EAM Portal 9.0.2

User's Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

EAM Portal User's Guide
Updated - November 2017
Version - 9.0.2

Contents

Preface

Subject	This guide describes how to use the Primary account, Access to applications and Self Enrollment menus of the Enterprise Access Management (EAM) portal.
Audience	This guide is intended for end-users.
Required Software	EAM 9.0 evolution 2 and later versions. For more information about the versions of the required operating systems and software solutions quoted in this guide, please refer to One Identity EAM Release Notes.
Typographical Conventions	Bold Indicates: • Interface objects, such as menu names, buttons, icons and labels. • File, folder and path names. • Keywords to which particular attention must be paid. *Italics* - Indicates references to other guides. `Code` - Indicates portions of program codes, command lines or messages displayed in command windows. CAPITALIZATI ON Indicates specific objects within the application (in addition to standard capitalization rules). < > Identifies parameters to be supplied by the user.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

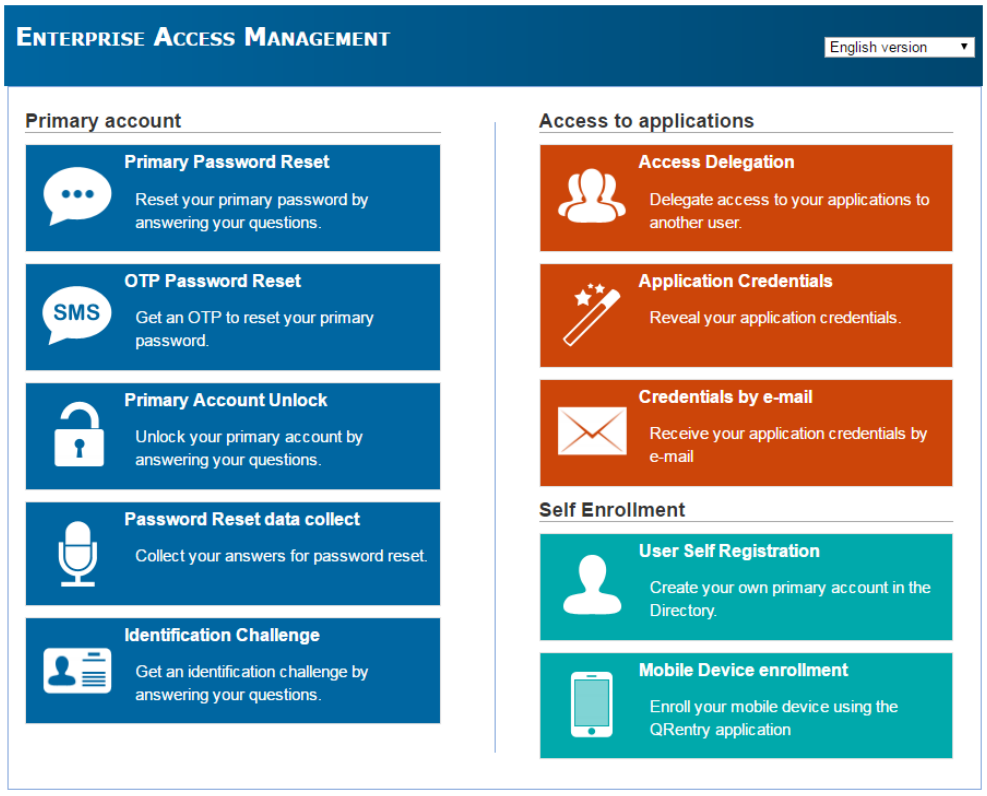
CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Documentation support	The information contained in this document is subject to change without notice. As our products are continuously enhanced, certain pieces of information in this guide can be incorrect. Send us your comments or suggestions regarding the documentation on the One Identity support website.

EAM Portal Presentation

The EAM portal provides an emergency access to different Enterprise Access Management (EAM) features. The main page of the portal is as follows:



NOTE: The display of the different sections of the portal may differ depending on the configuration performed by the EAM administrator.

This page displays a list of predefined emergency actions divided into three sections:

- The **Primary account** section enables you to:
  - Reset your primary password:
    - By answering your security questions.
    - With a confirmation code.
  - Unlock your primary account.
  - Initialize the "Self Service Password Request" by saving your answers to the security questions.
  - Retrieve an identification challenge to provide to the helpdesk.
- The **Access to applications** section enables you to:
  - Delegate access to one of your accounts to another user.
  - Reveal your application passwords.
  - Receive your credentials by e-mail.
- The **Self Enrollment** section enables you to:
  - Create your user account in the corporate directory.
  - Enroll your mobile device via QRentry.

