

Challenge Question Configuration Guide


Introduction

Use this guide to configure the Challenge Question function for Help Desk Authentication. The Challenge Question lets a Help Desk staff member verify an end-user's identity by asking a question only that user can answer. This feature of Multi-Factor Authentication helps secure the enterprise against [Social Engineering Attacks](#) in which an intruder masquerades as an employee asking for help.

The Challenge Question must be entered on the [User Self-services Account Update Page](#), and can be reviewed from the [Help Desk Account Management Page](#).

Prerequisites

1. Configure the [User Self-services Account Update realm](#) in which to input the Challenge Question and Answer

 The Challenge Question and Answer can only be set on the User Self-services page


2. Create a **New Realm** or access an existing realm in which Help Desk is used as a Multi-Factor Authentication method

3. Configure the following tabs in the Web Admin

- **Overview** – the description of the realm and SMTP connections must be defined
- **Data** – one or more data stores can be integrated with SecureAuth IdP
- **Workflow** – the way in which users will access the target must be defined
- **Registration Methods / Multi-Factor Methods** – the Multi-Factor Authentication method that will be used to access the target (if any) must be defined
- **Post Authentication** – the target resource or post authentication action must be defined
- **Logs** – the logs that will be enabled or disabled for this realm must be defined

 The Registration Methods tab in SecureAuth IdP Version 9.0 has been renamed Multi-Factor Methods as of Version 9.0.1

Challenge Question / User Self-services Realm Configuration Steps

 **Note:** These steps are required in addition to the configuration steps in the [User Self-services Account Update Page](#) guide to enable the creation of a challenge question to be used in Help Desk verification for 2-Factor Authentication

Data

▼ Profile Fields

Property	Source	Field	Data Format	Writable
Groups	Default Provider	memberOf		<input type="checkbox"/>
First Name	Default Provider	givenName		<input type="checkbox"/>
Last Name	Default Provider	sn		<input type="checkbox"/>
Phone 1	Default Provider	telephoneNumber		<input checked="" type="checkbox"/>
Phone 2	Default Provider	mobile		<input checked="" type="checkbox"/>
Phone 3	Default Provider			<input type="checkbox"/>
Phone 4	Default Provider			<input type="checkbox"/>
Email 1	Default Provider	mail		<input checked="" type="checkbox"/>
Email 2	Default Provider			<input type="checkbox"/>
Email 3	Default Provider			<input type="checkbox"/>
Email 4	Default Provider			<input type="checkbox"/>
PIN	Default Provider	facsimileTelephoneNumber		<input checked="" type="checkbox"/>
KB Questions	Default Provider	houseIdentifier		<input checked="" type="checkbox"/>
KB Answers	Default Provider	info		<input checked="" type="checkbox"/>
Aux ID 1	Default Provider		Plain Text	<input type="checkbox"/>
Aux ID 2	Default Provider		Plain Text	<input type="checkbox"/>

[Add Property](#)

1. In the **Profile Fields** section, map the **KB Questions** property to a directory attribute

This must be an attribute to which the SecureAuth IdP service account has read and write access (e.g. houseIdentifier)

2. Map the **KB Answers** property to a directory attribute

This must be an attribute to which the SecureAuth IdP service account has read and write access (e.g. info)

3. Enable **Writable** for both **KB Questions** and **KB Answers**



Refer to [LDAP Attributes / SecureAuth IdP Profile Properties Data Mapping](#) for more information



Click **Save** once the configurations have been completed and before leaving the **Data** page to avoid losing changes

Identity Management

Help Desk: [Configure help desk page](#)

Self Service: [Configure self service page](#)

4. In the **Identity Management** section, click **Configure self service page**

Self Service

Self Service

SecureAuth Field	Display Type	Datastore Filename	Regular Expression
First Name:	Show Required	givenName	
Field Count:	0		be entered
KBQ-KBA:	Show Enabled	houseIdentifier - info	Knowledge Based Questions
KBQ Count:	6		Number of kb questions to display
Number of Answers:	2		Minimum number of kb answers required to be answered
HelpDesk Challenge:	Show Enabled		For Help Desk verification

5. Select **Show Enabled** from the **HelpDesk Challenge** dropdown



Click **Save** once the configurations have been completed and before leaving the **Self Service** page to avoid losing changes

End-user Configuration Steps

User ID

First Name

Last Name

Phone 1

Phone 2

Email 1

PIN Hide

OATH Seed

Update
Reset

Knowledge Based Questions (optional) Hide Typing Below

What city were you born in?

.....

What was your favorite childhood game?

.....

What was your dream job as a child?

.....

For Help Desk verification

What was the model of your first car?

