Part II: Configure the Admin realm (SecureAuth0)

Introduction

SecureAuth0 is the Admin realm, the main realm on SecureAuth IdP Web Admin. Since this realm manages the SecureAuth IdP server, it should be configured first to ensure the security of the appliance and all realms to be created and housed on the appliance. This realm also enables Multi-Factor Authentication for all end-users.

You can configure SecureAuth0 for local access via Remote Desktop Protocol (RDP) or remote access via the Web Admin interface.

If configuring SecureAuth0 for remote access:

- An integration with an enterprise data store is required to access the Web Admin interface.
- Multi-Factor methods must be configured for end-users to use Multi-Factor Authentication.

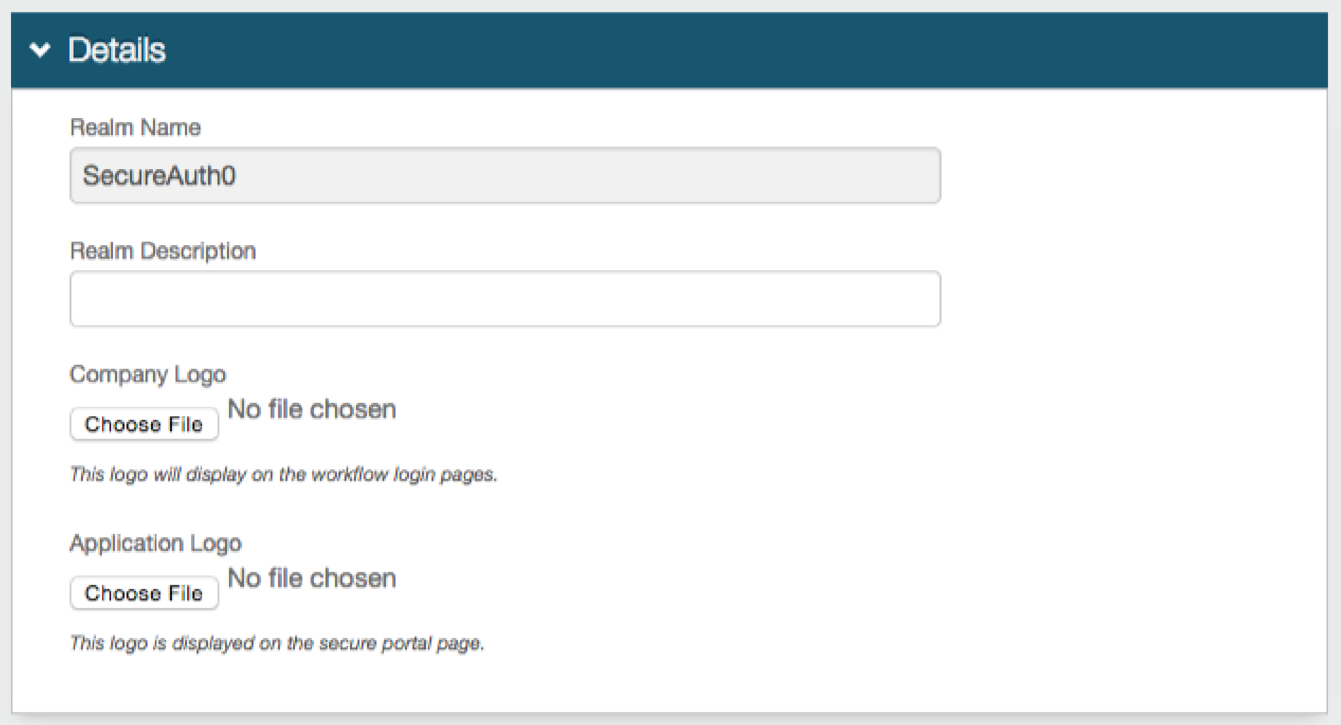
Admin realm configuration steps

Overview tab

1. In the Details section, **SecureAuth0** is set as the Realm Name.

2. OPTIONAL: Provide a Realm Description.

3. **Save** the configuration.



Details

Realm Name

SecureAuth0

Realm Description

Company Logo

No file chosen

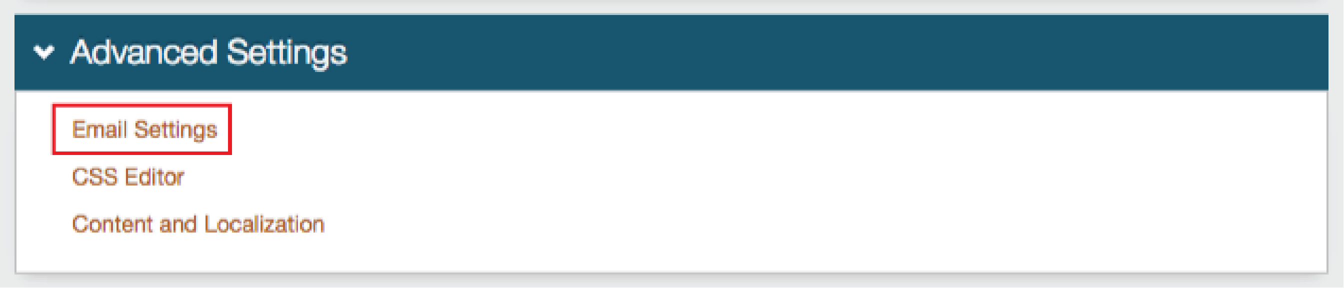
This logo will display on the workflow login pages.

Application Logo

No file chosen

This logo is displayed on the secure portal page.

4. On the Advanced Settings section, click **Email Settings**.



5. To configure SMTP settings:

   a. Provide the Simple Mail Transfer Protocol (SMTP) **Server Address** from which SecureAuth IdP will send emails.

   b. If the SMTP server uses a port other than the default **Port 25**, change the Port number.

   c. Provide the **Username**, **Password**, and / or **Domain** if required by the SMTP Relay.

   d. If emails will be sent through a Secure Socket Layer (SSL), then select **True** from the SSL dropdown.

6. To configure Email settings:

   a. OPTIONAL: Upload a Logo to be used in email messages sent from SecureAuth IdP.

