAlert® 9

## Mobile App DMZ Preauthentication HTTP Flows

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

# 1 HTTP REQUEST FLOW WITH AUTHENTENTICATION IN DMZ

This document contains HTTP flows that apply when the Enterprise Alert mobile app communicates with its backend API in the following setup:

- Access to the backend API is protected with a reverse proxy in the DMZ that pre-authenticates acess
- DMZ proxy has OAuth2 capabilities
- DMZ proxy is integrated with an OAuth2 identity system, in this document this system is ADFS

## 1.1 Required DMZ Reverse Proxy Routes

The table below indicates required routes in the Proxy in the DMZ, in oder to be able to access the EA mobile API and to be able to authenticate clients in the DMZ.

The first rule must not enforce any authentication because it allows users to authenticate on your identity system (e.g. ADFS). All other routes may require that authentication. The second route represents the EA Mobile API to be used by the EA Mobile app.

| Public URL | Internal URL | Auth Type |
|---|---|---|
| https://adfs.enterprisealert.com/adfs/ | https://adfs.domain.local/adfs/ | Pass through |
| https://mobile.enterprisealert.com/eamobileapi/ | https://ea.domain.local/sts/ | ADFS / OAuth2 |

## 1.2 Full request flow

The following HTTP request/response flow is performed by the EA Mobile App from the very start until it is authenticated and could access ANY endpoint/controller on the EA Mobile API, i.e. any url path behind the second rule above.




PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

### 1.2.1 Request1

| Source | EA Mobile App |
|---|---|
| Destination | EA Mobile API |
| Respose By | DMZ Reverse Proxy (e.g. WAP) |
| Request | |

```
GET https://mobile.enterprisealert.com/eamobileapi/api/version HTTP/1.1
Host: mobile.enterprisealert.com
Connection: keep-alive
```

Response

```
HTTP/1.1 401
Content-Length: 0
WWW-Authenticate: Bearer
authorization_uri=https://adfs.enterprisealert.com/adfs/oauth2/authorize
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 22 Jul 2020 16:36:04 GMT
```

| Remarks | App attemps to get down to an information endpoint on the EA Mobile API. That is supposed to fail, because that request is unauthenticated. It does not contain any authentication token or the Authentication header itself is missing.<br><br>DMZ proxy rejects that request and indicates to the client where to obtain the token from in the "WWW-Authenticate" header. In that header, the authorization endpoint of ADFS must be present.<br><br>Reponse Code MUST BE 401. If the response is a 307 (Temprary redirect) to the ADFS login page itself, the EA mobile app will crash because it cannot digest HTML in the response on that REST API endpoint. It is expectes JSON or auth instructions in the headers.<br><br>If WAP does not return 401 on that route, the according application that represents the route must be enabled/flagged for OAuth2 with that PowerShell:<br><br>Set-WebApplicationProxyApplication -ID <WAP APP ID> -UseOAuthAuthentication |
|---|---|




PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

### 1.2.2 Request2

| Source | EA Mobile App via Mobile OS Browser Control |
|---|---|
| Destination | ADFS |
| Respose By | ADFS *via DMZ Reverse Proxy (e.g. WAP)* |

Request

```
GET https://adfs.enterprisealert.com/adfs/oauth2/authorize?
resource=urn%3Aderdack.enterprisealert.mobileapi&
response_type=code&
client_id=CFA89266-483F-448F-AFA7-243BEFD6304E&
redirect_uri=eaapp%3A%2F%2Fcom.derdack.enterprisealert HTTP/1.1
Host: adfs.enterprisealert.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
HTTP/1.1 302 Found
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8,text/html; charset=utf-8
Expires: -1
Location: eaapp://com.derdack.enterprisealert/?code=bZSrP9GYbEiYhm-vKfx6iA.AIrH8lwu2A
gsAIpfbHuEjZKBGMQ.XHrTOAJwIJtX86irkXfQQOOFM7pU4eyr3rtCSdOFuXs5f57kjqauNQ166uOZDXhHxeZ
BWqzw9Fy5_iH7wA_357YWDOO8jijYPDDg4Z-9syLnxevqrJb_1u4ijTPwp7-b-a9gdPaMy61kGUnqeW49MENJ
DBUpaOOUtx-mJcMx3Dc-yYIFHc9NooZVw0yANWjIpphnHRrT8lZRp88IA5ap9VPt9-p2XS9C2Ppgzqpxe4Bg8
FSVqeXxTOalsuUWUDI8sRHroPOEpDLA3qPMDRmQ3ChOBS6iDnkgmbnSUxCgvH2EEOtScYV7nKKyRmTaX__W1u
aeexLmkkzKJ7KV9omuZQ
Server: Microsoft-HTTPAPI/2.0 Microsoft-HTTPAPI/2.0
P3P: CP="ADFS doesn't have P3P policy, please contact your site's admin for more details."
Set-Cookie: MSISAuthenticated=MjIuMDcuMjAyMCAxNjozMzoyMQ==; path=/adfs; HttpOnly; Secure;
SameSite=None
Set-Cookie: MSISLoopDetectionCookie=MjAyMC0wNy0yMjoxNjozMzoyMVpcMQ==; path=/adfs;
HttpOnly; Secure; SameSite=None
Date: Wed, 22 Jul 2020 16:33:32 GMT
```

