LOADBALANCER

MANUALS

Loadbalancer.org ADC Portal

Version 1.0.3

Table of Contents

1. Introduction

The ADC Portal is an ultra-secure, cloud-based ADC management platform that enables ADCs from multiple vendors to be centrally monitored and managed. ADCs from F5, Citrix Netscaler, Progress Kemp and Loadbalancer.org are currently supported.

Enhance Visibility

The ADC Portal provides a single consolidated view of all load balancing assets, wherever they are located. Key information such as the operational state, HA status, software version and IP address of all ADCs can easily be viewed. ADCs can be grouped and organised using custom Namespaces and Tags to simplify management. One-click access to any ADC's WebUI directly from the Portal is also provided whether the ADC is located locally or in a completely different network.

Improve Security

The Portal simplifies security management in multiple ways. Continuous, real-time CVE (Common Vulnerabilities and Exposure) monitoring of all ADCs ensures that any issues found are highlighted and can be promptly dealt with. SSL certificates installed on each ADC are also monitored and any that have expired or are expiring soon are highlighted. Software update notifications to inform when a new version is available for each ADC is coming soon.

Automate Tasks

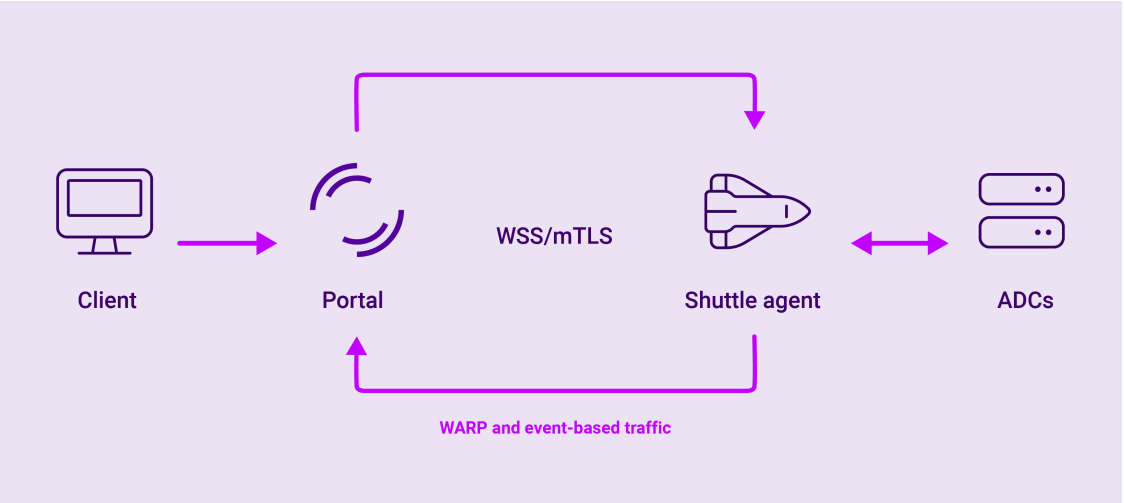
ADC backups can be scheduled to run once or on a daily, weekly, monthly or annual cadence. Each backup is encrypted and securely stored in the ADC Portal and can be easily viewed, restored, downloaded for storage elsewhere or deleted. The ability to schedule other tasks including software updates is coming soon.

2. Technology

The ADC Portal is built on a zero-trust security model and uses full end-to-end encryption. This approach ensures that all data within the Portal is always encrypted (both at rest and in transit) using a unique pair of organisation and account private keys. This means that no one can ever see or read your data, and that all data encryption and decryption occurs within your own environment.

2.1. Communication

All communication takes place via a secure WebSocket protocol (WSS) with mTLS. With mTLS, the client is required to present its certificate to the server (and visa versa). Hence mutual certificate authentication occurs. This double layer of authentication provides an additional layer of protection against impersonation attacks. And it is only once this two-way authentication has taken place that a secure connection is established, leading to the exchange of data.



Within this encrypted WSS channel, there are two methods of communication:

Event-driven requests

Explicitly defined requests are sent as events to the Shuttle for added security and efficiency.

Remote HTTP proxy

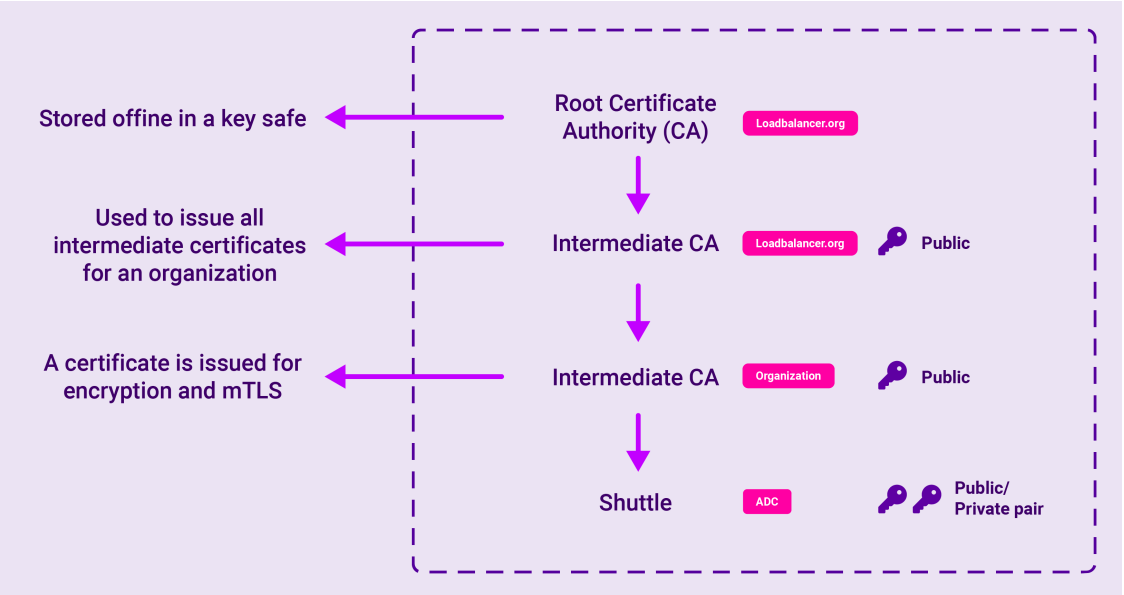
This is a WARP-enabled, remote HTTP proxy to your network. It allows you to see the WebUI of each appliance and provides a facility to manage it over an encrypted connection across the Loadbalancer.org ADC Portal network.

2.1.1. WARP

WARP is a proxy that helps you connect to the internet while simultaneously optimizing and securing (i.e. encrypting) your connection, giving you access to you appliance, no matter where you are.

2.1.2. PGP Encryption for Extra Security

In addition to the secure WebSocket encryption outlined above, the Portal also contains a second layer of security: PGP encryption.