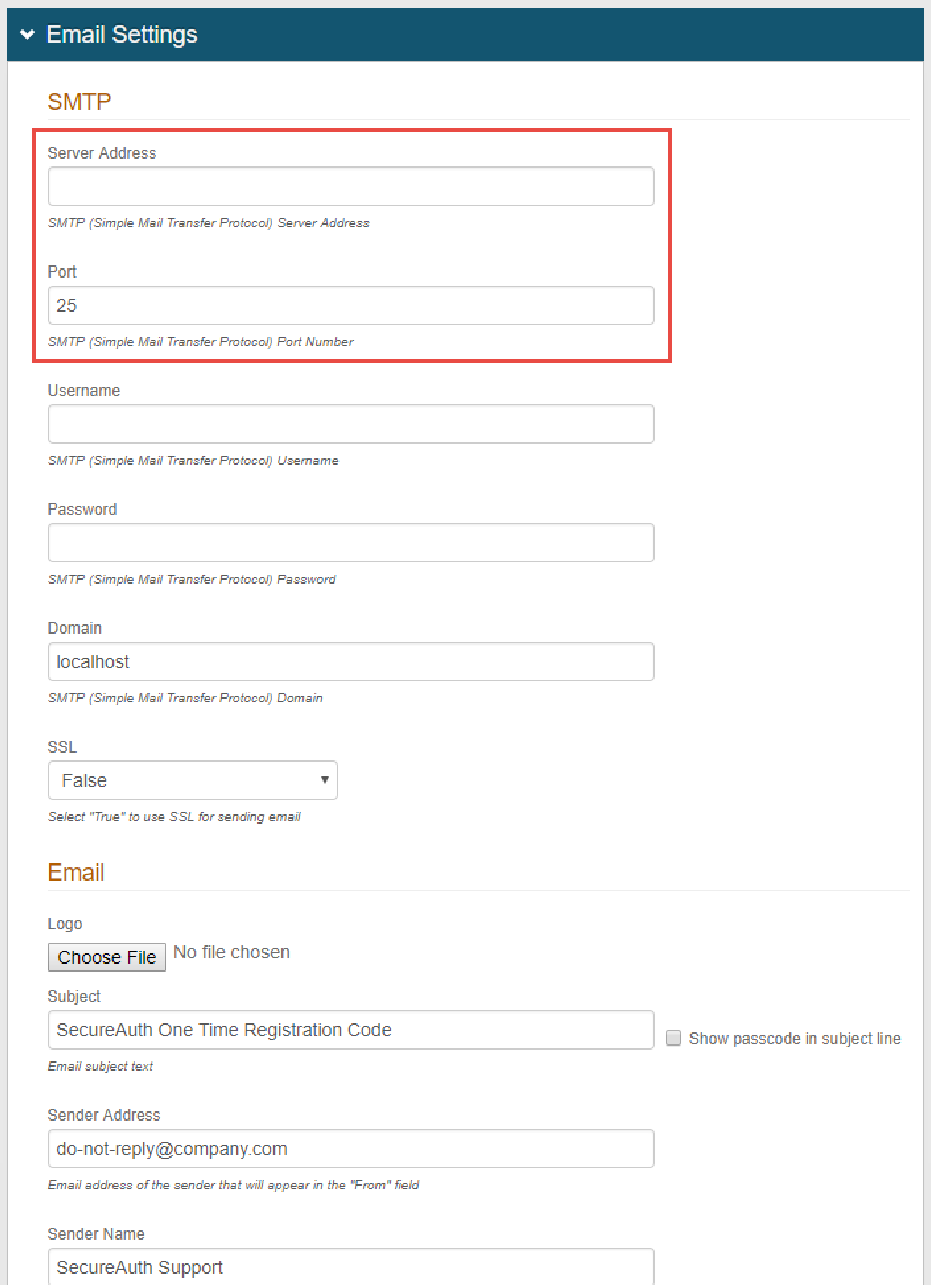
   b. Provide the **Subject** line for SecureAuth IdP email messages.

   c. Provide the **Sender Address** for SecureAuth IdP email messages.

   d. Provide the **Sender Name** for SecureAuth IdP email messages.

   e. Select a **Template** to be used for SecureAuth IdP email messages.

7. **Save** the configuration.