Using the EAM Portal

Managing your primary account

Initializing the Self Service Password Request feature

Subject

You must initialize the Self Service Password Request (SSPR) feature to reset your password in case you lost or forgot it.

Initializing the SSPR consists in choosing a set of questions and saving the associated answers. You will have to provide these answers when you want to reset your password.

You can perform this task every time you want to update or change your questions/answers.

IMPORTANT: If there is a translation for the question, the language set for the navigator is the one used to display the questions.

When the SSPR is enabled, you can define your questions (optional) and answers the first time that your Authentication Manager is activated. Then you may need to modify this information in the following cases:

- The questions have changed, so you have to update your answers.
- You must enter your answers periodically.
- You want to change your questions/answers.

You can initialize the SSPR through the Authentication Manager icon (see *Authentication Manager for Windows User's Guide*) or by using the EAM portal as detailed in the following procedure.

Procedure

1. Enter the EAM portal URL in your Web browser, such as: **http://yourwebserver.yourdomain.com/**

   The **EAM portal** page opens.

2. Click **Password Reset data collect**.

   The **Authentication** page appears.

3. To authenticate with your:

- Credentials:

a. Select your **domain** in the drop down list.

b. Enter your **Username** and **Password** in the corresponding fields.

c. Click **Sign in**.

- Mobile device:

Without network	With network (Android only)
Enter your **Username** and click  .	Enter your **Username** and click **Sign in**..
Scan the displayed QR code.	Tap the notification received on your mobile device.
Enter the displayed code in the corresponding field and click **Sign in**.	Authorize the authentication by tapping **Authorize**.

4. Answer the displayed questions and click **Submit your answer**.

   Once you have answered all the questions, the SSPR is initialized.

Resetting your primary password

Subject

The Reset Password feature allows you to reset your password to open your Windows session even if you have forgotten your smart card or cannot remember your password.

You can reset your password upon session opening (see *Authentication Manager for Windows User's Guide*) or by using the EAM portal, as detailed in the following procedure.

Resetting with the SSPR

Before starting

You have chosen a set of questions and recorded the associated answers using the Self Service Password Request Wizard, as described in Initializing the Self Service Password Request feature.

NOTE: If you have not initialized the Self Service Password Request and therefore cannot reset your password by yourself, the administrator can still modify your primary password from EAM Console.

Procedure

1. Enter the EAM portal URL in your Web browser, such as: **http://yourwebserver.yourdomain.com/**

   The **EAM portal** page opens.

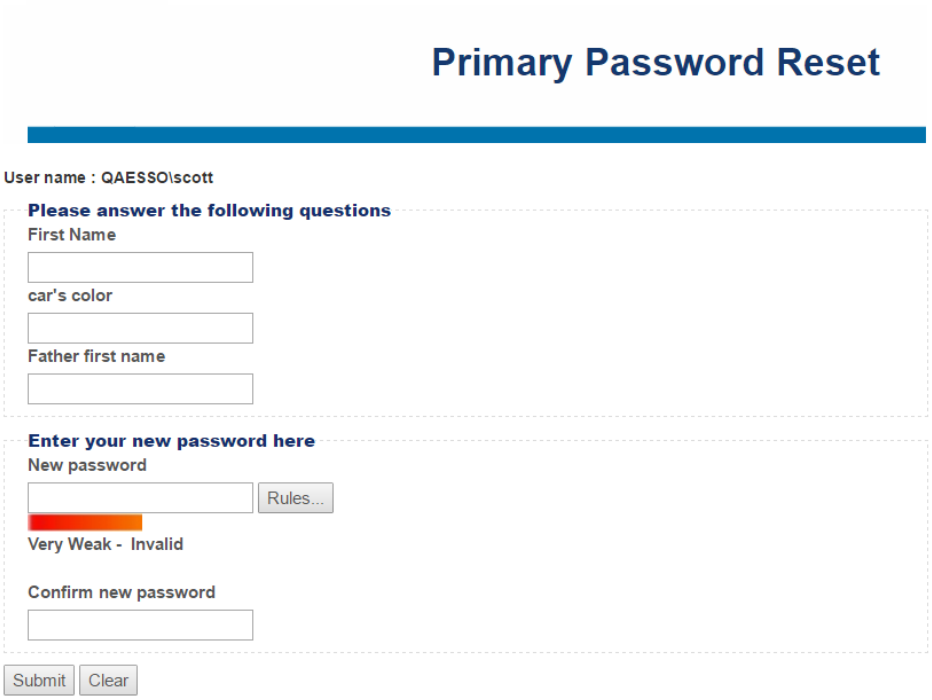
2. Click **Primary Password Reset**.