Once the initial mTLS handshake has been completed, the Shuttle then creates its own PGP keys, which are then used for communication and verification with the ADCs. However, before data can be transferred from the client to the Shuttle, it must first pass through an intermediary key. This Certificate Chain enables the receiver to verify that the sender and all Certificate Authorities are trustworthy.

Every user needs not only their own private key, but also a copy of the organisation key to read the data that's coming in from the Shuttle. This means new users will need to be invited by the organisation to register, and actively given a copy of the organisation key (as well as activating their own private user key). In this way it is the organisation who is the owner of everything - not the user.

And with the potential for multiple levels of encryption using different keys, it would be almost impossible to decrypt what is imprinted on the public key without also being in possession of a private key. In this way, if someone were to compromise or intercept the messages being transmitted by the Shuttle, break the TLS encryption and obtain the encrypted PGP data, they would still need the Shuttle's private key to be able to read it.

In this way, data communications are sent via the Shuttle which acts as an intermediary or sidecar agent. but the Shuttle is unable to read these messages. Its only role is to act as a vector to forward this information when, and only when, the private and public keys match.

2.2. ADC Communication Services & Methods

As discussed above, the Shuttle is a key component in ADC portal communication. In addition, the gateway service is used on Loadbalancer.org appliance and API calls are used with 3rd party appliances.

Shuttle Service

A Shuttle can be provisioned as a standalone Linux instance running the Shuttle service or as a Loadbalancer.org ADC appliance with its Shuttle service enabled.

Gateway Service

The gateway service applies to Loadbalancer.org ADC appliances only. When enabled, it's used to gather Loadbalancer.org appliance details and pass them to a Shuttle. It also enables appliance backups and other remote tasks to be run.

Vendor Specific API Calls

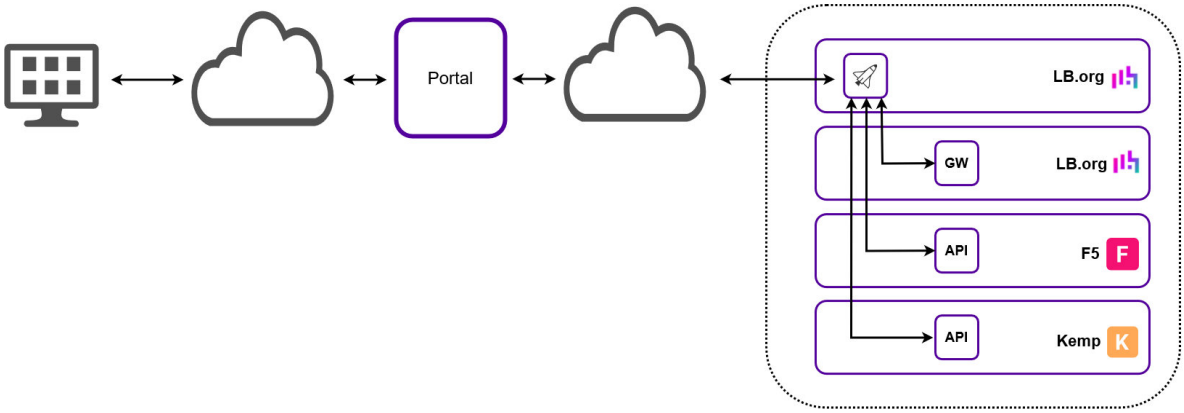
Used to gather details for ADC appliances from 3rd party vendors and pass them to a Shuttle. API calls are also used to control ADC appliance backups and other remote tasks.

2.3. Connection Options

There are a number of ways that the connection to the ADC Portal can be provided. The sections below describe each option.

2.3.1. Single Shared Connection with Single Dedicated Shuttle

All Portal communication is handled by a dedicated Shuttle separate from all load balancing workload.



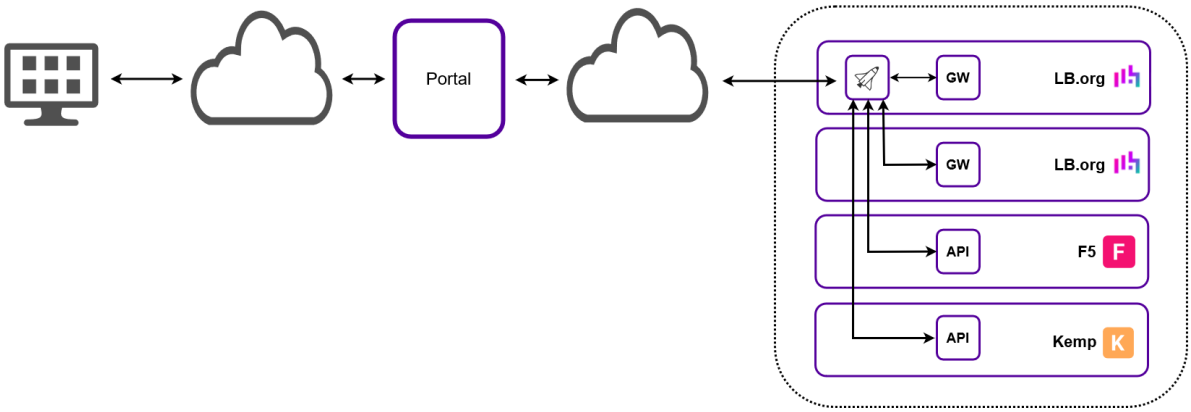
- Requires a single shared connection to the ADC Portal.
- Requires a single Shuttle, this can be either:
  - A Standalone Shuttle.
  - A dedicated Loadbalancer Enterprise appliance with the Shuttle service enabled.
- All appliances communicate with the ADC Portal via the standalone Shuttle/dedicated loadbalancer.org ADC.

> **Note**
>
> If the Shuttle is to be used to monitor & control ADCs in remote subnets, those subnets must be configured on the Shuttle (subnets can be configured for the standalone Shuttle only). For more information, please refer to Network Topology. Alternatively, an additional Shuttle can be added to each remote subnet to serve those ADCs.

- The Gateway service on each Loadbalancer.org appliance must be enabled.
- The API must be enabled on all non Loadbalancer.org appliances.

2.3.2. Single Shared Connection with Single Non-Dedicated Shuttle

All Portal communication is handled by a designated Loadbalaner.org appliance in addition to its own load balancing workload.