Email Settings

SMTP

Server Address

SMTP (Simple Mail Transfer Protocol) Server Address

Port

25

SMTP (Simple Mail Transfer Protocol) Port Number

Username

SMTP (Simple Mail Transfer Protocol) Username

Password

SMTP (Simple Mail Transfer Protocol) Password

Domain

localhost

SMTP (Simple Mail Transfer Protocol) Domain

SSL

False ▾

Select "True" to use SSL for sending email

Email

Logo

Choose File No file chosen

Subject

SecureAuth One Time Registration Code

□ Show passcode in subject line

Email subject text

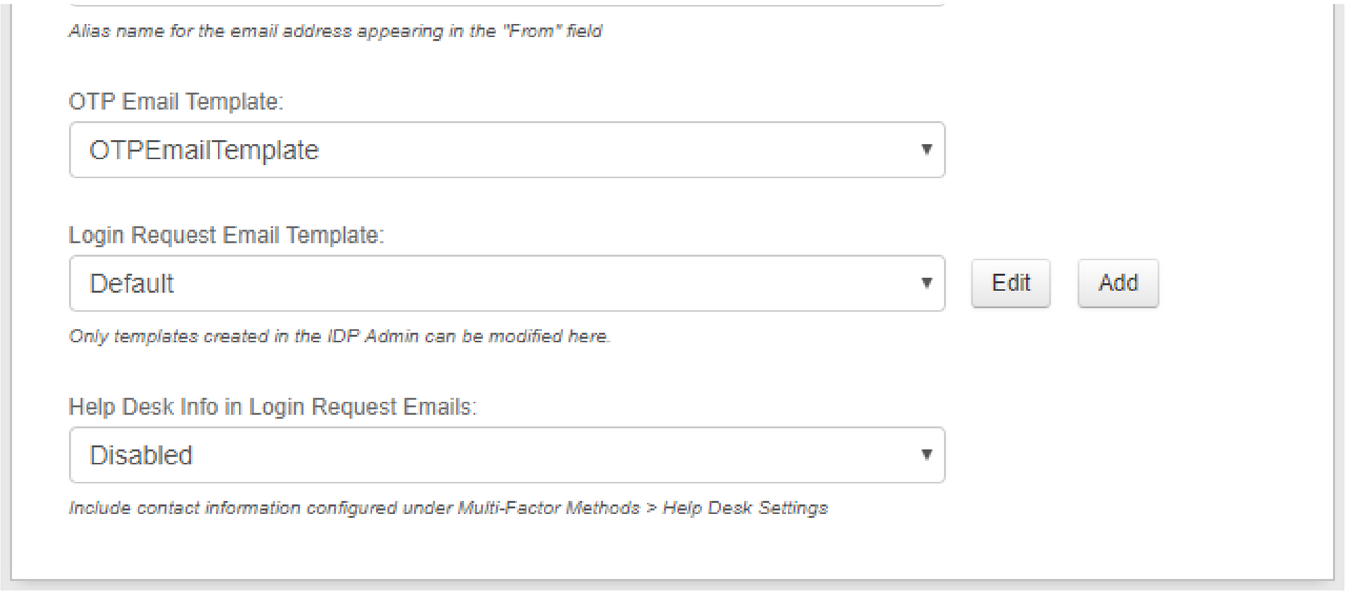
Sender Address

do-not-reply@company.com

Email address of the sender that will appear in the "From" field

Sender Name

SecureAuth Support



Alias name for the email address appearing in the "From" field

OTP Email Template: OTPEmailTemplate

Login Request Email Template: Default

Only templates created in the IDP Admin can be modified here.

Help Desk Info in Login Request Emails: Disabled

Include contact information configured under Multi-Factor Methods > Help Desk Settings

NOTE: For the complete Overview configuration steps, refer to Overview Tab Configuration.

Data tab

NOTE: The Data tab needs to be configured only if remote access will be allowed to SecureAuth0.

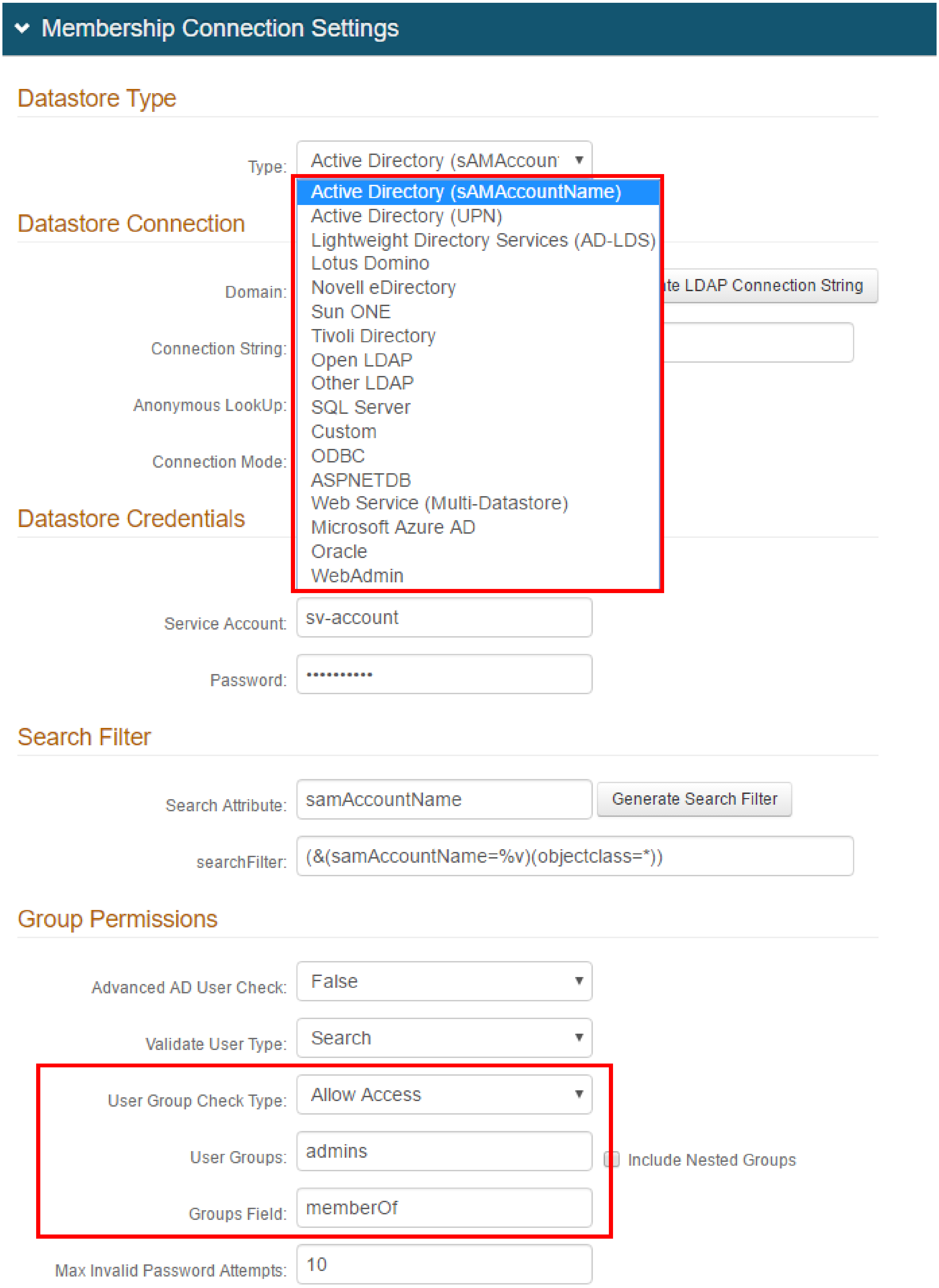
8. In the Membership Connection Settings section, select the directory to be integrated with SecureAuth IdP from the **Data Store** dropdown. This directory will be used for end-user Multi-Factor Authentication and assertion:

- Active Directory (sAMAccountName)
- Active Directory (UPN)
- Lightweight Directory Services (AD-LDS)
- Lotus Domino
- Novell eDirectory
- Sun ONE
- Tivoli Directory
- Open LDAP
- Other LDAP
- SQL Server
- Custom – for directories not listed. This would require custom coding, so please contact SecureAuth for configuration steps / requirements
- ODBC
- ASPNETDB
- Web Service (Multi-Datastore)
- Microsoft Azure AD
- Oracle
- WebAdmin (*for SecureAuth0 Admin Realm only*)

9. Follow the instructions for the selected data store, as well as the instructions on this page.

10. Under Group Permissions, restrict access to SecureAuth0 to a specific admin group. In the corporate data store, create an admin user group comprised of only those members who will have access to the Web Admin.