| Remarks | The EA mobile app compiles a GET request which is based on the URL in the WWW-Authenticate header and internal hard codings for OAuth2 Protocol. This data is added as request parameters to the request URI (see in bold). <u>These values cannot be configured in EnterpriseAlert.</u><br><br>The URL is passed to an OS browser control, any credential entry is transparent / abstracted from the mobile app. It cannot inspect these user inputs.<br><br>If the authentication by the user was successful, the OS passes the 302 Redirect back to the app, when the URI in the Location header matches what the app has registered with the OS.<br><br>The app then extracts the OAuth2 authorization code that was issued by ADFS. It will redeem that code and obtain a token in the next request. |
|---|---|




PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

### 1.2.3 Request3

| Source | EA Mobile App |
|---|---|
| Destination | ADFS |
| Respose By | ADFS *via DMZ Reverse Proxy (e.g. WAP)* |
| Request | |

```
POST https://adfs.enterprisealert.com/adfs/oauth2/token HTTP/1.1
Host: adfs.enterprisealert.com
Accept: application/json
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 579
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

code=bZSrP9GYbEiYhm-
vKfx6iA.AIrH8lwu2AgsAIpfbHuEjZKBGMQ.XHrTOAJwIJtX86irkXfQQO0FM7pU4eyr3rt
CSdOFuXs5f57kjqauNQ166u0ZDXhHxeZBWqzw9Fy5_iH7wA_357YWDOO8jijYPDDg4Z-
9syLnxevqrJb_1u4ijTPwp7
ba9gdPaMy61kGUnqeW49MENJDBUpaOOUtx-mJcMx3Dc-
yYIFHc9NooZVwOyANWjIpphnHRrT8lZRp88IA5ap9VPt9p2
XS9C2Ppgzqpxe4Bg8FSVqeXxTOalsuUWUDI8sRHroPOEpDLA3qPMDRmQ3ChOBS6iDnkgmbnSUxCgvH2EEOtScYV7
nKKyRmTaX__W1uaeexLmkkzKJ7KV9omuZQ&
grant_type=authorization_code&
client_id=CFA89266-483F-448F-AFA7-243BEFD6304E&
resource=urn%3Aderdack.enterprisealert.mobileapi&
redirect_uri=eaapp%3A%2F%2Fcom.derdack.enterprisealert
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store
Pragma: no-cache
Content-Length: 8038
Content-Type: application/json;charset=UTF-8
Server: Microsoft-HTTPAPI/2.0 Microsoft-HTTPAPI/2.0
Date: Wed, 22 Jul 2020 16:34:15 GMT

{
    "access_token": "eyJwcm94eV90b2tlbiI6ImV5SjBlWEFpT2lKS1YxUW...",
    "token_type": "bearer",
    "expires_in": 1800,
    "refresh_token": "PX5mshBE8WlQsJEKmkCnyqvklm-a_mtmRfnEFRQ5Z-..."
}
```

| Remarks | The EA mobile app compiles a POST request that sends form data. The URL to the token endpoint is created via hard codings. Note the content type and how the OAuth2 parameters including the obtained authorization code are formatted and sent to the server.<br><br>The server issues an access token and a refresh token. Response body must be in JSON format.<br><br>If no refresh token is contained in the response from ADFS, the configuration in ADFS may need to be adjusted. It may only issue |
|---|---|

| | |
|---|---|
| | refresh tokens when there is a certain trust level for the client with ID CFA89266-483F-448F-AFA7-243BEFD6304E<br><br>If only an access token is issued, mobile users may have to re-login quite frequently!<br><br>The app extracts the tokens and uses them in all subsequent requests in the Authorization header as Bearer tokens.<br><br>Security is enforced as the DMZ proxy is supposed to reject all requests without such a valid header token, except the request is destinated to the identity provider (ADFS) itself. |




PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

### 1.2.4 Request4

| Source | EA Mobile App |
|---|---|
| Destination | EA Mobile API |
| Respose By | EA Mobile API *via DMZ Reverse Proxy (e.g. WAP)* |
| Request | |

```
GET https://mobile.enterprisealert.com/eamobileapi/api/users/me HTTP/1.1
Host: mobile.enterprisealert.com
Connection: keep-alive
Accept: application/json
Authorization: Bearer eyJwcm94eV9Ob2tlbiI6ImV5SjBlWEFpT2lKS1YxUWlMQOpoYkdjaU9pSlN...
```

Response

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 33
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/7.5 Microsoft-HTTPAPI/2.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 23 Jul 2020 09:32:37 GMT

{
    "id": 3547,
    "name": "Rene Bormann"
}
```

| Remarks | App makes use of the obtained token for the first time on the Enterprise Alert mobile API.<br><br>It reads details of the current user. In this and all subsequent API requests, it adds the current access token in the Authorization header. |
|---|---|

### 1.3 Remarks

The above traffic was reverse engineered with browser tools. Headers (e.g. Cookie, Set-Cookie, User-Agent) may have been removed or altered. The displayed headers may not be identical with what the mobile app sends.

If the deployed DMZ proxy is not WAP but another system reverse proxy, it is unknown how that system validates the provided access tokes in the Authorization header.

"Validates that the edge token signature is from the federation service that is configured in the Web Application Proxy configuration.", more details can be found here:

https://docs.microsoft.com/en-us/windows-server/remote/remote-access/web-application-proxy/publishing-applications-using-ad-fs-preauthentication

Signing is based on a Token Signing certificate that ADFS uses to sign tokens. The public key of that certificate must be known in the used DMZ proxy that has OAuth2 capabilites.

Dedack recommends the use of WAP as DMZ proxy whenever possible.




PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

## 2 ABOUT

Derdack is an independent software vendor offering advanced enterprise notification and rapid response software. Derdack's premium products help clients to automate alert notifications and to communication-enable business processes and applications. Derdack is recognized for its intuitive yet inspiring software products and has customers in over 50 countries worldwide. Derdack was founded in 1999 and its corporate headquarters are in Berlin, Germany.

## 3 FURTHER INFORMATION

Please visit www.derdack.com or:

| | |
|---|---|
| Corporate Blog: | https://www.derdack.com/news/ |
| Technical Blog: | https://www.derdack.com/category/technical-blog/ |
| YouTube: | http://www.youtube.com/derdack |
| Facebook: | http://www.facebook.com/derdack |
| LinkedIn: | http://www.linkedin.com/groups?gid=1701707 |
| Twitter: | http://twitter.com/#!/derdack |

## 4 CONTACT

Please visit www.derdack.com for further information on Enterprise Alert® or contact us:

| | |
|---|---|
| Germany: | +49 (331) 29878-20 (German, English, Spanish), Fax: +49 (331) 29878-22 |
| UK: | +44 (20) 88167095 |
| US: | +1 (202) 4700885 |
| Email: | info@derdack.com |

### 4.1 Mailing Address

Derdack Corp.
4470 Cox Road, Suite 250
Glen Allen, VA 23060
USA

Derdack GmbH
Friedrich-Ebert-Straße 8
14467 Potsdam
Germany

### 4.2 Hours of Operation

Monday – Friday 09:00 a.m. – 06:00 p.m. Central European Time (GMT+1)

Closed Saturday and Sunday and on German and local public holidays

## 5 DISCLAIMER





Phone +49 331 29878-0 · Fax +49 331 29878-22 · www.derdack.com
Amtsgericht Potsdam, HRB 13071 · Managing Director: Matthes Derdack · EU VAT ID: DE 812 810 585