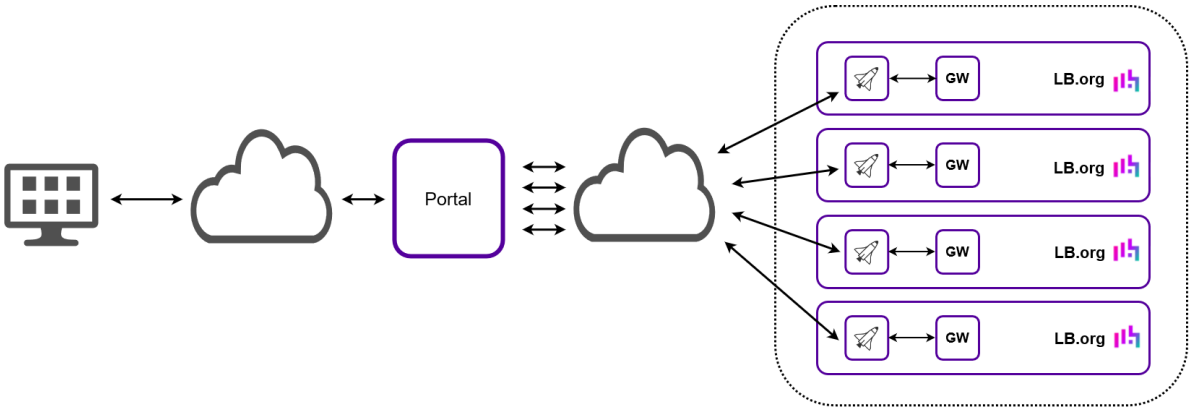
- Requires a single shared connection to the ADC Portal.
- Requires a single Shuttle - the Shuttle service on a Loadbalancer.org ADC must be enabled.
- All appliances communicate with the ADC Portal via the Shuttle service on the chosen ADC.

> **Note**
>
> The Shuttle should be deployed in a subnet that has access to all ADCs to be monitored & managed. If this is not possible, an additional Shuttle can be added to each remote subnet to serve those ADCs. Alternatively, a standalone Shuttle with all remote subnets configured can be used as described in Single Shared Connection with Single Dedicated Shuttle.

- The gateway service on each Loadbalancer.org appliance must be enabled.
- The API must be enabled on all non Loadbalancer.org appliances.

2.3.3. Multiple Connections and Multiple Non-dedicated Shuttles (Loadbalancer.org ADCs Only)

Each Loadbalancer.org appliance handles its own Portal communication in addition to its own load balancing workload.



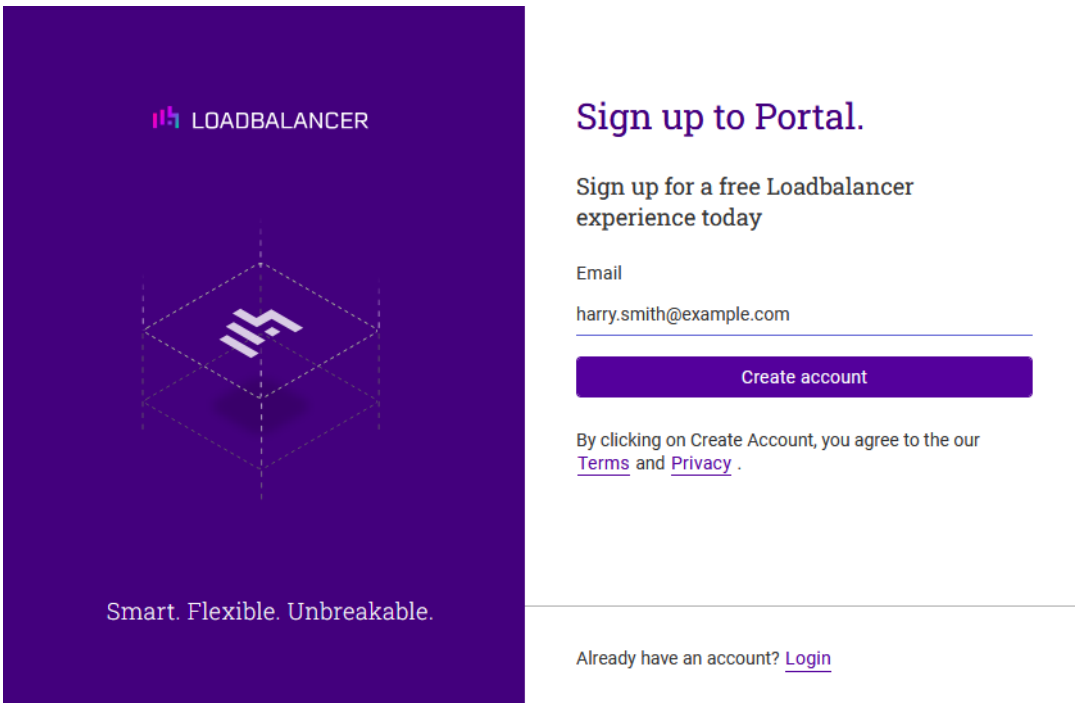
- Each appliance has its own connection to the Portal.
- The gateway and Shuttle services on each Loadbalancer.org appliance must be enabled.

3. Getting Started

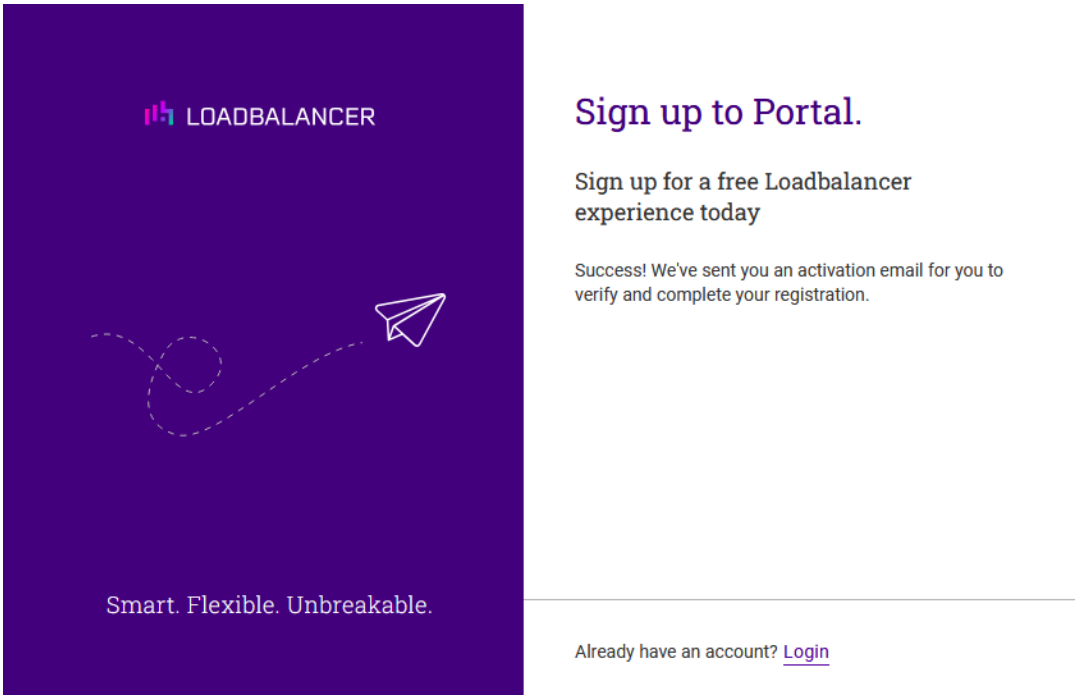
3.1. Account Creation

> **Important**
>
> If a new user requires access to an existing organisation, the user must be created within that organisation. For more details, please refer to User Management.