> NOTE: SecureAuth advises configuring access to the SecureAuth0 realm with security best practices in mind. Recommendations are listed below, but it is the customer's responsibility to determine the best settings for their specific deployment. These recommendations do not constitute a guarantee of security.
>
> a. (AD/LDAP) In the User Group Check Type field, select **Allow Access**.
>
> b. In the **User Groups** (AD/LDAP) or **Allowed Groups** (SQL) field, enter the name of the admin group.
>
> c. (AD/LDAP) Set the **Groups Field** field to the LDAP attribute that contains user group information – for example: memberOf



Membership Connection Settings

Datastore Type

Type: Active Directory (sAMAccoun

Datastore Connection

Domain:

Connection String:

Anonymous LookUp:

Connection Mode:

Datastore Credentials

Service Account: sv-account

Password: ••••••••••

Search Filter

Search Attribute: samAccountName

searchFilter: (&(samAccountName=%v)(objectclass=*))

Group Permissions

Advanced AD User Check: False

Validate User Type: Search

User Group Check Type: Allow Access

User Groups: admins

□ Include Nested Groups

Groups Field: memberOf

Max Invalid Password Attempts: 10

The Profile Fields section is for LDAP data stores only; refer to the specific directory configuration guide for more information.

NOTE: The **Fields** shown in the image below are only *examples*; each data store is organized differently and may have different values for each **Property**.

11. Map the SecureAuth IdP **Field** to the appropriate data store **Property**.

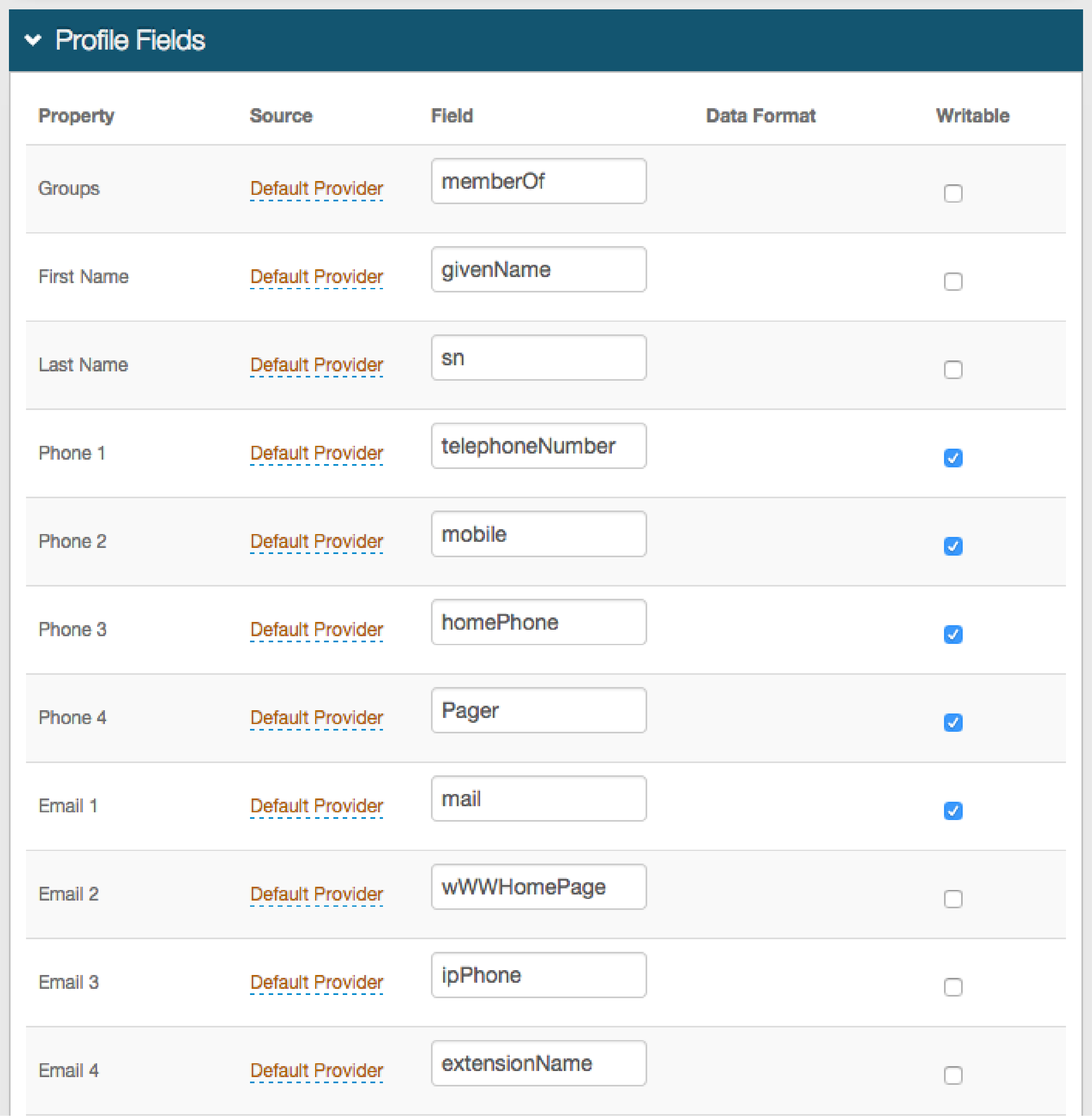
    For example, the **memberOf** data store Field is located under the **Groups** Property.

12. If another directory is enabled in the Profile Connection Settings section and contains this **Property**:

    a. Click **Default Provider** and select another Source from the dropdown.

    b. Check **Writable** for a Property that will be changed in the data store by SecureAuth IdP – for example, user account information (telephone number) or authentication mechanisms (knowledge based questions, fingerprints).

13. **Save** the configuration.