....

Digital Fingerprints (Uncheck to revoke)


- Windows 7 - Chrome 46.0.2490: 11/19/2015 10:23:43 AM
- Windows 7 - Chrome 47.0.2526: 1/21/2016 4:12:35 PM
- Windows 7 - Chrome 49.0.2623: 3/28/2016 8:47:36 AM

Push notification devices (uncheck to remove)

- iPod touch: 11/24/2015 2:25:12 PM: 11/24/2015 2:25:12 PM

[Restart Login](#)

1. Log in to the **User Self-services** page
2. In the **For Help Desk verification** section, select a Challenge Question from the dropdown
3. Enter an answer to the Challenge Question
4. Click **Update**

 The verification Question and Answer are written to the data store



Note: These configuration steps must be applied to *a//*realms using Help Desk with Challenge Question for Multi-Factor Authentication

Data

▼ Profile Fields				
Property	Source	Field	Data Format	Writable
Groups	Default Provider	memberOf		<input type="checkbox"/>
First Name	Default Provider	givenName		<input type="checkbox"/>
Last Name	Default Provider	sn		<input type="checkbox"/>
Phone 1	Default Provider	telephoneNumber		<input checked="" type="checkbox"/>
Phone 2	Default Provider	mobile		<input checked="" type="checkbox"/>
Phone 3	Default Provider			<input type="checkbox"/>
Phone 4	Default Provider			<input type="checkbox"/>
Email 1	Default Provider	mail		<input checked="" type="checkbox"/>
Email 2	Default Provider			<input type="checkbox"/>
Email 3	Default Provider			<input type="checkbox"/>
Email 4	Default Provider			<input type="checkbox"/>
PIN	Default Provider	facsimileTelephoneNumber		<input checked="" type="checkbox"/>
KB Questions	Default Provider	houseIdentifier		<input checked="" type="checkbox"/>
KB Answers	Default Provider	info		<input checked="" type="checkbox"/>
Aux ID 1	Default Provider		Plain Text	<input type="checkbox"/>
Aux ID 2	Default Provider		Plain Text	<input type="checkbox"/>

[Add Property](#)



The **KB Questions** and **KB Answers** settings must be the same as the ones applied on the User Self-services realm

1. In the **Profile Fields** section, map the **KB Questions** property to a directory attribute

This must be an attribute to which the SecureAuth IdP service account has read and write access (e.g. houseIdentifier)

2. Map the **KB Answers** property to a directory attribute

This must be an attribute to which the SecureAuth IdP service account has read and write access (e.g. info)

3. Enable **Writable** for both **KB Questions** and **KB Answers**



Refer to [LDAP Attributes / SecureAuth IdP Profile Properties Data Mapping](#) for more information



Click **Save** once the configurations have been completed and before leaving the **Data** page to avoid losing changes

Registration Configuration

KB Conversion:

Help Desk Settings

Help Desk 1:	<input type="text" value="Enabled"/>
Phone:	<input type="text" value="555-555-1213"/>
Email:	<input type="text" value="YourSupport@Company.com"/>
Help Desk 2:	<input type="text" value="Disabled"/>
Phone:	<input type="text" value="555-555-1213"/>
Email:	<input type="text" value="YourSupport@Company.com"/>

Advanced Settings

<input type="checkbox"/> Inline Initialization:	<input type="checkbox"/> Missing Phone
<input type="checkbox"/> Self-Service Settings	<input type="checkbox"/> Missing Email
<input checked="" type="checkbox"/> Missing KB Answers	<input type="checkbox"/> Missing PIN
Auto-Submit When One Avail:	<input type="text" value="Disabled"/>
OTP Length:	<input type="text" value="4"/>
Lock User (after max attempts):	<input type="text" value="False"/>

4. In the **Registration Configuration** section, under **Help Desk Settings**, select **Enable** from at least one of Help Desk options dropdowns (**Help Desk 1** and / or **Help Desk 2**)

5. Enter the **Phone** number and **Email** address that the user can use to contact the Help Desk

6. Under **Advanced Settings**, check **Missing KB Answers** in the **Inline Initialization** field to enable users to create a Challenge Question and Answer during the login process (if information is missing from the directory)



Click **Save** once the configurations have been completed and before leaving the **Registration Methods** page to avoid losing changes

Optional Help Desk Page Configuration Steps



Note: To enable administrative review of Challenge Questions, follow these configuration steps in addition to steps from the [Account Management \(Help Desk\) Page Configuration Guide](#)