1. Navigate to the ADC Portal home page (https://portal.loadbalancer.org) and click the **Create account** link.

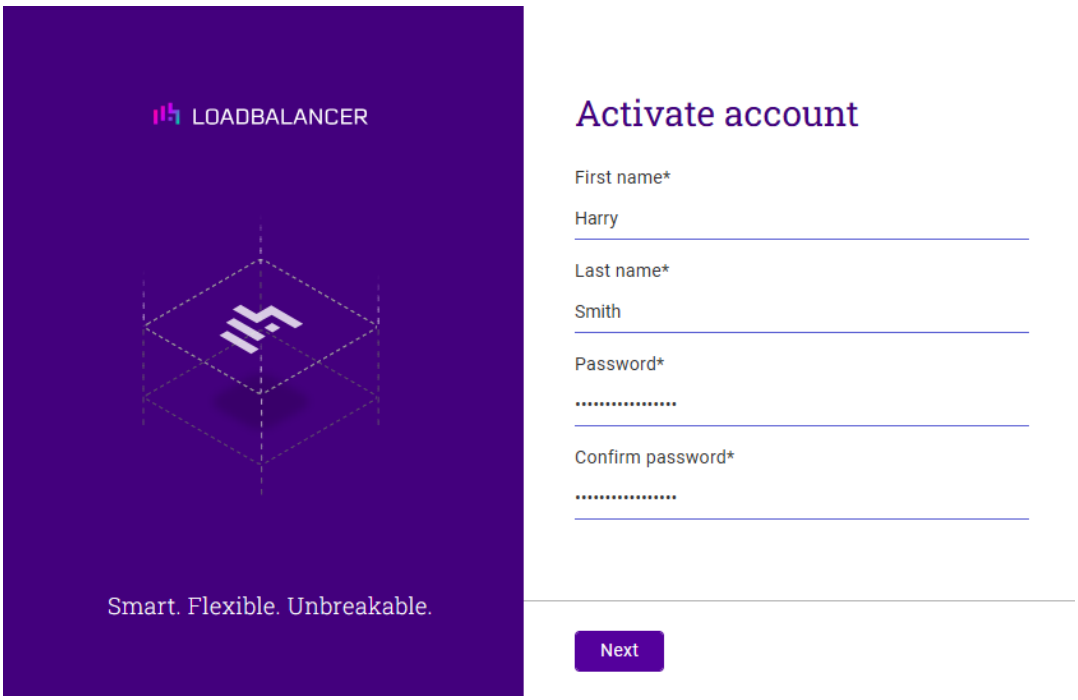


2. Enter the email address to be associated with the new account and click **Create account**.

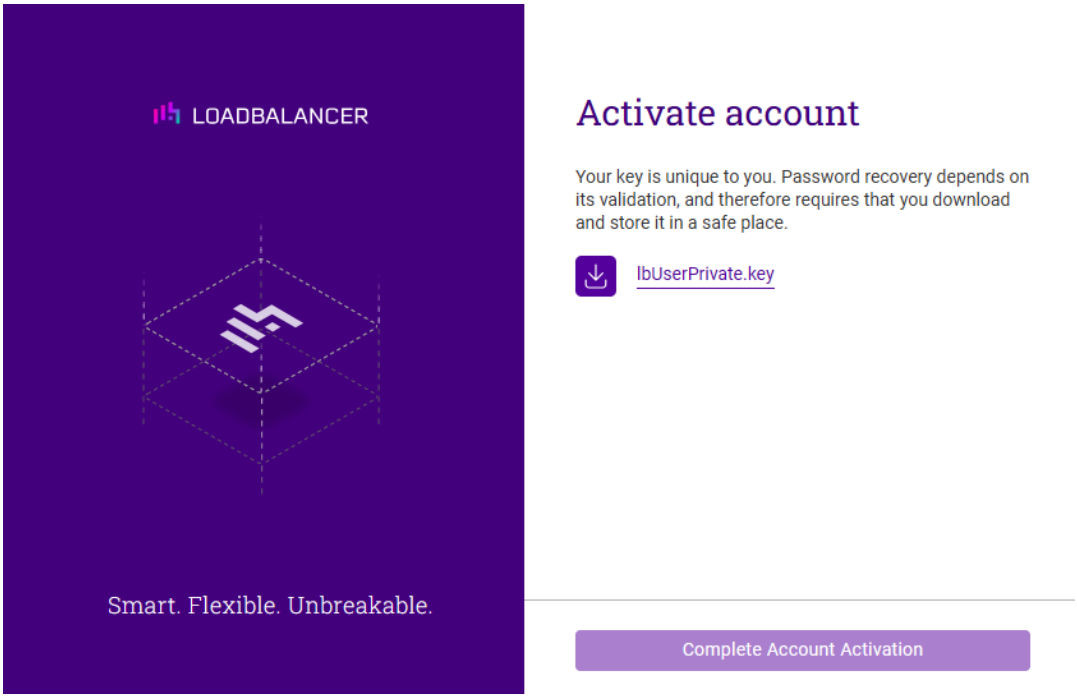


3. An activation email will be sent to the email address provided to verify and complete your registration. Open the email and click on the link to start the account activation process.

> **Note** If the activation email doesn't arrive, be sure to check in any spam folders. The activation email will come from portal@loadbalancer.org.



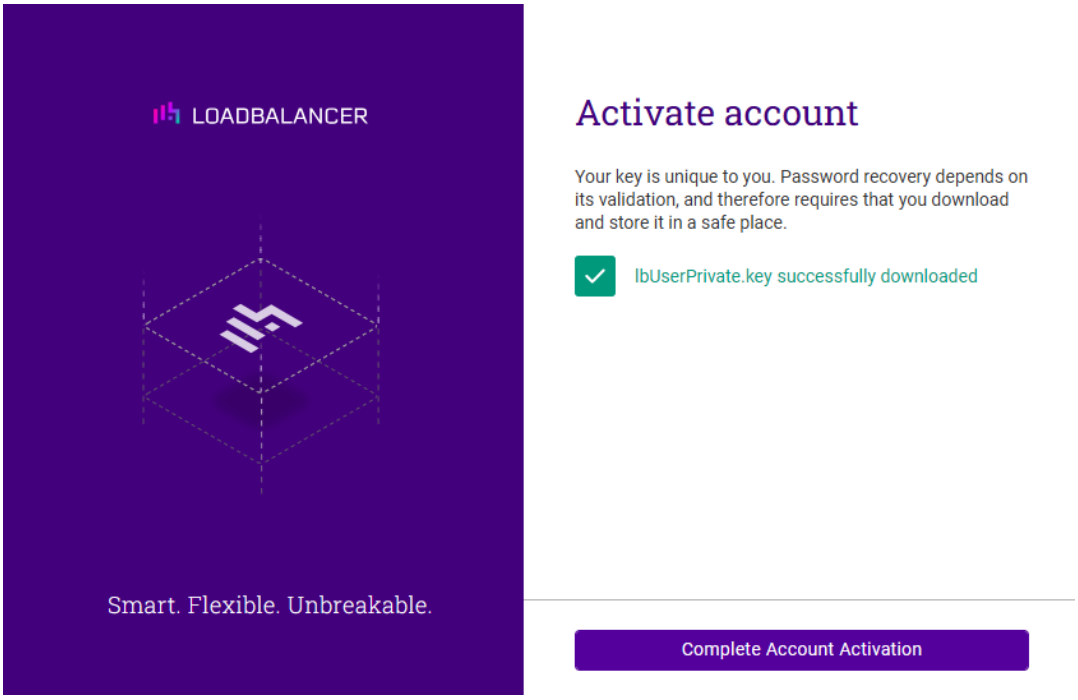
4. Provide a first and last name, set a password, and click **Next**.