Profile Fields

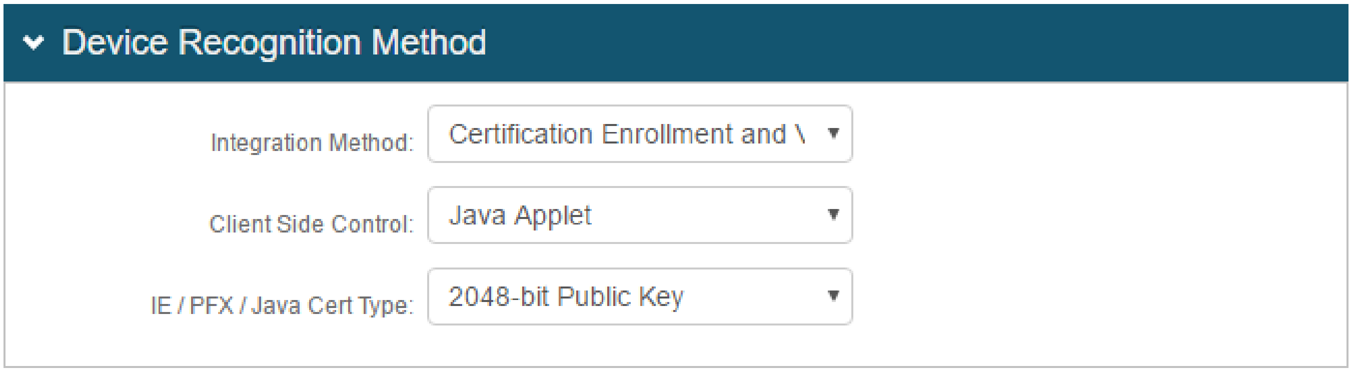
Property	Source	Field	Data Format	Writable
Groups	Default Provider	memberOf		☐
First Name	Default Provider	givenName		☐
Last Name	Default Provider	sn		☐
Phone 1	Default Provider	telephoneNumber		☑
Phone 2	Default Provider	mobile		☑
Phone 3	Default Provider	homePhone		☑
Phone 4	Default Provider	Pager		☑
Email 1	Default Provider	mail		☑
Email 2	Default Provider	wWWHomePage		☐
Email 3	Default Provider	ipPhone		☐
Email 4	Default Provider	extensionName		☐

NOTE: For the complete Data configuration steps, refer to Data Tab Configuration.

Workflow tab

14. In the Device Recognition Method section, select the **Integration Method**, and the **Client Side Control** and **IE / PFX / Java Cert Type** that apply to the first selection.

NOTE: See variations in Workflow configuration.


Device Recognition Method

Integration Method: Certification Enrollment and \

Client Side Control: Java Applet

IE / PFX / Java Cert Type: 2048-bit Public Key

15. Enforce full authentication requirements for each logon attempt to SecureAuth0.

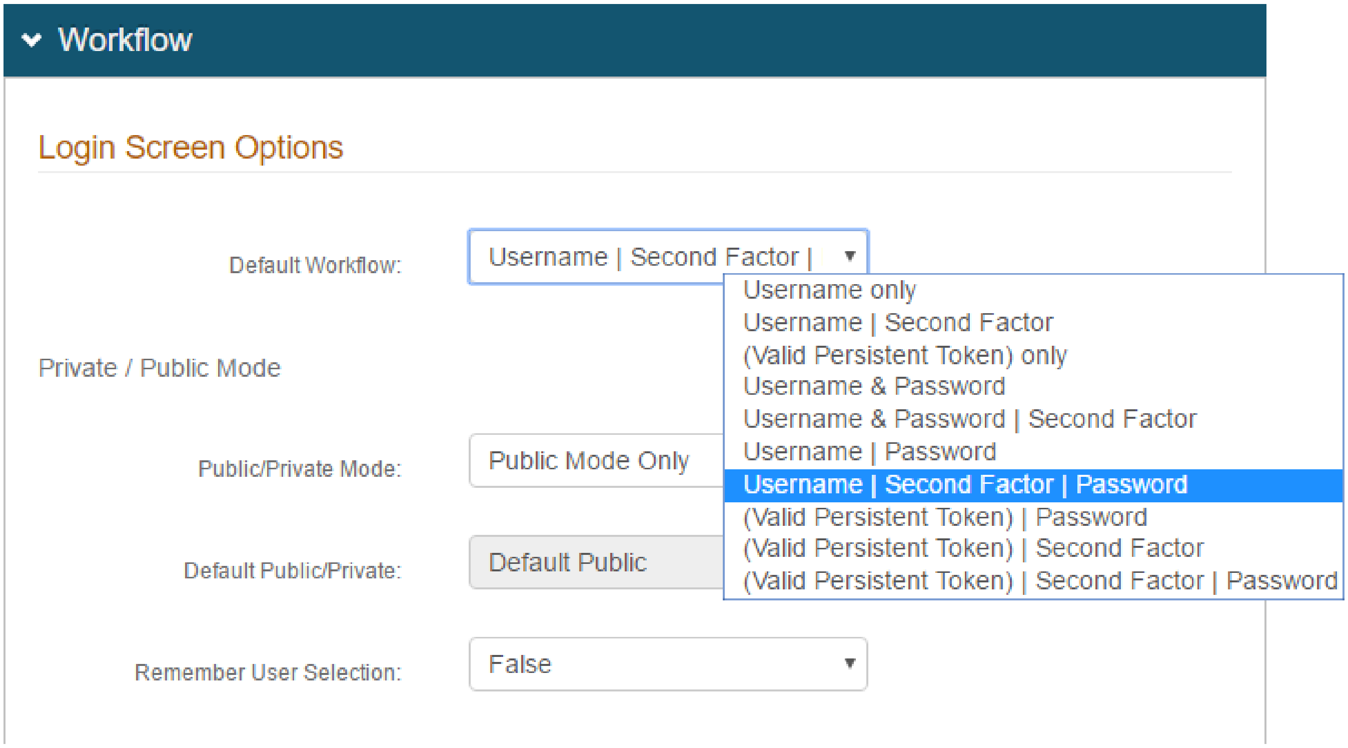
    NOTE: SecureAuth advises configuring remote access to the SecureAuth0 realm with security best practices in mind. Recommendations are listed below, but it is the customer's responsibility to determine the best settings for their specific deployment. These recommendations do not constitute a guarantee of remote security.

    a. Set the Default Workflow to **Username | Second Factor | Password**.

    b. Set the Public/Private Mode field to **Public Mode Only**.

    These settings force users to authenticate fully on each logon attempt.

16. **Save** the configuration.