Data

▼ Profile Fields

Property	Source	Field	Data Format	Writable
Groups	Default Provider	<input type="text" value="memberOf"/>		<input type="checkbox"/>
First Name	Default Provider	<input type="text" value="givenName"/>		<input type="checkbox"/>
Last Name	Default Provider	<input type="text" value="sn"/>		<input type="checkbox"/>
Phone 1	Default Provider	<input type="text" value="telephoneNumber"/>		<input checked="" type="checkbox"/>
Phone 2	Default Provider	<input type="text" value="mobile"/>		<input checked="" type="checkbox"/>
Phone 3	Default Provider	<input type="text"/>		<input type="checkbox"/>
Phone 4	Default Provider	<input type="text"/>		<input type="checkbox"/>
Email 1	Default Provider	<input type="text" value="mail"/>		<input checked="" type="checkbox"/>
Email 2	Default Provider	<input type="text"/>		<input type="checkbox"/>
Email 3	Default Provider	<input type="text"/>		<input type="checkbox"/>
Email 4	Default Provider	<input type="text"/>		<input type="checkbox"/>
PIN	Default Provider	<input type="text" value="facsimileTelephoneNumber"/>		<input checked="" type="checkbox"/>
KB Questions	Default Provider	<input type="text" value="houseIdentifier"/>		<input checked="" type="checkbox"/>
KB Answers	Default Provider	<input type="text" value="info"/>		<input checked="" type="checkbox"/>
Aux ID 1	Default Provider	<input type="text"/>	Plain Text	<input type="checkbox"/>
Aux ID 2	Default Provider	<input type="text"/>	Plain Text	<input type="checkbox"/>

[Add Property](#)



The **KB Questions** and **KB Answers** settings must be the same as the ones applied on the User Self-services realm and in the realm(s) using Help Desk with Challenge Question for Multi-Factor Authentication

1. In the **Profile Fields** section, map the **KB Questions** property to a directory attribute

This must be an attribute to which the SecureAuth IdP service account has read and write access (e.g. houseIdentifier)

2. Map the **KB Answers** property to a directory attribute

This must be an attribute to which the SecureAuth IdP service account has read and write access (e.g. info)

3. Enable **Writable** for both **KB Questions** and **KB Answers**



Refer to [LDAP Attributes / SecureAuth IdP Profile Properties Data Mapping](#) for more information



Click **Save** once the configurations have been completed and before leaving the **Data** page to avoid losing changes

▼ Identity Management

Help Desk: [Configure help desk page](#)

Self Service: [Configure self service page](#)

4. In the **Identity Management** section, click **Configure help desk page**

Help Desk

▼ Help Desk

SecureAuth Field	Display Type	Datastore Fieldname	Label
First Name:	Show Enabled ▼	<i>givenName</i>	First Name
Last Name:	Show Enabled ▼	<i>sn</i>	Last Name
Phone 1:	Show Enabled ▼	<i>telephoneNumber</i>	Phone 1
Phone 2:	Show Enabled ▼	<i>mobile</i>	Phone 2
Phone 3:	Hide ▼		Phone 3
Phone 4:	Hide ▼		Phone 4
Email 1:	Show Enabled ▼	<i>mail</i>	Email 1
Email 2:	Hide ▼	<i>otherMailbox</i>	Email 2
Email 3:	Hide ▼		Email 3
Email 4:	Hide ▼		Email 4
Clear KBQ-KBA CheckBox:	Show ▼	<i>houseIdentifier - info</i>	Clear the user's Knowledge Based Answers
Challenge Question:	Show ▼		Challenge Question:

5. Select **Show** from the **Challenge Question** dropdown



Click **Save** once the configurations have been completed and before leaving the **Help Desk** page to avoid losing changes

Help Desk

User55

Get User

Reset Password

Lock

Disable

Delete

User55

Status: Normal

Password Last Changed: 3/28/2016 8:46:38 AM

First Name

Last Name

Phone 1

Phone 2

Email 1

Update

Clear the user's Knowledge Based Answers *(disabled if no answer to clear)*

Challenge Question: What was the model of your first car?

User's Answer:

Digital

Fingerprints
(Uncheck to revoke):

- Windows 7 - Chrome 49.0.2623: 3/28/2016 8:47:36 AM
- Windows 7 - Chrome 47.0.2526: 1/21/2016 4:12:35 PM
- Windows 7 - Chrome 46.0.2490: 11/19/2015 10:23:43 AM

Reset Fingerprints

Push notification devices
(uncheck to remove)

- iPod touch: 11/24/2015 2:25:12 PM

Reset Push Devices

OTP devices
(uncheck to remove)

No OTP Devices

Reset OTP Devices

Reset All Registrations

[Restart Login](#)

The Challenge Question and Answer can be viewed (but not edited) on the Help Desk Admin Page