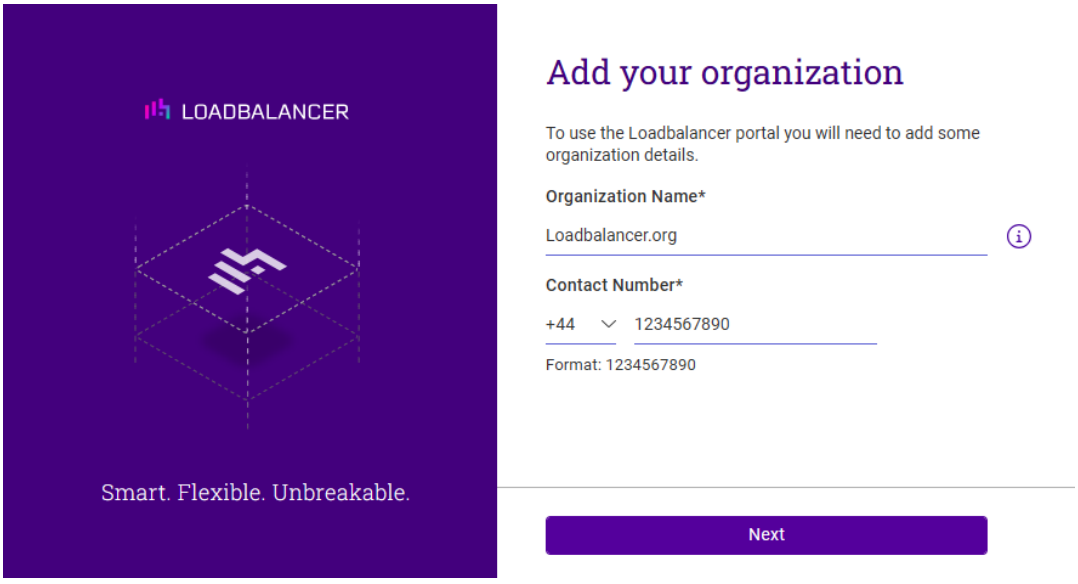
5. Download the private key for the new account by clicking on the download link. Be sure to store the key in a safe place.

> **Important** Resetting user passwords ***requires*** the user's private key. It's important to store the key file in a safe location.

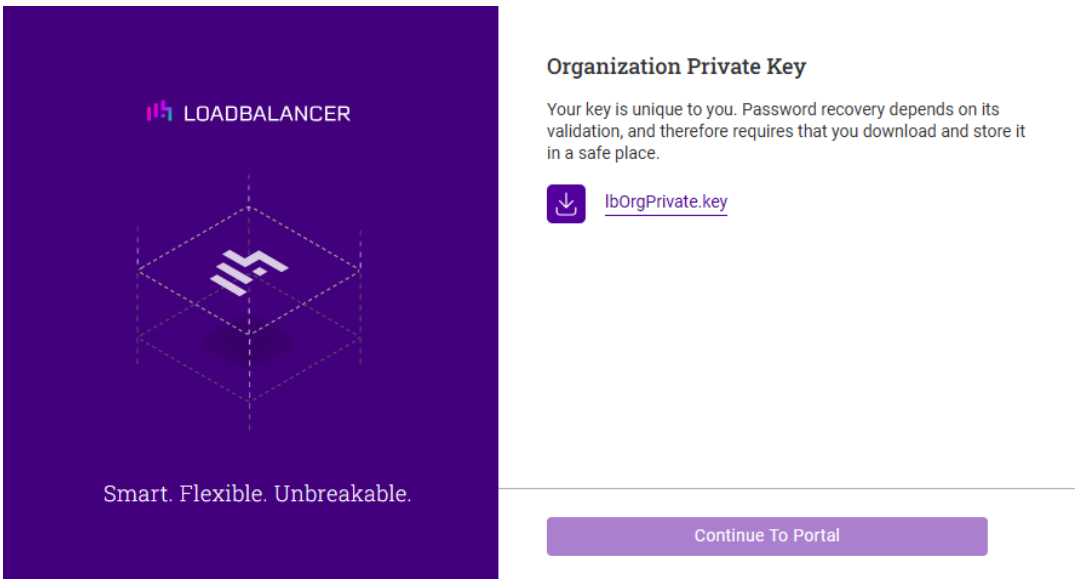
6. Once the account's private key has been downloaded, the **Complete Account Activation** button can be clicked to complete the activation process.



7. Once clicked, you'll be prompted to enter details about the organisation.



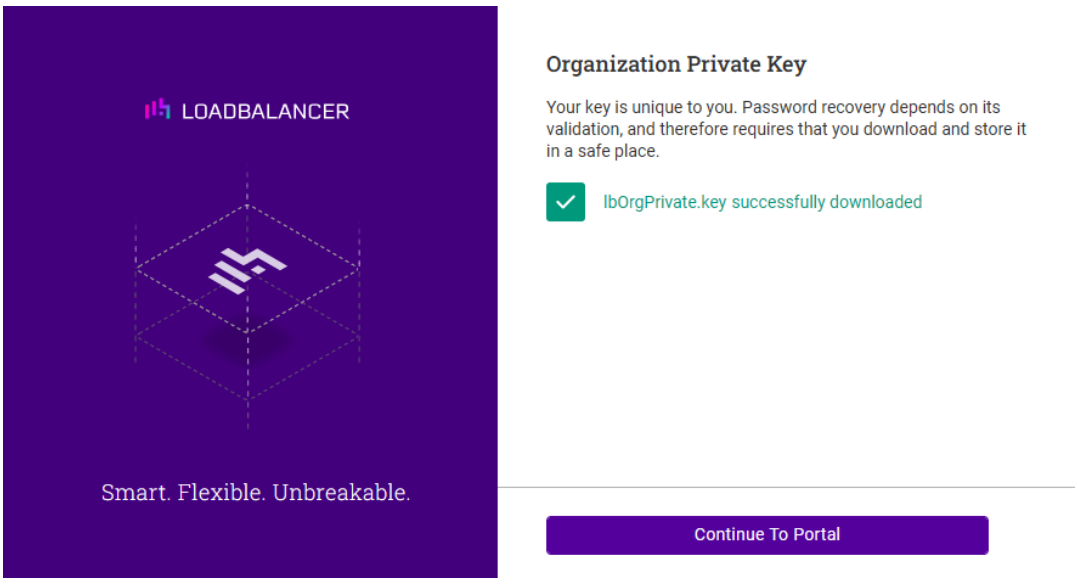
8. Enter the name and contact phone number for the organisation and click **Next**.