   The **Password Reset** page opens.

3. Select your **domain** in the drop down list, enter your **Username** and click **Submit**.

NOTE: If a Captcha check is required, reproduce the Captcha code in the corresponding field.

The **Question** page opens.



4. Enter your answers to the corresponding questions.
5. Enter your new password in the **New password** and **Confirm new password** fields and click **Submit**.

NOTE: Depending on the portal configuration, password selection tips can be displayed:

- The **Rules** button helps you with the password format control policy.
- An indicator informs you about the compliance and strength of your password.

6. Click the **Submit** button.

   Your password has been reset.

Resetting with an OTP

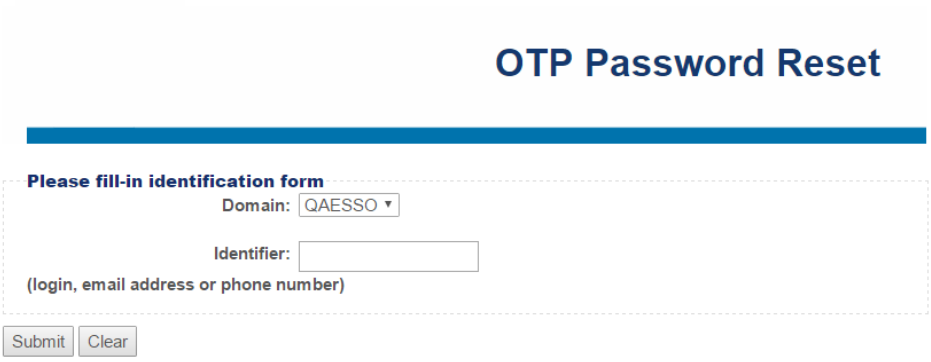
Procedure

1. Enter the EAM portal URL in your Web browser, such as: **http://yourwebserver.yourdomain.com/**

   The **EAM portal** page opens.

2. Click **OTP Password Reset**.

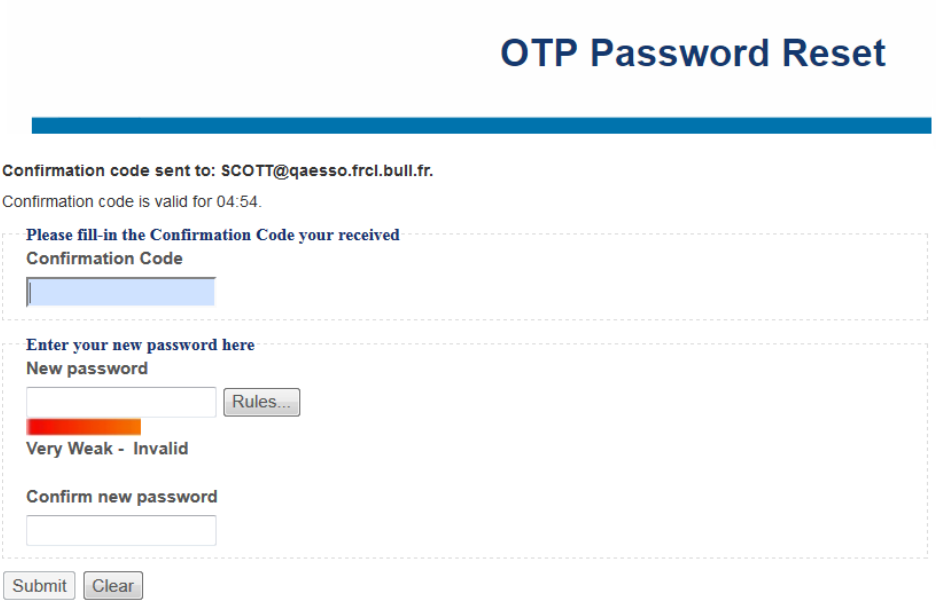
   The **Password Reset** page opens.



3. Select your **domain** in the drop down list, enter your **Identifier** and click **Submit**.

NOTE: If a Captcha check is required, reproduce the Captcha code in the corresponding field.

An e-mail or an SMS containing an OTP is sent to you.



4. Enter this OTP in the **confirmation code** field.
5. Enter your new password in the **New password** and **Confirm new password** fields and click **Submit**.

NOTE: Depending on the portal configuration, password selection tips can be displayed:

- The **Rules** button helps you with the password format control policy.
- An indicator informs you about the compliance and strength of your password.

6. Click the **Submit** button.

Your password has been reset.

Unlocking your primary account

Description

If you have locked your primary account by typing a wrong password several times in a row, execute the following procedure to unlock your account.

Procedure

1. Enter the EAM portal URL in your Web browser, such as: **http://yourwebserver.yourdomain.com/**

   The **EAM portal** page opens.

2. Click **Primary Account Unlock**.

   The **Authentication** page appears.

3. Select your **domain** in the drop down list, enter your **Username** and click **Submit**.

NOTE: If a Captcha check is required, reproduce the Captcha code in the corresponding field..

4. Answer the displayed questions and click **Submit your answer**.

   Once you have answered all the questions, your primary account is unlocked.

Retrieving an identification challenge

Subject

To identify yourself to a helpdesk operator, you must retrieve and provide an identification challenge by answering your SSPR questions. This section explains how to retrieve this challenge.

Before starting

You have chosen a set of questions and recorded the associated answers as described in Initializing the Self Service Password Request feature.

Procedure

1. Enter the EAM portal URL in your Web browser, such as: **http://yourwebserver.yourdomain.com/**

   The **EAM portal** page opens.

2. Click **Identification Challenge**.

The **Authentication** page appears.

3. Select your **domain** in the drop down list, enter your **Username** and click **Submit**.

NOTE: If a Captcha check is required, reproduce the Captcha code in the corresponding field.

4. Answer the displayed questions and click **Submit**.

   Once you have answered all the questions, your identification challenge is displayed. Provide this challenge to your helpdesk operator to identify yourself.

Managing access to your applications

Delegating a user account

You can delegate one or several user accounts quickly and simply by following this procedure:

Procedure

1. Enter the EAM portal URL in your Web browser, such as:
   http://yourwebserver.yourdomain.com/

   The **EAM portal** page opens.

2. Click **Access Delegation**.

   The **Authentication** page opens.

3. To authenticate with your:

- Credentials:

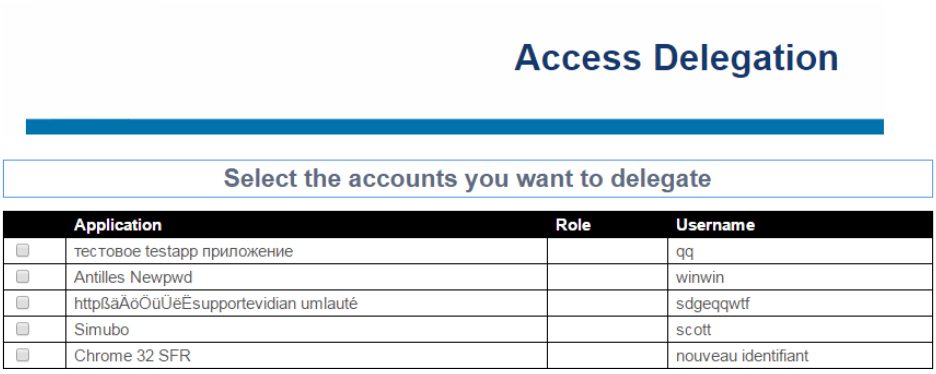
a. Select your **domain** in the drop down list.
b. Enter your **Username** and **Password** in the corresponding fields.
c. Click **Sign in**.

- Mobile device:

Without network	With network (Android only)
Enter your **Username** and click  .	Enter your **Username** and click **Sign in**..
Scan the displayed QR code.	Tap the notification received on your mobile device.
Enter the displayed code in the corresponding field and click **Sign in**.	Authorize the authentication by tapping **Authorize**.

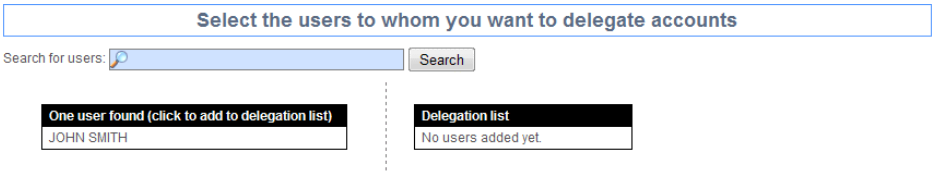
The **Account Delegation** page opens.

4. Select the account(s) you want to delegate by selecting the corresponding check boxes.

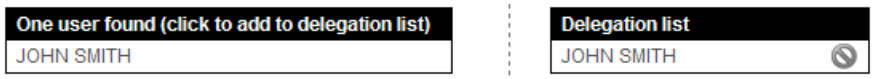


5. Enter the name of the user to whom you want to delegate your account(s) in the **Search for users** field and click **Search**.

The list of users appears.



6. Click the user to add him/her to the **Delegation list**.



NOTE: You can:

- Search for more users to add them to the **Delegation list**.
- Delete the added user(s) by clicking  .

7. Click **Proceed**.

   Your account(s) has/have been delegated to the selected user(s).

Revealing your application passwords

You can reveal your application password by using Enterprise SSO (see Enterprise SSO Administrator's Guide) or by using the EAM portal as detailed in the following procedure.

An account password is revealable only if the application profile associated with the access allows it, just like SSO Engine.

NOTE: You cannot reveal the password of a delegated account.

Procedure

1. Enter the EAM portal URL in your Web browser, such as: **http://yourwebserver.yourdomain.com/**

   The **EAM portal** page opens.

2. Click **Application Credentials**.

   The **Authentication** page opens.

3. To authenticate with your:

- Credentials:

a. Select your **domain** in the drop down list.

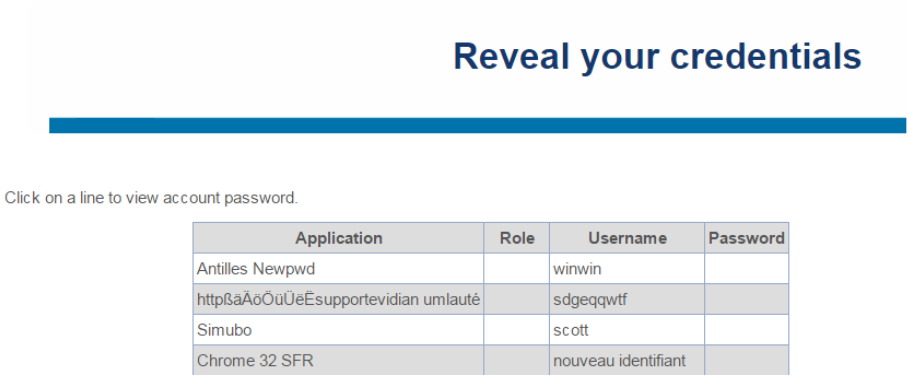
b. Enter your **Username** and **Password** in the corresponding fields.

c. Click **Sign in**.

- Mobile device:

Without network	With network (Android only)
Enter your **Username** and click  .	Enter your **Username** and click **Sign in**..
Scan the displayed QR code.	Tap the notification received on your mobile device.
Enter the displayed code in the corresponding field and click **Sign in**.	Authorize the authentication by tapping **Authorize**.

The **Reveal Your Credentials** page opens.



4. Click the application name to reveal the associated password.

Retrieving your application credentials

You can receive your application data (application name, login, password etc.) by using the EAM portal, as detailed in the following procedure.

In this case the Web portal allows you to receive the information by e-mail.

NOTE: You cannot reveal the following accounts:

- Shared accounts.
- Delegated accounts: you must ask your colleague for their password.

Procedure

1. Enter the EAM portal URL in your Web browser, such as: **http://yourwebserver.yourdomain.com/**

   The **EAM portal** page opens.

2. Click **Credentials by e-mail**.
3. Enter your **e-mail** address or your **login** and click **Request your data**.

NOTE: If a Captcha check is required, reproduce the Captcha code in the corresponding field.

The information of your SSO accounts has been sent to your e-mail address.

Managing self enrollment

Managing your primary account

Subject

You can create your user account, or "primary" account, directly in the corporate directory. This will allow you to authenticate with your password or mobile device.

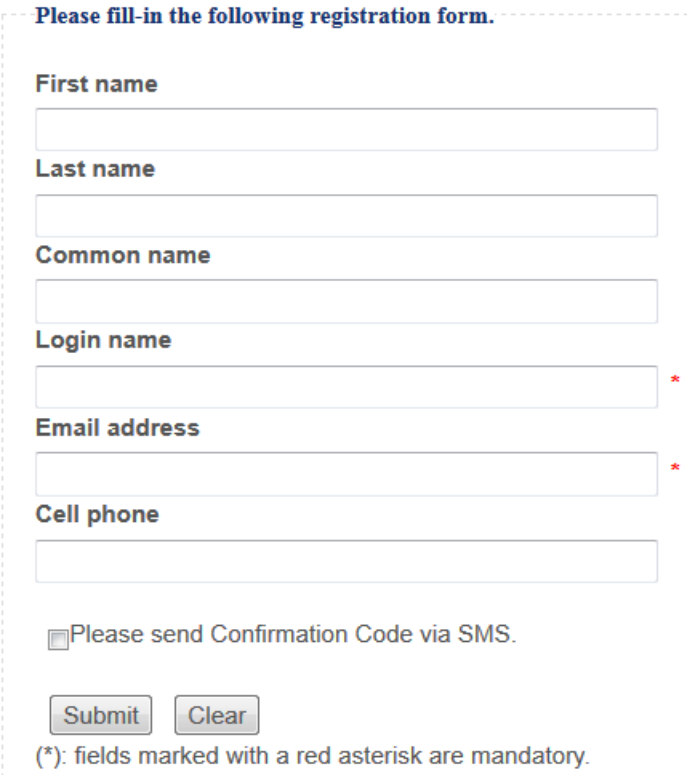
Procedure

1. Enter the EAM portal URL in your Web browser, such as: **http://yourwebserver.yourdomain.com/**

   The **EAM portal** page opens.

2. Click **User Self Registration**.

   The **User Self Registration** page opens.



3. Complete the fields of the form and click **Submit**.

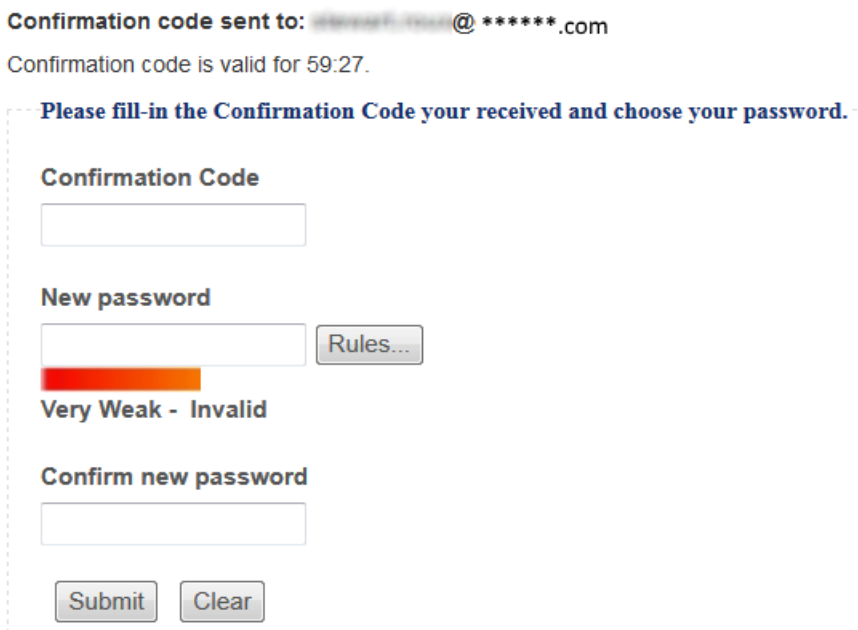
IMPORTANT: The following fields are mandatory:

- Login name: select a login name easy to remember (example: jsmith), indeed you will need this login name to authenticate to open your session.
- Email address: enter the email address known by your company (example: john.smith@oneidentity.com).

NOTE:

- Select the **Please send Confirmation Code via SMS** check box if you want to receive the code by email and SMS.
- If a Captcha check is required, reproduce the Captcha code in the corresponding field.

- A confirmation code is sent to you by email and SMS if you have requested it.
- The confirmation page opens.



4. Enter the confirmation code in the corresponding field.
5. Choose your password and confirm it.

NOTE: Depending on the portal configuration, password selection tips can be displayed:

- The **Rules** button helps you with the password format control policy.
- An indicator informs you about the compliance and strength of your password.

6. Click the **Submit** button.

   If your code and your password are valid, your primary account is created.

Enrolling your mobile devices

Subject

You can enroll a mobile device through the Authentication Manager icon (see *QRentry User's Guide*) or by using the EAM portal as detailed in the following procedure.

Before starting

The QRentry application is installed on your mobile device. For more information, see *QRentry User's Guide*.

Procedure

1. Enter the EAM portal URL in your Web browser, such as: **http://yourwebserver.yourdomain.com/**

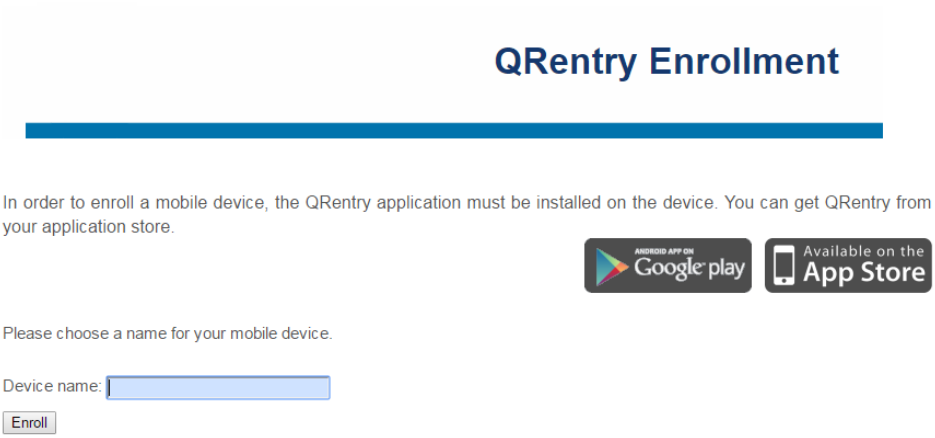
   The **EAM portal** page opens.

2. Click **Mobile Device enrollment**.

   The **Authentication** page opens.

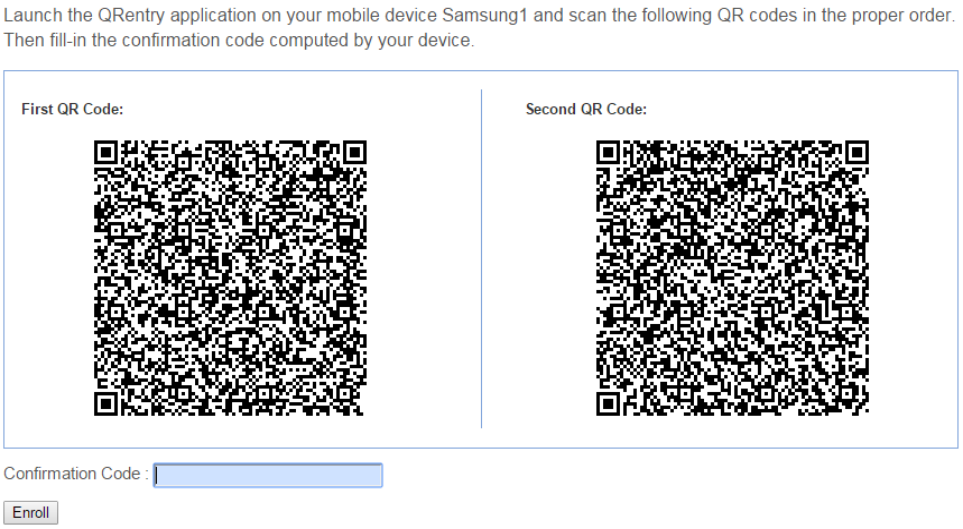
3. Select your **domain** in the drop down list, enter your **Username** and **Password** in the corresponding fields and click **Sign in**.

   The **QRentry Enrollment** page opens.



4. Enter a name for your mobile device and click **Enroll**.

   The page containing the QR codes to scan opens.



5. From your mobile device, start the QRentry application.
6. Tap **Scan** and scan the first QR code on the left with your mobile device.
7. Scan the QR code on the right.

   An enrollment code appears on your mobile device.
8. Enter the code displayed on your mobile device.
9. Click **Set**.

   Your mobile device is enrolled.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product