

# Access the Armor API System via an API token.mobile.phone

## Armor Knowledge Base

[Armor Knowledge Base](#) / [Armor API Guide](#) / [Pre-Shared Key Authentication Method - Legacy](#)

### Access the Armor API System via an API token (C#)

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.

#### Step 1: Create an API key

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.

#### Step 2: Authenticate into the Armor API system

To authenticate, you need to build a header with the following components:

Parameter	Description
<b>apiKey</b>	Enter the <b>Key ID</b> generated from AMP. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> In the example below, replace <b>use the api key id</b> with your key ID.</div>
<b>secretKey</b>	Enter the <b>Secret Key</b> generated from AMP. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> In the example below, replace <b>use the secret key</b> with your secret key.</div>
<b>nonce</b>	Enter a unique ID. <ul style="list-style-type: none"><li>• This ID cannot be longer than 128 characters.</li><li>• This ID cannot contain a colon (:).</li></ul>
<b>requestPath</b>	
<b>requestBody</b>	
<b>timestamp</b>	Enter a Unix time stamp within 5 minutes of the current time.
<b>httpMethod</b>	Enter GET or POST.

```

{
    using System;
    using System.Security.Cryptography;
    using System.Text;

    public static class AuthHeaderHelper
    {
        /// <summary>
        /// The following function creates the needed authentication header to work for ApiToken
        /// HttpRequestMessage.Headers.Authorization = new AuthenticationHeaderValue("ARMOR-PSK", authValue)
        /// </summary>
        /// <param name="apiKey">use the api key id</param>
        /// <param name="secretKey">use the secret key</param>
        /// <param name="nonce">A unique value, has 5 min lifespan</param>
        /// <param name="requestPath">absolute path: Example: /accounts/2</param>
        /// <param name="requestBody">Request body applies.</param>
        /// <param name="timestamp">Must be current time</param>
        /// <param name="httpMethod">Http Method: GET, POST, ...</param>
        /// <returns>string auth header Example: 'ARMOR-PSK apiKey:signature:nonce:unixTime'</returns>
        public static string CreateAuthorizationHeader(string apiKey, string secretKey, string nonce, string
requestPath, string requestBody, DateTime? timestamp, string httpMethod = "GET")
        {
            var dateTime = timestamp ?? DateTime.UtcNow;

            using (var sha512 = new SHA512Managed())
            {
                var requestBodyBytes = Encoding.ASCII.GetBytes(requestBody);
                var content = Convert.ToBase64String(sha512.ComputeHash(requestBodyBytes));
                requestBody = content.Length != 0 ? content : string.Empty;
            }

            Console.WriteLine("Request Body is: {0}", requestBody);
            requestPath = "/"accounts/2".ToLower();

            var unixTime = (Int32)(dateTime.Subtract(new DateTime(1970, 1, 1)).TotalSeconds);
            var requestData = string.Format("{0}{1}{2}{3}{4}{5}", apiKey, httpMethod, requestPath, unixTime,
nonce, requestBody);
            Console.WriteLine("Request Data is: {0}", requestData);
            string signature = string.Empty;
            using (var hmac = new HMACSHA512(Encoding.UTF8.GetBytes(secretKey)))
            {
                var result = hmac.ComputeHash(Encoding.UTF8.GetBytes(requestData));
                signature = Convert.ToBase64String(result);
            }

            return string.Format("{0}:{1}:{2}:{3}", apiKey, signature, nonce, unixTime);
        }
    }
}

```

### Step 3: Make an API Call

To learn about the different calls that you can make, see [Armor API Guide](#).

### Related Documentation

- To learn about the different calls that you can make, see [Armor API Guide](#).
- To learn how to create an API key or to learn a different way to access the Armor API system, see [Pre-Shared Key Authentication Method - Legacy](#).



**Was this helpful?**

\*

Your Rating:



Results:



1 rates