Workflow

Login Screen Options

Default Workflow: Username | Second Factor |

Username only
Username | Second Factor
(Valid Persistent Token) only
Username & Password
Username & Password | Second Factor
Username | Password
Username | Second Factor | Password
(Valid Persistent Token) | Password
(Valid Persistent Token) | Second Factor
(Valid Persistent Token) | Second Factor | Password

Private / Public Mode

Public/Private Mode: Public Mode Only

Default Public/Private: Default Public

Remember User Selection: False

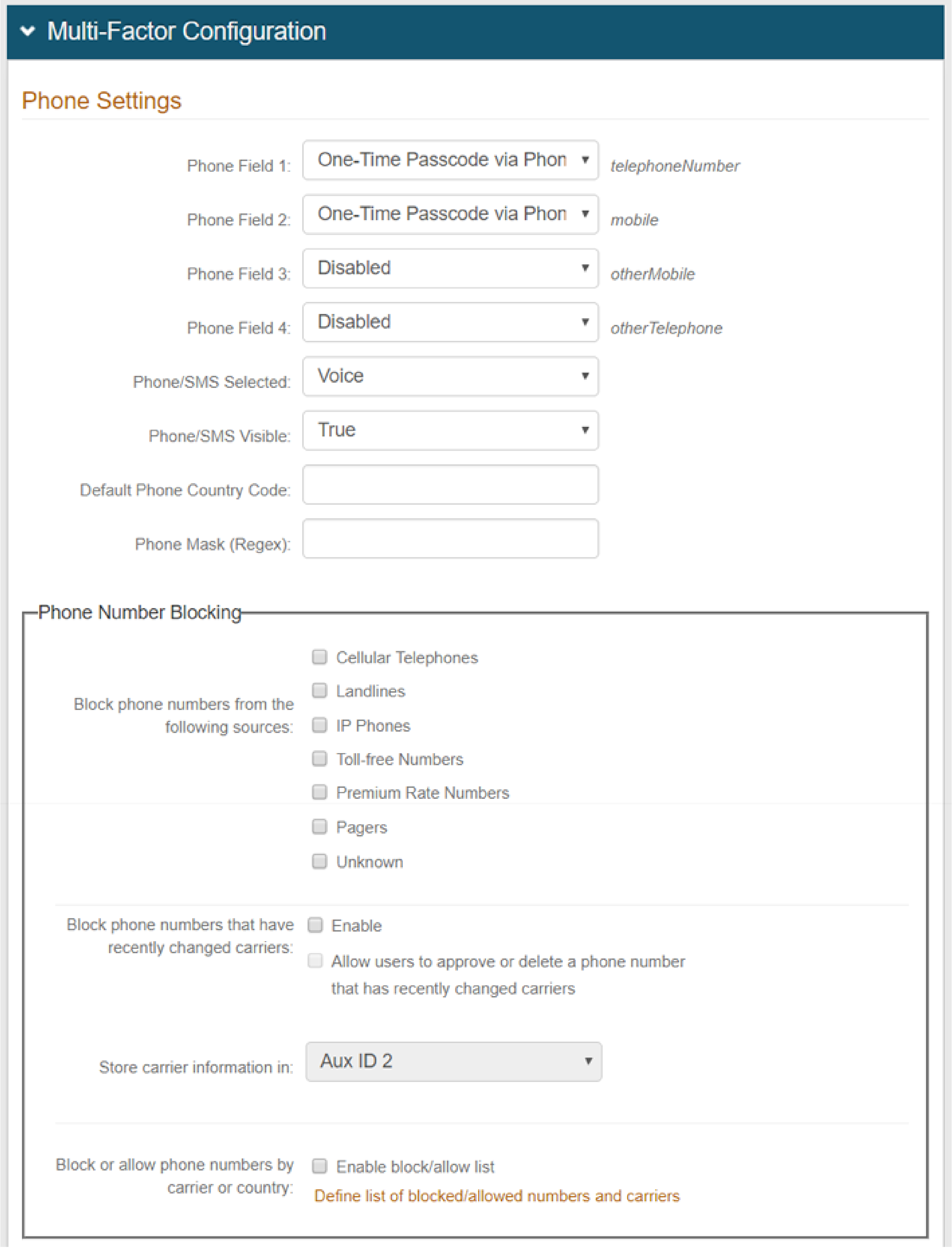
NOTE: For the complete Workflow configuration steps, refer to Workflow configuration.

Multi-Factor Methods tab

NOTE: Multi-Factor Methods configuration steps are only required if using Multi-Factor Authentication for remote access.

17. In the Multi-Factor Configuration section, enable at least one authentication method if a **Default Workflow** for Multi-Factor Authentication is configured on the **Workflow** tab.

18. **Save** the configuration.



Multi-Factor Configuration

Phone Settings

Phone Field 1:	One-Time Passcode via Phon	*telephoneNumber*
Phone Field 2:	One-Time Passcode via Phon	*mobile*
Phone Field 3:	Disabled	*otherMobile*
Phone Field 4:	Disabled	*otherTelephone*
Phone/SMS Selected:	Voice	
Phone/SMS Visible:	True	
Default Phone Country Code:		
Phone Mask (Regex):		

Phone Number Blocking

Block phone numbers from the following sources:
- □ Cellular Telephones
- □ Landlines
- □ IP Phones
- □ Toll-free Numbers
- □ Premium Rate Numbers
- □ Pagers
- □ Unknown

Block phone numbers that have recently changed carriers:
- □ Enable
- □ Allow users to approve or delete a phone number that has recently changed carriers

Store carrier information in: Aux ID 2

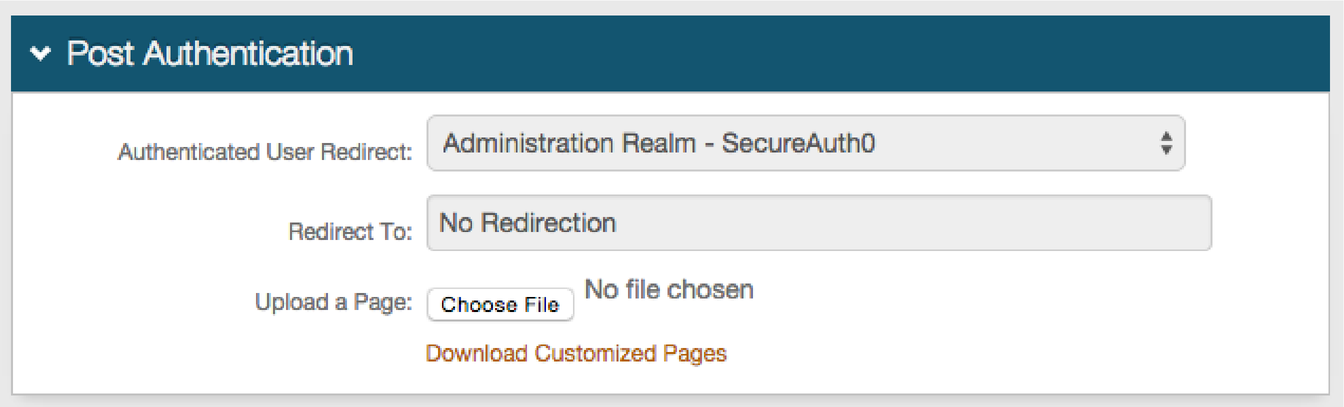
Block or allow phone numbers by carrier or country:
- □ Enable block/allow list

Define list of blocked/allowed numbers and carriers

NOTE: For the complete Multi-Factor Methods configuration steps, refer to Multi-Factor Methods configuration.

Post Authentication tab

19. In the Post Authentication section, the **Authenticated User Redirect** and **Redirect To** fields are auto-populated by default.



Post Authentication

Authenticated User Redirect: Administration Realm - SecureAuth0

Redirect To: No Redirection

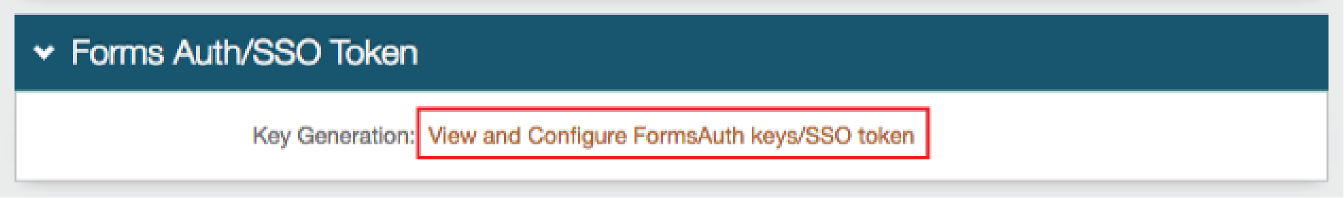
Upload a Page: Choose File No file chosen

Download Customized Pages

20. **Save** the configuration.

21. OPTIONAL: Click **View and Configure FormsAuth keys / SSO token** to configure SecureAuth0's token / cookie settings.

NOTE: See Configure token or cookie settings.



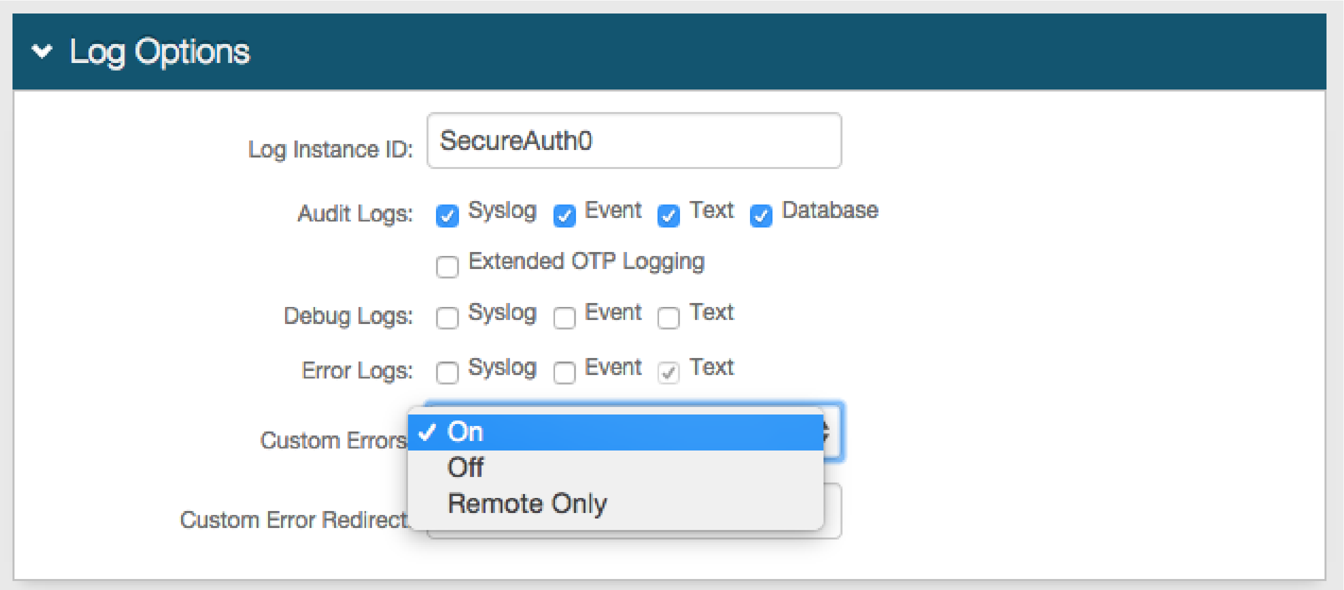
Forms Auth/SSO Token

Key Generation: View and Configure FormsAuth keys/SSO token

Logs tab

22. In the Log Options section, provide the **Log Instance ID** – for example, the Application Name or the realm name (SecureAuth0)

23. Enable the logs to use under the **Audit**, **Debug**, and **Error Logs** sections.



Log Options

Log Instance ID: SecureAuth0

Audit Logs: ☑ Syslog ☑ Event ☑ Text ☑ Database

□ Extended OTP Logging

Debug Logs: □ Syslog □ Event □ Text

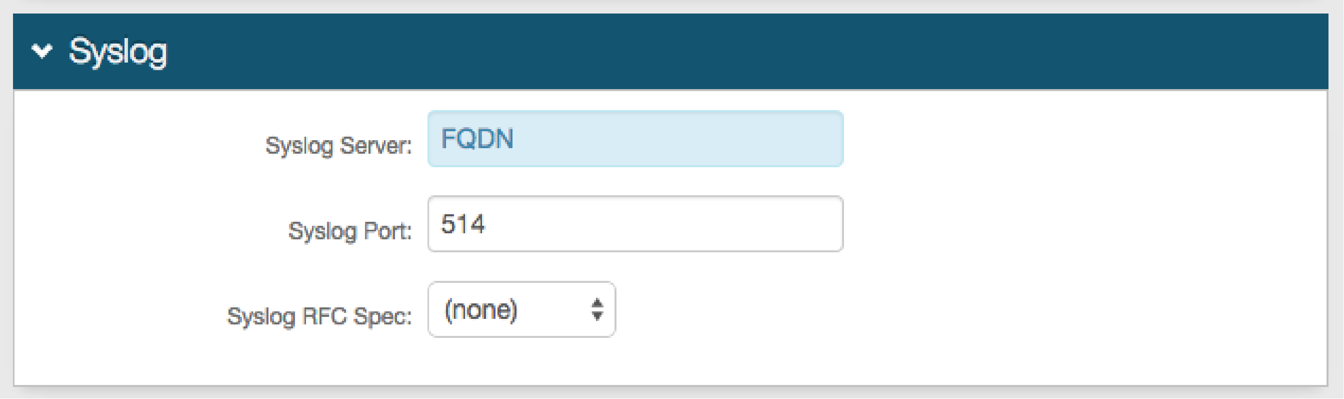
Error Logs: □ Syslog □ Event ☑ Text

Custom Errors: ✓ On
Off
Remote Only

Custom Error Redirect:

24. If SysLog is enabled, then provide the **FQDN** or **IP Address** of the **Syslog Server**.

25. Provide the **SysLog Port** number.



Syslog

Syslog Server: FQDN

Syslog Port: 514

Syslog RFC Spec: (none)

26. If Database is enabled, then configure the following settings:

   a. Data Source – Provide the **FQDN** or the **IP Address** of the database.

   b. Initial Catalog: Provide the **Database Name**.

   c. Integrated Security – If the web page's ID is to be included in the Connection String, then select **True**.

   d. Persist Security Info – Select **True** if access to username and password information is allowed.

   e. Connection Timeout – Set an amount of time (in seconds) before the connection times out and the admin must re-authenticate.

   f. User ID – Provide the **User Id** of the database.

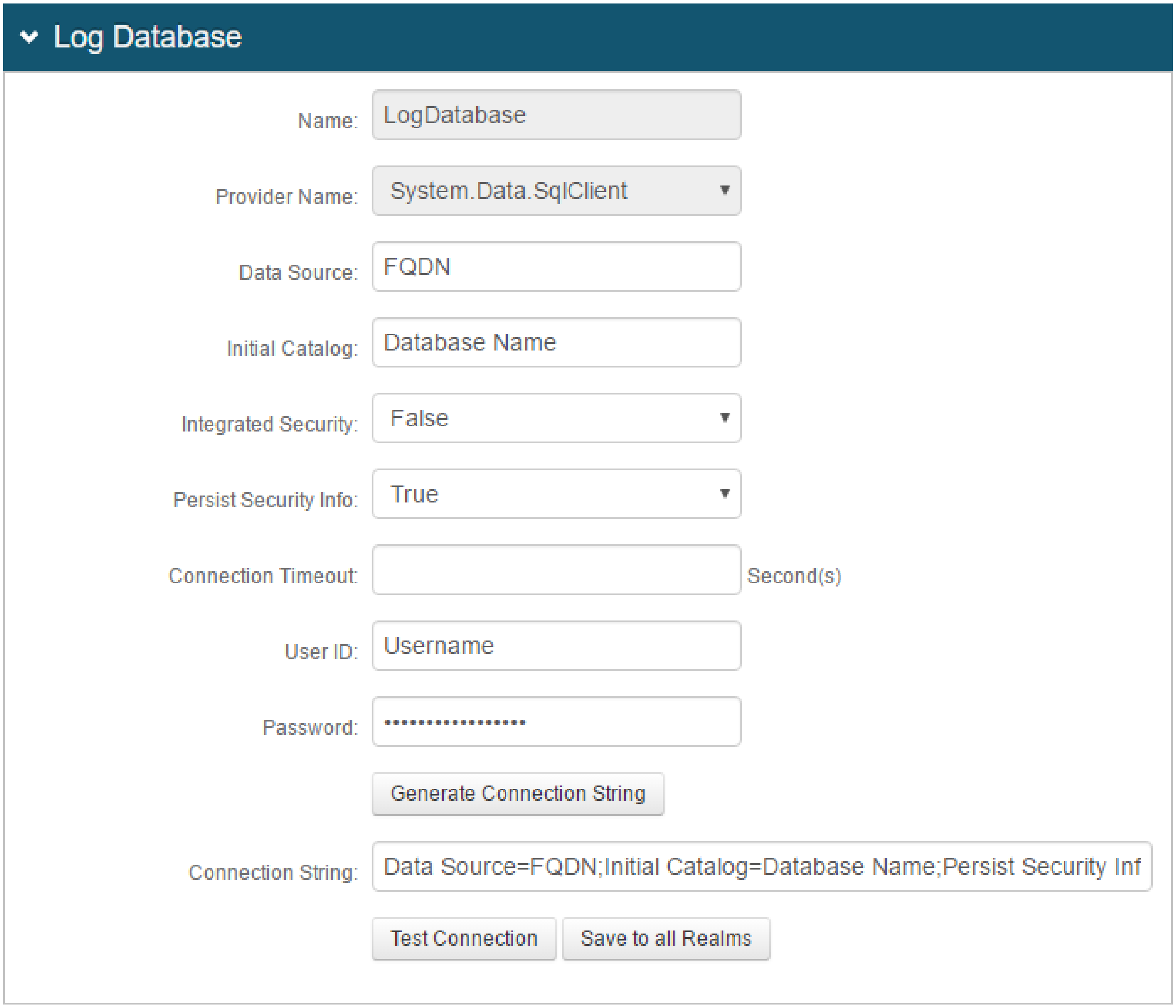
   g. Password – Provide the **Password** associated with the **User ID**.

   h. Click **Generate Connection String**.

   The **Connection String** auto-populates with content based on the previous fields.

27. Click **Test Connection** to ensure the integration is successful.

28. If these Database settings are to be used on each SecureAuth IdP realm, then click **Save to all Realms**.



Log Database

Name: LogDatabase

Provider Name: System.Data.SqlClient

Data Source: FQDN

Initial Catalog: Database Name

Integrated Security: False

Persist Security Info: True

Connection Timeout: Second(s)

User ID: Username

Password: •••••••••••••••••

Connection String: Data Source=FQDN;Initial Catalog=Database Name;Persist Security Inf

29. **Save** the configuration.

NOTE: For all Logs configuration steps, refer to Logs Tab Configuration.

What's Next

Move on to Part III: Configure a blueprint realm to configure a realm with common settings that should be used across all realms.

Additional information

- Learn more about realms in Work with SecureAuth IdP realms.
- See Third-Party Integration & Configuration Guides for specific configuration and integration guides. Additional methods of support are listed below.

Support options

- Support web portal: https://support.secureauth.com
- Phone: 949-777-6959, option 2
- Support documentation, searchable database: https://docs.secureauth.com
- SecureAuth services status and notification service: http://status.secureauth.com