Pre-Shared Key Authentication Method - Legacy

This document outlines how to access the Armor API system using the Pre-Shared Key (PSK) authentication method. This method applies to all **Legacy** Armor API's.

Option 1: Create an API key in AMP, and then authenticate through the command line

You can use the API tokenization feature in the Armor Management Portal (AMP) to create an API key. This key will help you log into the Armor API system.

After you create a key, you can use a GET request to log into the Armor API system.

⚠ Before you begin:

If you access the Armor API system through an AMP-generated API Key, then you will not be able to access the following endpoints:

- GET /users/{id}/keys
- DELETE /users/{id}/keys/{key}
- POST /users/{id}/keys
- GET /users/{id:int}/ActivationCode
- POST /users/resetpassword
- POST /users/setpassword
- PUT /users/{id:int}
- POST /users/status
- POST /users/
- POST /users/{userId:int}/invite
- GET /users/LockedOut/{accountId}/{email}
- POST /users/unlock/{accountId}/{email}
- DELETE /users/softDelete
- PUT /usersecurity/challengephrase
- GET /usersecurity/securityinformation/{referencekey}
- POST /usersecurity/securityinformation/{referencekey}
- POST /usersecurity/securityinformation/existing/{referencekey}
- GET /usersecurity/challengephrase/{userId}
- POST /usersecurity/validatemfaphone
- POST /usersecurity/securityinformation/{accountId}/{userId}
- POST /usersecurity/validatephoneapppin

When you create an API Key, you will generate a **Secret Key**. This key does not expire; you must securely store this key because Armor cannot retrieve this key for you.

⚠ If you lose the **Secret Key**, then you must delete the corresponding API Key in AMP. Afterwards, you must create a new API Key.

Armor cannot retrieve your **Secret Key**.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Account**.
2. Click **Users**.
3. Click **API Keys**.
4. Click the plus icon.
5. Enter a descriptive name, and then click **Create Key**.
6. Copy the **Key ID** and **Secret Key**.
7. Click **Close**.
8. The **API Keys** table will display a new entry.

At a high-level, to authenticate into the Armor API system with your API token, you must create a header with the following information:

- **ARMOR-PSK {Private Key ID}:{HMACSHA512 Signature}:{Nonce}:{Timestamp}**

⚠ Review the following sample authentication header:

```
ARMOR-PSK 20a37099-4a0b-432f-bf46-5fa690a0405c:
8wliK5PMXBrMNQX0DmXkkpC2YD5j+QtPH2xVRZM7jaaS0hC6jhRmtxy+nKJidDnYTpFc6blsO7+4VfKqslbqzA==:8jbj872s2h:
1528140529
```

Authentication Component	Description	Example
Authorization Type	Use **ARMOR-PSK**.	**ARMOR-PSK**
API Key ID	Use the **Key ID** generated in AMP.	**20a37099-4a0b-432f-bf46-5fa690a0405c**
HMAC signature	Specifically, create a SHA512 signature that includes the following parameters: • API key ID (generated in AMP) • httpMethod • requestPath • nonce • timestamp • requestbody • Secret Key (generated from AMP)	**8wliK5PMXBrMNQX0DmXkkpC2YD5j+QtPH2xVRZM7jaaS0hC6jhRmtxy+nKJidDnYTpFc6blsO7+4VfKqslbqzA==**
Nonce	Enter a unique ID. • This ID should be unique per request. • This ID cannot be longer than 128 characters. • This ID cannot contain a colon (:).	**8jbj872s2h**
Timestamp	Enter a Unix time stamp within 5 minutes of current time.	**1528140529**

⚠ Based on your API application, review the following documents for additional authentication information:

- Postman / Javascript
- C#
- Python

To review the API calls, as well as implement the calls, access the interactive Armor API tool at https://developer.armor.com/.

Troubleshooting

If you cannot create or access the **API Keys** screen, consider that:

- You may not have permissions to use this feature.
  - You must have the following permissions enabled:
    - API Keys All Read
    - API Keys All Delete
    - API Keys Self Manage
  - To learn how to update your permissions, see Roles and Permissions.

Option 2: Fully authenticate through the command line

Before you begin:

- The base URL is https://api.armor.com.
- This endpoint requires TLS 1.2+.
- The API uses standard OAuth authentication.
- If you intend to use your account as an API service account, please contact Armor Support to update the MFA setting on the account.
- If your Armor Management Portal (AMP) account requires multi-factor authentication (MFA), you should configure your HTTP client to have a timeout that allows sufficient time to enter the MFA response.

1. To access the API, you must first authenticate. Enter the login information for the Armor Management Portal (AMP). Review the following example:

```
POST /auth/authorize

{
  "username": "user@domain.com",
  "password": "password123%^&"
}
```

2. If the authentication is successful, you will receive the authorization code (**code**). Review the following example:

```
{
 "redirect_uri": null,
 "code": "<<base64-hash>>",
 "success": true
}
```

3. Redeem the authorization code (**code**) to retrieve the access token. You must redeem this code within two minutes of the previous request. Review the following example:

```
POST /auth/token

{
  "code":"<<base64-hash>>",
  "grant_type":"authorization_code"
}
```

4. If the request is successful, you will receive the **access token (access_token)**. Review the following example:

```
{
 "access_token": "<<32-bit-uuid>>",
 "id_token": "<<base64-hash>>",
 "expires_in": 15,
 "token_type": "Bearer"
}
```

5. Enter the access token (**access_token**) to complete the authentication process. Review the following example:

```
Authorization: FH-AUTH <<access_token>>
```

6. (Optional) The access token expires every 15 minutes. If you want to extend the session, then you can request a new access token before the current access token expires. In this example, you do not need to authenticate again with the new access token. Review the following example:

```
POST /auth/token/reissue

{
        "token": "<<32-bit-uuid>>"
}
```

7. (Optional) If the request is successful, you will receive the previous access token without the ID token. Review the following example:

```
{
 "access_token": "<<32-bit-uuid>>",
 "id_token": null,
 "expires_in": 15,
 "token_type": "Bearer"
}
```

8. (Optional) If you have multiple accounts in AMP, you may want to specify the account to configure. Enter the integer for the account ID. Review the following example:

```
X-Account-Context: <<int>>
```


There are two ways to retrieve your account ID:

Via the command line:

1. In the command line, enter the **GET /me** command.

Via AMP:

1. Access the Armor Management Portal (AMP).
2. On the left-side navigation, click **Account**.
3. Copy the number in **Account Number**.
4. In the command line, for **X-Account-Context**, enter the **Account Number**.

Was this helpful?

Your Rating:  Results:  6 rates