9. Download the private key for the new organisation by clicking on the download link. Enter the account password when prompted.

> **Important** Resetting user passwords ***requires*** the organisations's private key. It's important to store the key file in a safe location.

10. Once the organisation's private key has been downloaded, the **Continue To Portal** button can be clicked to finish the process.



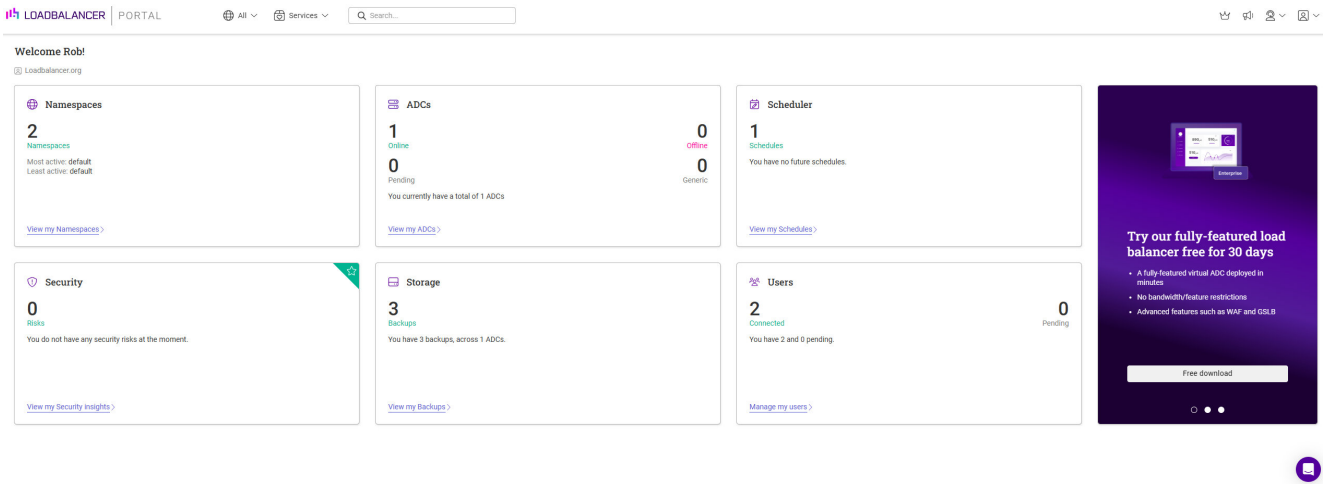
Once clicked, the ADC Portal Dashboard will be displayed.

4. ADC Portal Dashboard

The ADC Portal Dashboard provides a clear and concise overview of all ADC appliances, actions and alerts. It also enables easy navigating directly to any area that requires attention. The Dashboard has six main panels to enable quick and easy access to key areas of the Portal.

4.1. Accessing the Dashboard

The Dashboard is displayed by default after logging in to the Portal. It can also be accessed at any time by clicking on **LOADBALANCER** | PORTAL in the main menu bar at the top of the screen.

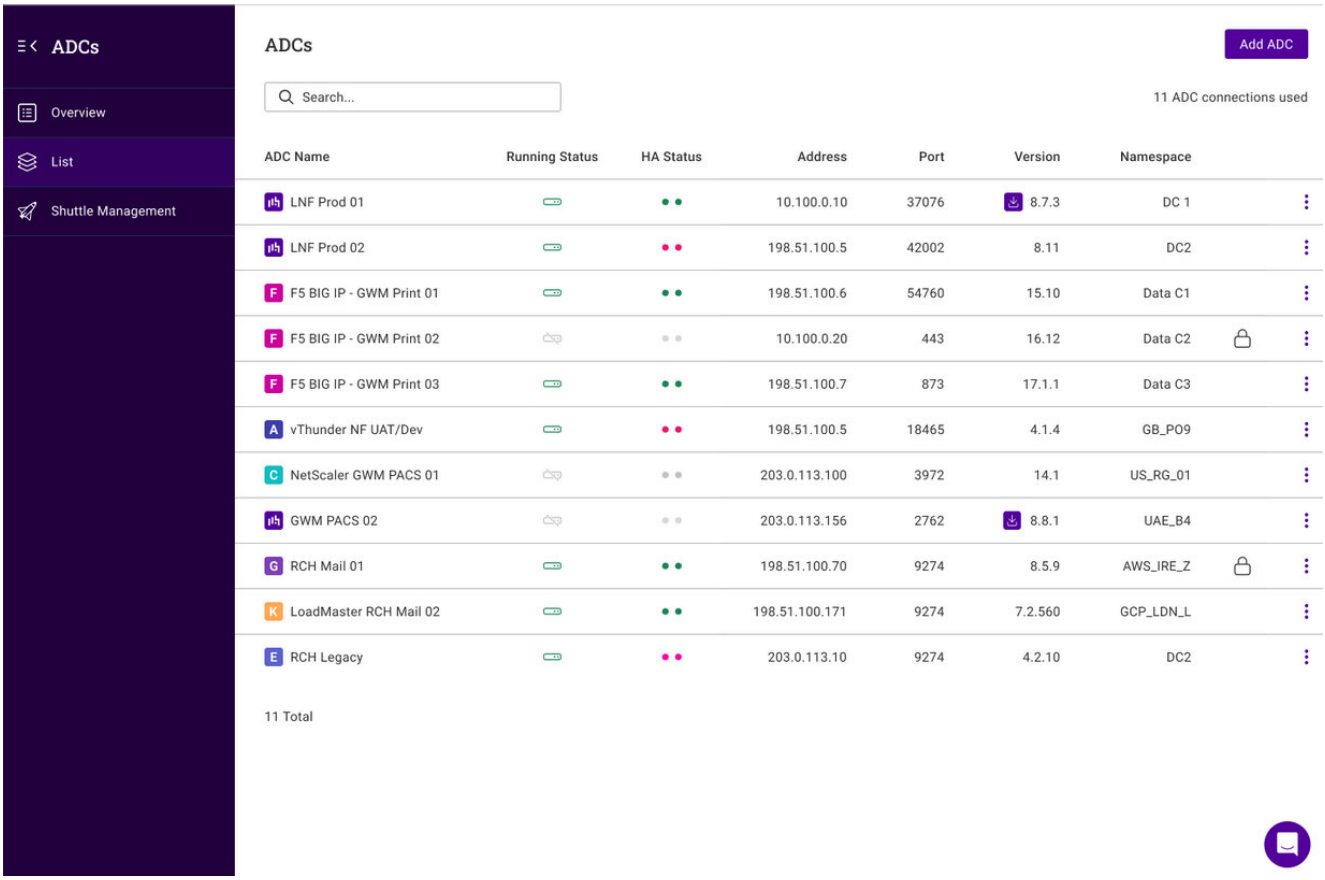


4.2. Menu Options

Symbol	Purpose
LOADBALANCER | PORTAL	Access the ADC Portal Dashboard
All	Filter by Namespace, default is all
Services	The Services menu - ADCs / Scheduler / Storage / Security
Search...	Search across all ADC Portal content
	View and change ADC Portal subscription options
	Access the latest ADC Portal news
	Create and view support tickets, view ADC Portal service status, provide feedback and access this documentation
	The Portal menu - Organisation / Account / Resources / Logout

4.3. ADC List

Once ADCs have been added to the Portal, the ADC list provides a comprehensive, easy to access overview. It shows the operational and HA status of each appliance and displays key information such as IP address, port and software version. The ADC list can be accessed from the ADCs panel in the Dashboard.



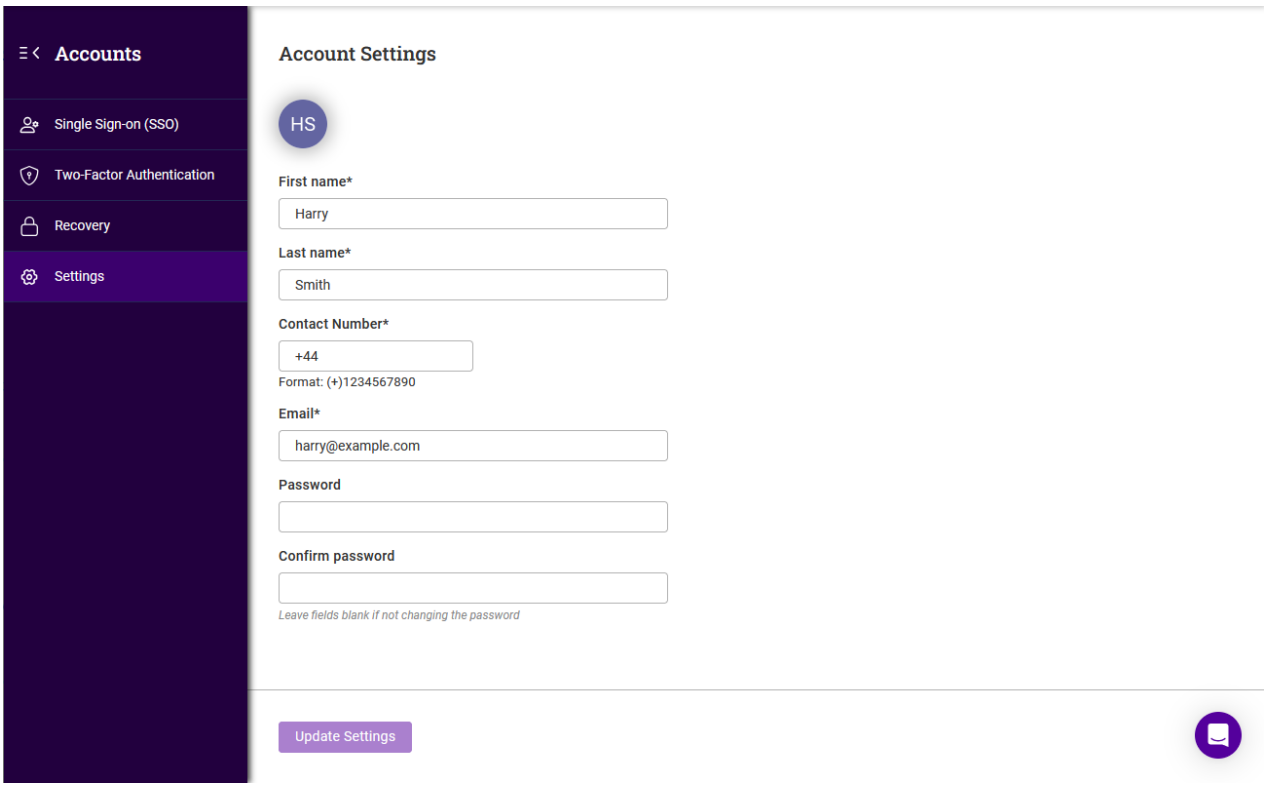
5. Account & Organisation Management

5.1. Account

5.1.1. Settings

To change the account name, contact details or password:

1. Click the ***Portal*** menu icon in the top right corner of the main menu bar and select ***Account***.
2. Using the menu to the left, select ***Settings***.



3. Update the required settings.

> **Note** To change the password you'll be prompted to enter your current password.

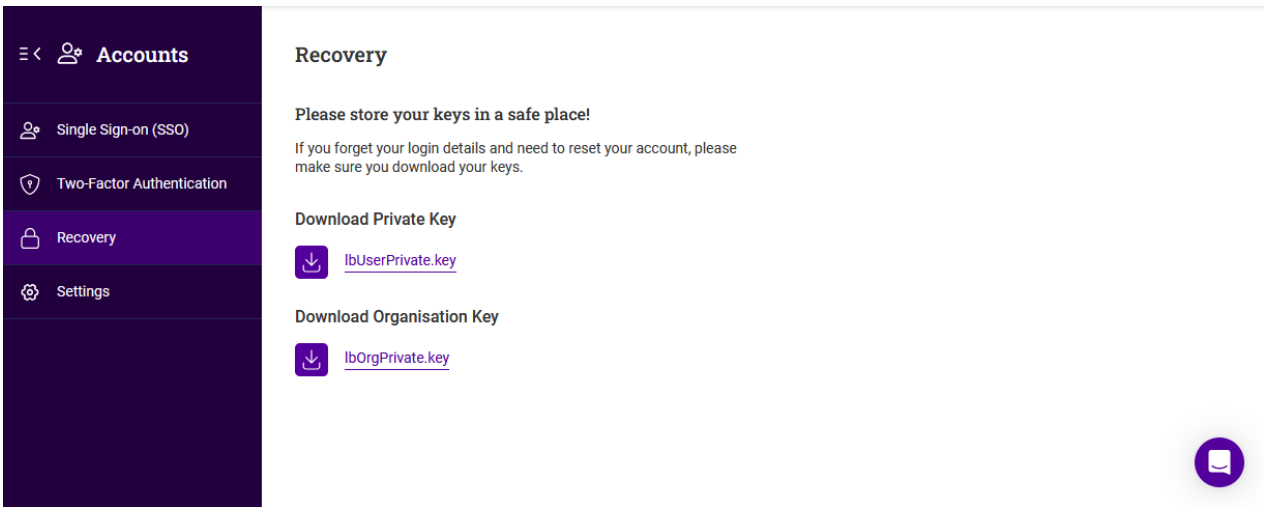
4. Click **Update Settings**.

5.1.2. Recovery

If at any point you forget your password and need to reset it, you will need your user account and organisation private keys. Both keys must be download as part of the sign-up process but can also be downloaded from the ADC Portal at any time.

To download the private keys:

1. Click the ***Portal*** menu icon in the top right corner of the main menu bar and select ***Account***.
2. Using the menu to the left, select ***Recovery***.



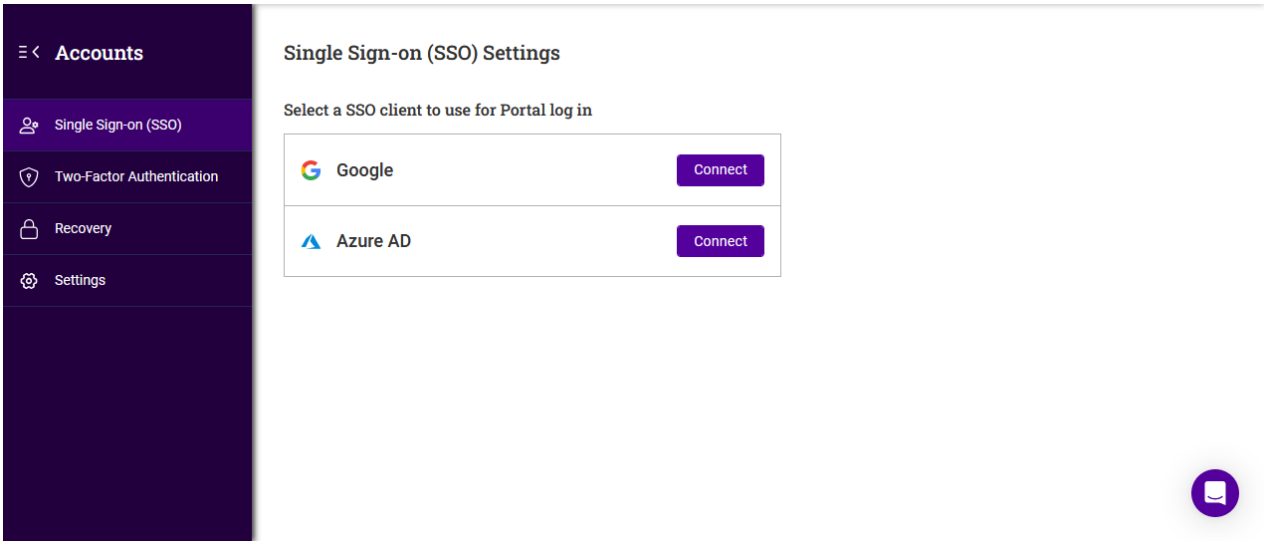
3. Click the **lbUserPrivate.key** link to download the user account private key.
4. Enter your password when prompted and click **Submit**.
5. Click the **lbOrgPrivate.key** link to download the organisation private key.
6. Enter your password when prompted and click **Submit**.
7. Save both private keys in a safe place.

5.1.3. Single Sign-On (SSO)

SSO can be enabled for each ADC Portal account. SSO simplifies Portal access by utilising login credentials from another system. SSO can be enabled using Google Workspace, Azure AD or SAML (depending on subscription level) protocols.

To configure SSO:

1. Click the *Portal* menu icon in the top right corner of the main menu bar and select *Account*.
2. Using the menu to the left, select *Single Sign-on (SSO)*.



3. Select the relevant **Connect** button and enter the credentials for the account to be used.

4. Follow the steps to complete the process.

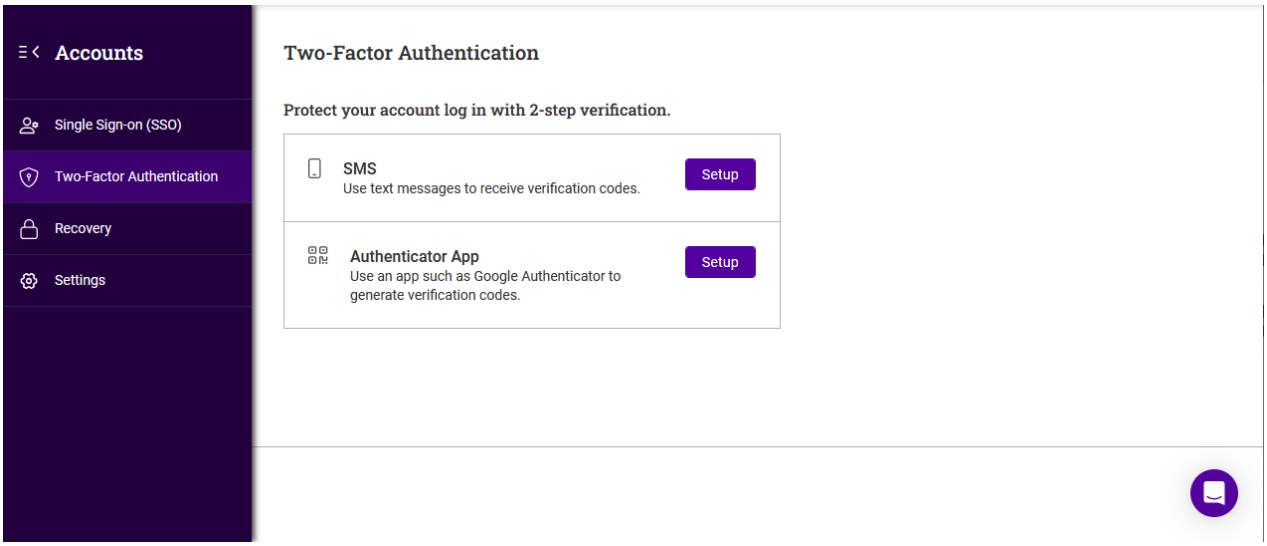
> **Note** To configure SAML for the organisation, please refer to Security Assertion Markup Language (SAML).

5.1.4. Two Factor Authentication (2FA)

2FA can be enabled for each ADC Portal account. 2FA requires a unique code in addition to the user's password. This code is supplied to the user via an SMS text message or via an authenticator app such as Google or MS Authenticator.

To configure 2FA:

1. Click the *Portal* menu icon in the top right corner of the main menu bar and select *Account*.
2. Using the menu to the left, select *Two-Factor Authentication*.



3. