Setting up Adminbot and Auditbot

Overview

Adminbot allows for an Element Administrator to become admin in any existing room or space on a managed homeserver. This enables you to delete rooms for which the room administrator has left your company and other useful administration actions.

Auditbot allows you to have the ability to export any communications in any room that the auditbot is a member of, even if encryption is in use. This is important in enabling you to handle compliance requirements that require chat histories be obtainable.

On using Admin Bot and Audit Bot

Currently, we deploy a special version of Element Web to allow you to log in as the adminbot and auditbot. Given this, please do not make changes to widgets in rooms while logged in as the adminbot or the auditbot. The special Element Web does not have any custom settings that you have applied to the main Element Web that your users use and as such, you can cause problems for yourself by working with widgets as the adminbot and auditbot. In the future, we are working to provide custom interfaces for these bots.

Configuring Admin Bot

From the Installer's Integrations page, click "Install" under "Admin Bot"

You will then see the following:

Adminbot

Remove

Deploys an Adminbot which automatically joins rooms. Admins can manage rooms by impersonating the Adminbot.

Secrets / Adminbot

Show Values

Config

(•) Configure Adminbot ( ) Enable Central Adminbot Access

Bot

The adminbot configuration

[ ] Enable DM Admin

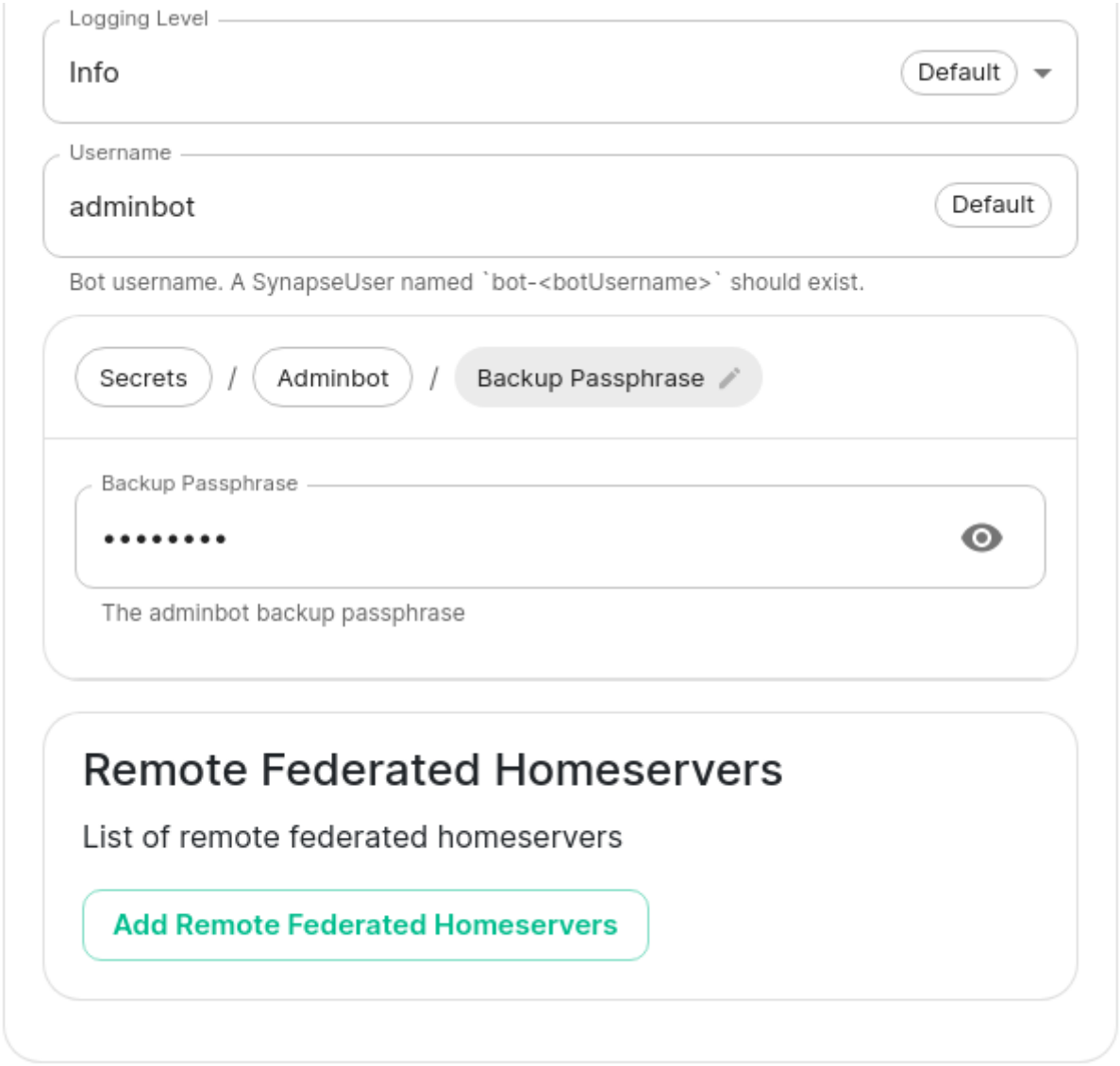
Enable admin of Direct Messages

Default

[x] Join Local Rooms Only

Audit only rooms local to the homeserver

Default



Your first choice is to configure adminbot or enable this server as part of a federated adminbot cluster. For most cases, you'll want to select "Configure Adminbot".

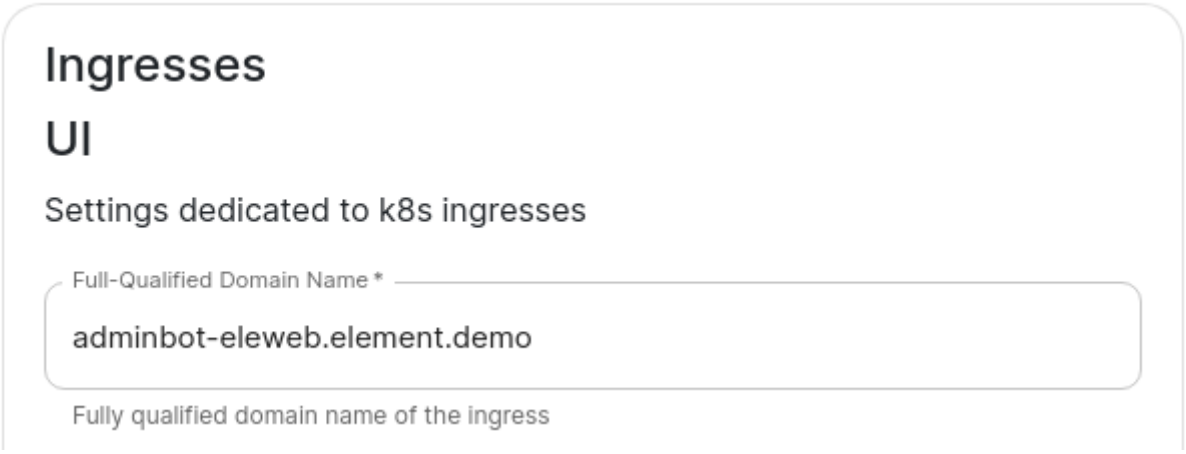
Below this, we have a checkbox to either allow the adminbot to participate in DM rooms (rooms with 1-2 people) or not.

We also have a checkbox to join local rooms only. You probably want to leave this on. If you turn it off, the adminbot will try to join any federated rooms that your server is joined to.

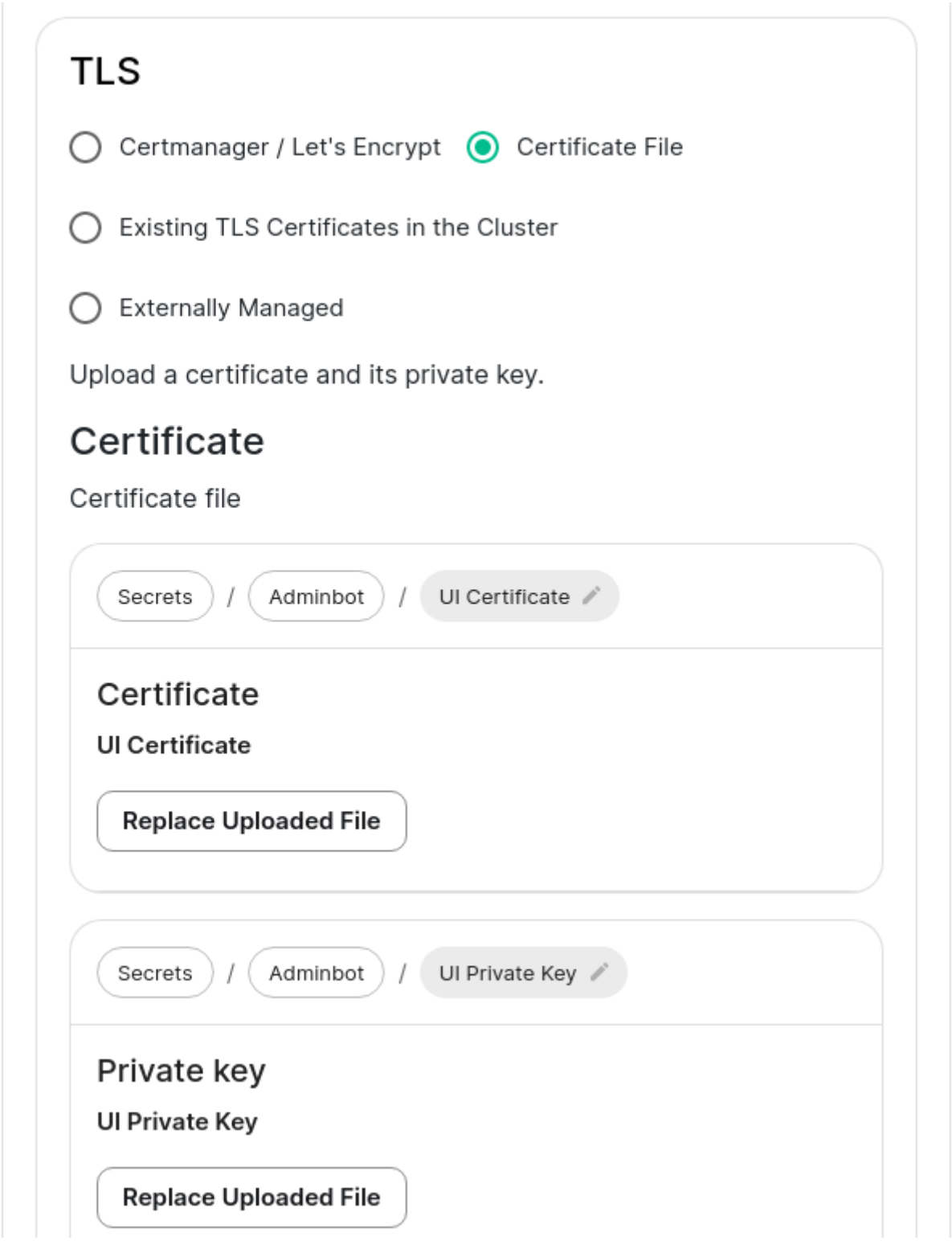
Moving on, we also have the ability to change the logging level and set the username of the bot.

After this, we have the ability to set the "Backup Passphrase" which is used to gain access to the key backup store.

Two settings that need to be set in the "Advanced" section are the fqdn for the adminbot element web access point and its certifactes. These settings can be found by clicking "Advanced" and scrolling to:


Ingresses
UI
Settings dedicated to k8s ingresses
Full-Qualified Domain Name *
adminbot-eleweb.element.demo
Fully qualified domain name of the ingress

and then:



Configuring Audit Bot

From the Installer's Integrations page, click "Install" under "Audit Bot".

You will then see the following:

Auditbot

Remove

Deploys an Auditbot which automatically joins rooms and logs every messages to configured outputs.

Config

(•) Configure Auditbot ( ) Enable Central Auditbot Access

Bot

The auditbot configuration

[x] Enable DM Audit

Enable audit of Direct Messages

[x] Join Local Rooms Only

Audit only rooms local to the homeserver

Default

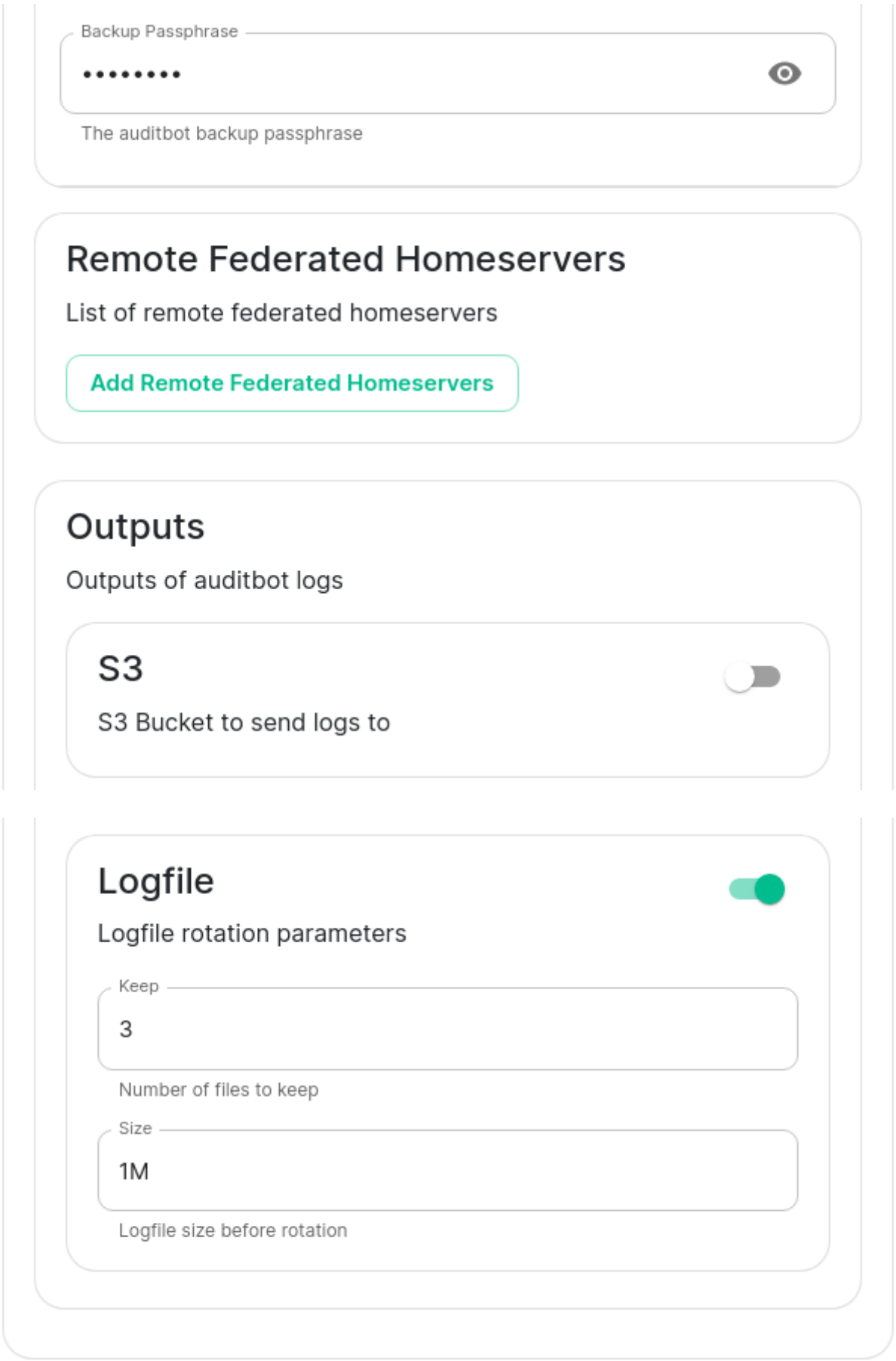
Logging Level

Debug

Username

auditbot Default

Bot username.



Your first choice is to configure auditbot or enable this server as part of a federated auditbot cluster. For most cases, you'll want to select "Configure Auditbot".

Below this, we have a checkbox to either allow the adminbot to participate in DM rooms (rooms with 1-2 people) or not.

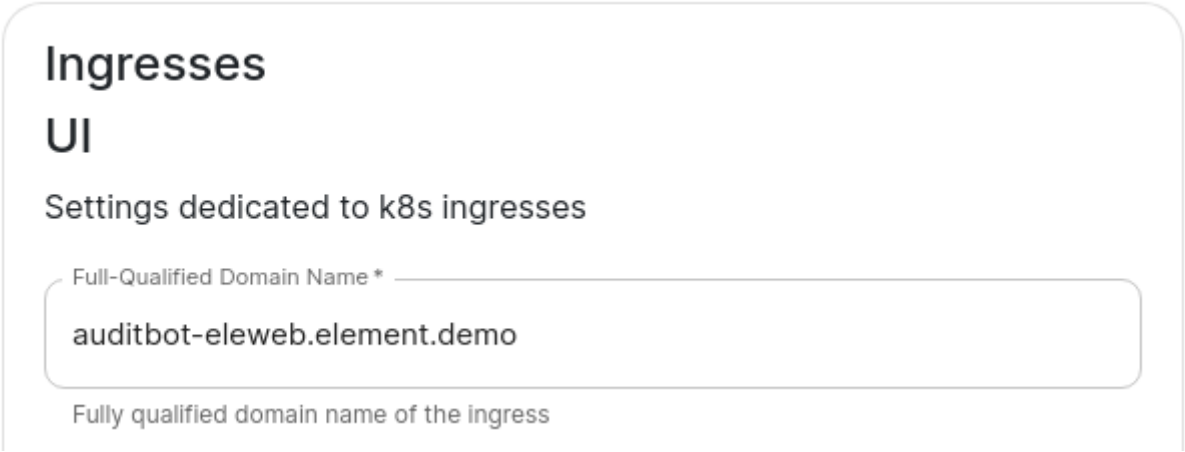
We also have a checkbox to join local rooms only. You probably want to leave this on. If you turn it off, the adminbot will try to join any federated rooms that your server is joined to.

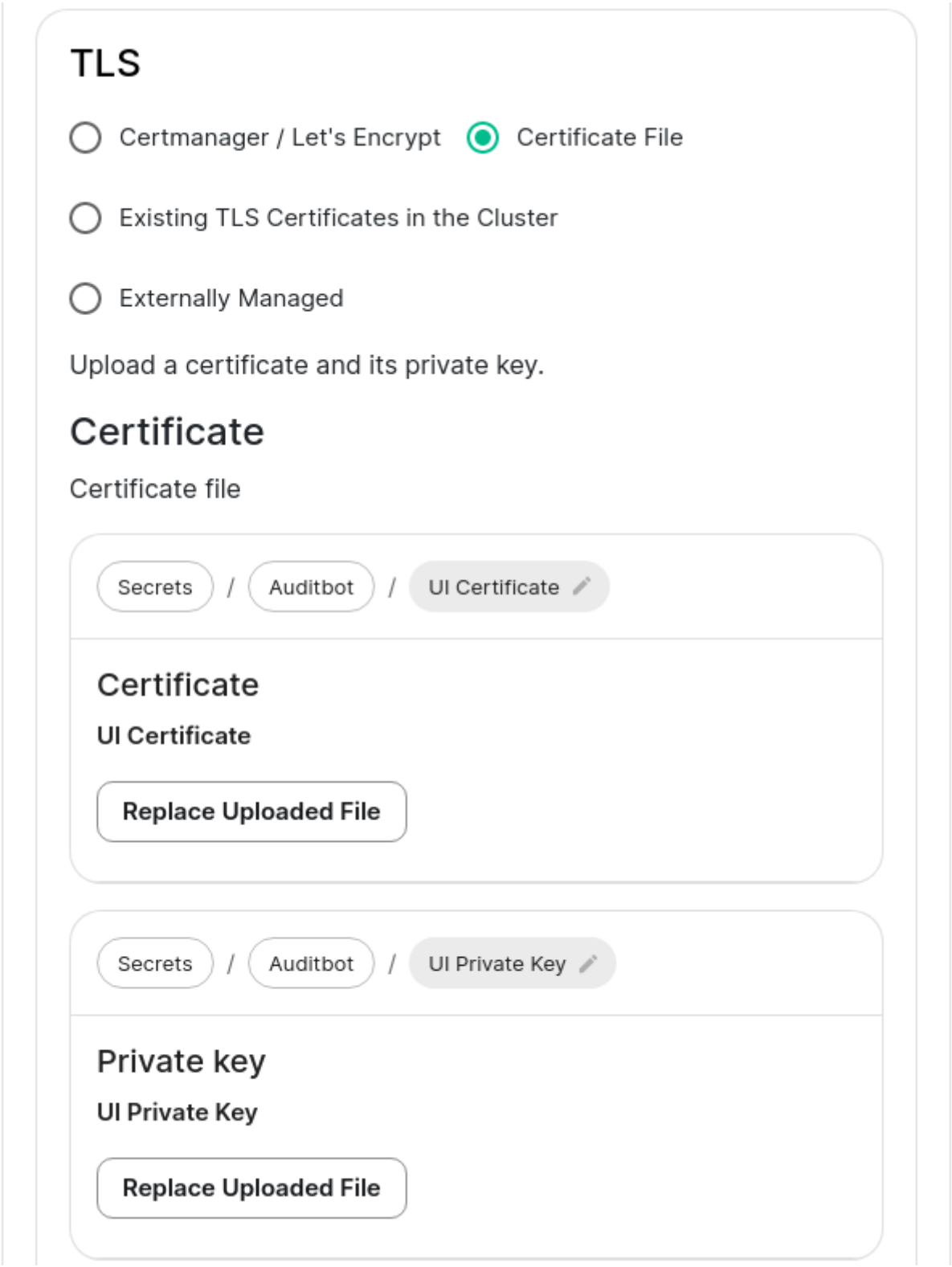
Moving on, we also have the ability to change the logging level and set the username of the bot.

After this, we have the ability to set the "Backup Passphrase" which is used to gain access to the key backup store.

You can also configure an S3 bucket to log to and you can configure how many logfiles should be kept and how large a log file should be allowed to grow to. By default, the auditbot will log to the storage that has been attached by the cluster (check the storage settings under the "Advanced" tab).

Two settings that need to be set in the "Advanced" section are the fqdn for the auditbot element web access point and its certifactes. These settings can be found by clicking "Advanced" and scrolling to:

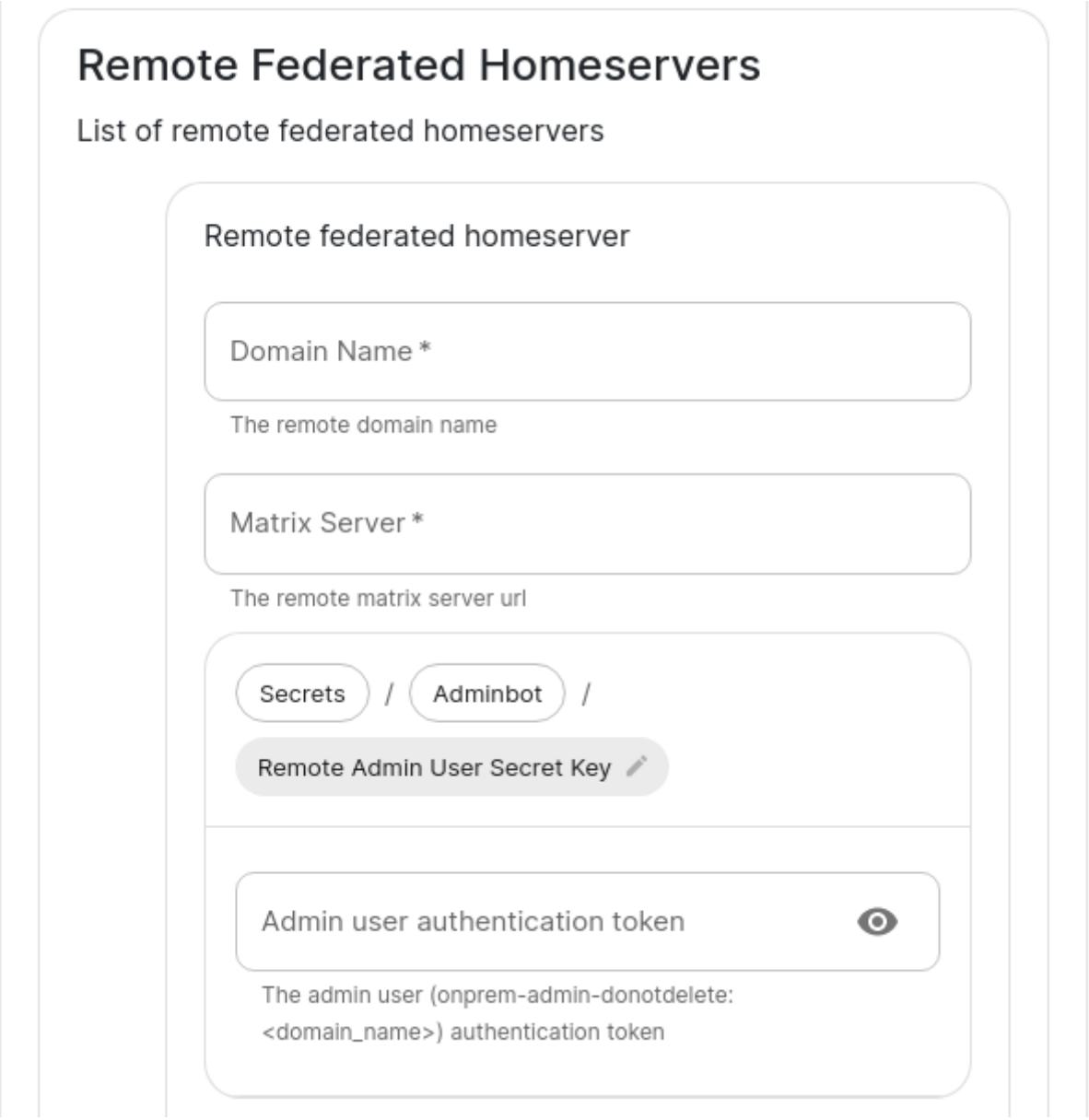


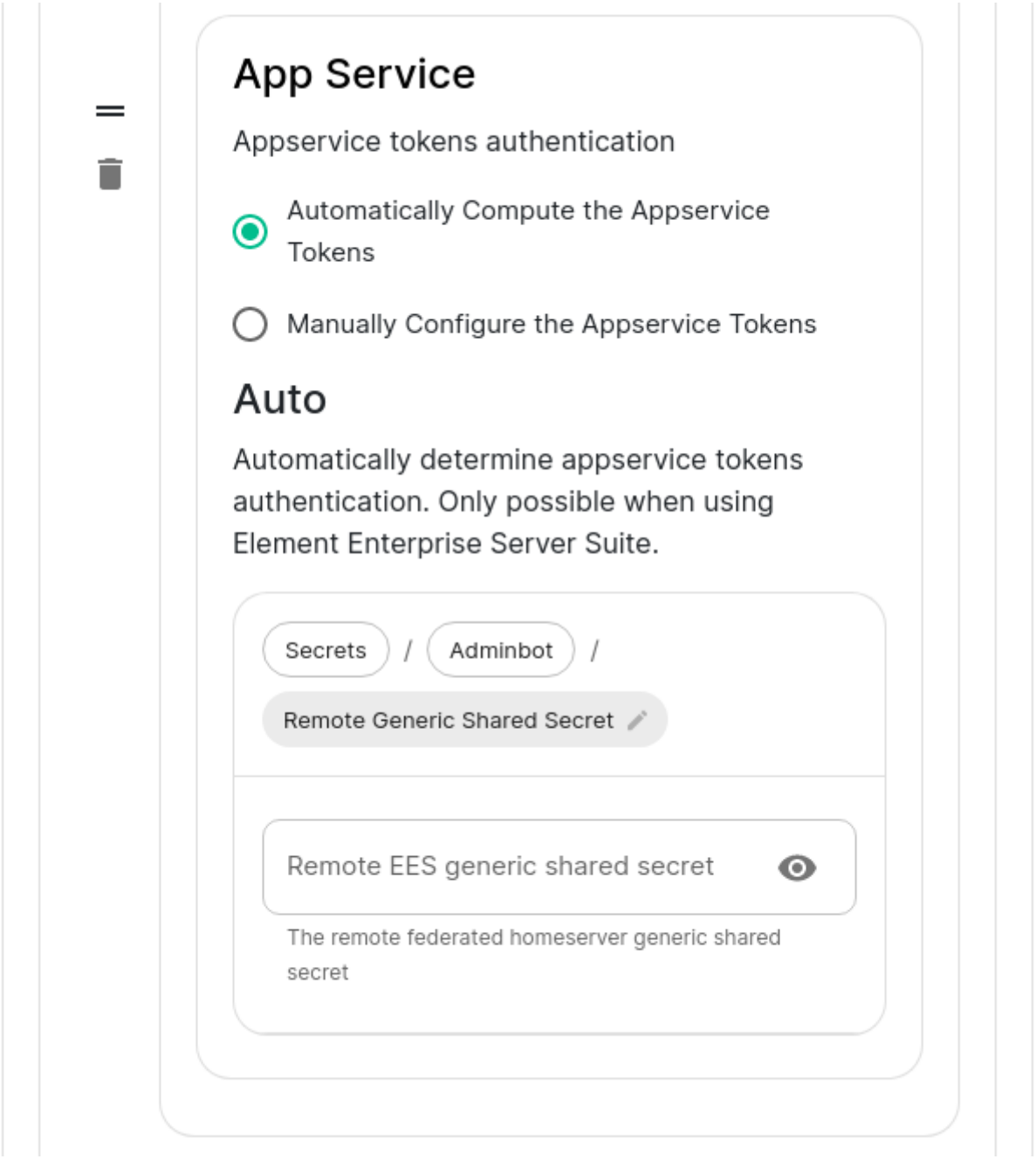


Adminbot Federation

On the central admin bot server

You will pick "Configure Admin Bot" and will fill in everything from the above Adminbot configuration instructions, but you will also add Remote Federated Homeservers in this interface:





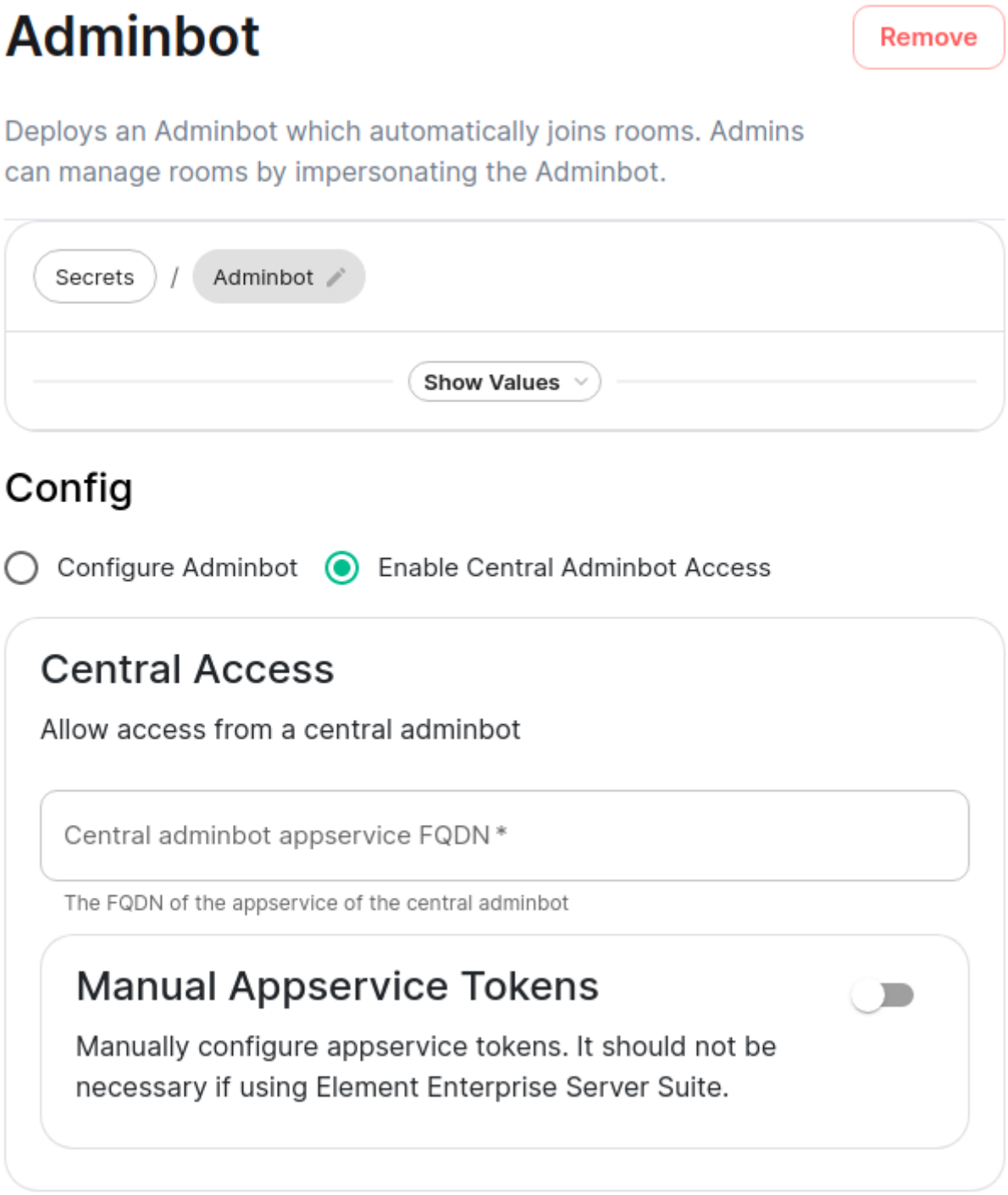
You will need to fill out this form for each remote server that will join the federation. You will need to set the domain name and the matrix server for each to get started.

You will also need to grab the Admin user authentication token for each server and specify that here. You may get this with the following command run against a specific server: `kubectl get synapseusers/adminuser-donotdelete -n element-onprem -o yaml`. You are looking for the value of the field `status.accessToken`.

Then in the app service, you can leave Automatically compute the appservice tokens set. You will need to also get the generic shared secret from that server and specify it here as well. You can get this value from running: `kubectl get -n element-onprem secrets first-element-deployment-synapse-secrets -o yaml | grep registration` and looking at the value for the registrationSharedSecret.

On the remote admin bot server

Instead of selecting "Configure Adminbot", you will pick "Enable Central Adminbot Access" and will then be presented with this UI:

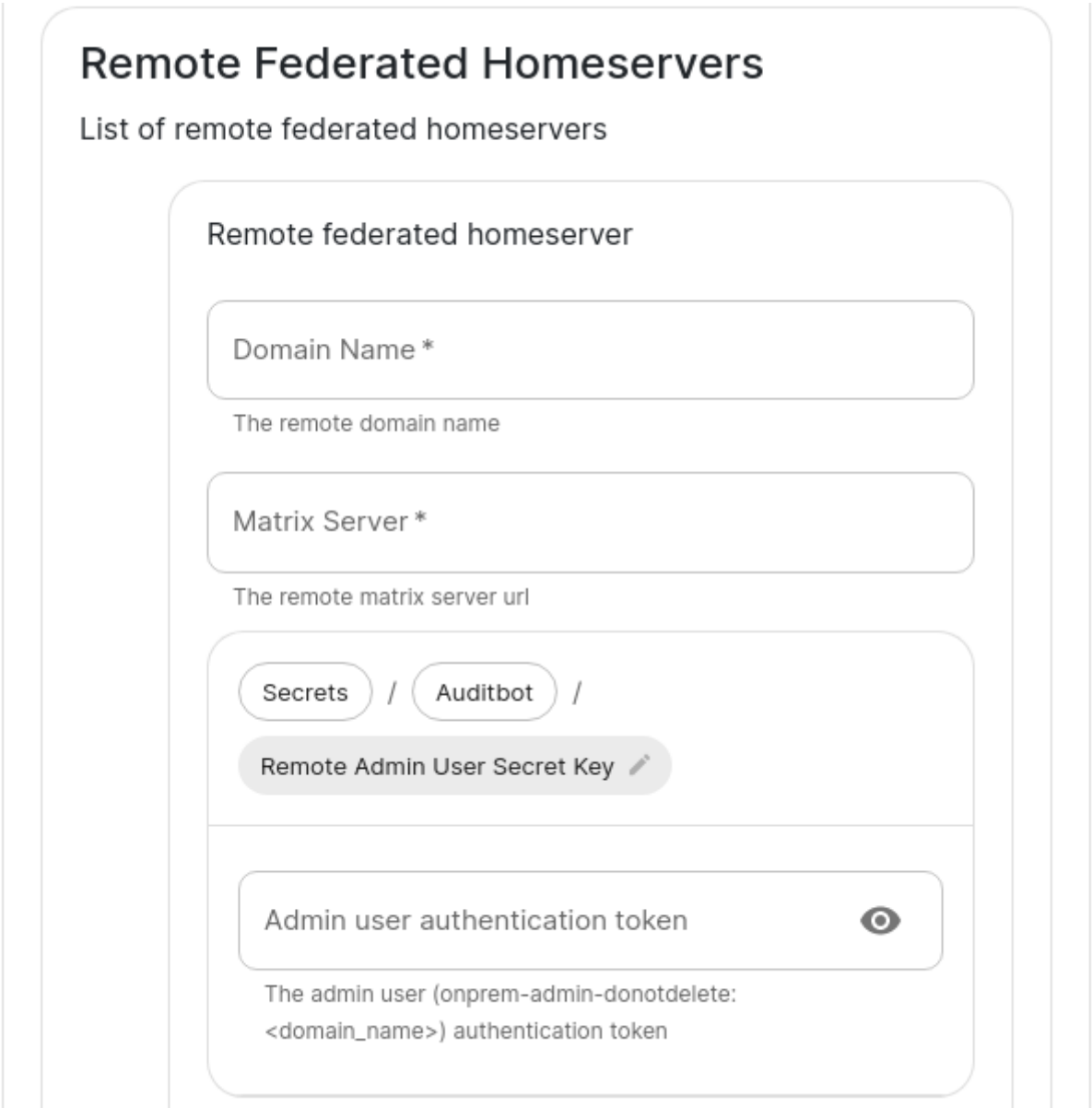


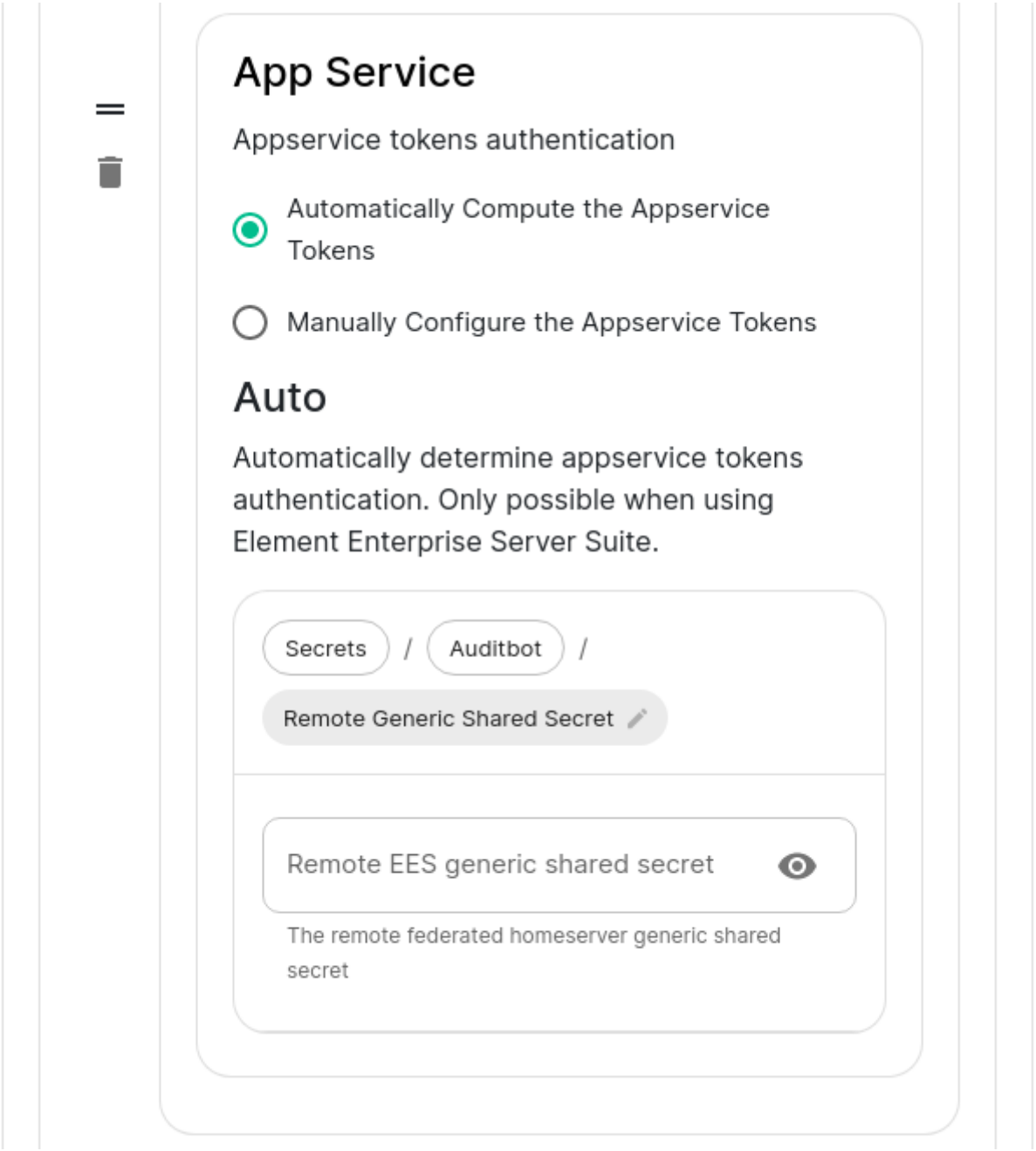
You will then specify the FQDN of the central adminbot server.

Auditbot Federation

On the central auditbot server

You will pick "Configure Audit Bot" and will fill in everything from the above Auditbot configuration instructions, but you will also add Remote Federated Homeservers in this interface:





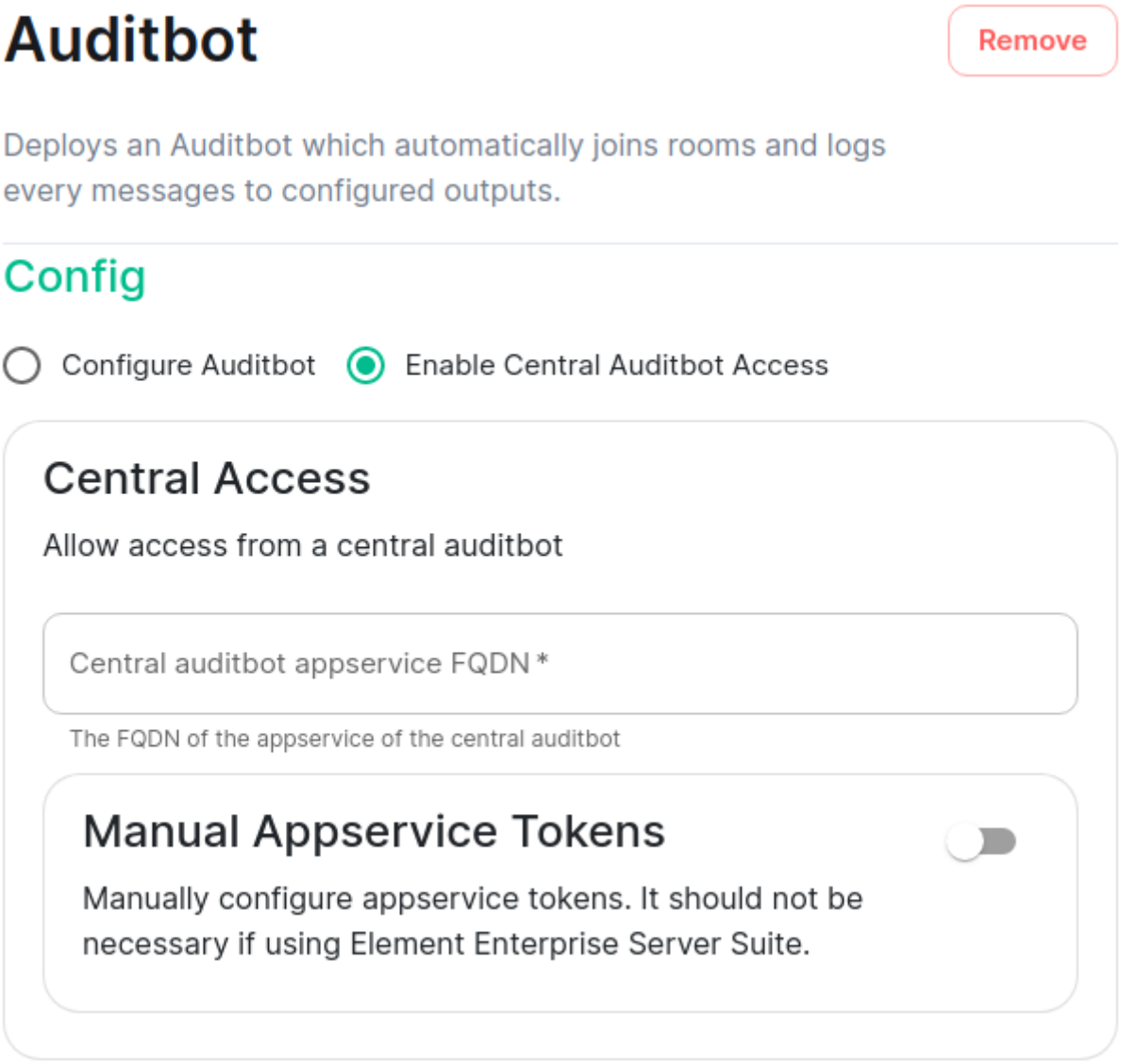
You will need to fill out this form for each remote server that will join the federation. You will need to set the domain name and the matrix server for each to get started.

You will also need to grab the Admin user authentication token for each server and specify that here. You may get this with the following command run against a specific server: `kubectl get synapseusers/adminuser-donotdelete -n element-onprem -o yaml`. You are looking for the value of the field `status.accessToken`.

Then in the app service, you can leave Automatically compute the appservice tokens set. You will need to also get the generic shared secret from that server and specify it here as well. You can get this value from running: `kubectl get -n element-onprem secrets first-element-deployment-synapse-secrets -o yaml | grep registration` and looking at the value for the registrationSharedSecret.

On the remote audit bot server

Instead of selecting "Configure Auditbot", you will pick "Enable Central Auditbot Access" and will then be presented with this UI:



You will then specify the FQDN of the central auditbot server.

Revision #3
Created 23 August 2024 08:22:20 by Kieran Mitchell Lane
Updated 6 November 2024 13:21:29 by Kieran Mitchell Lane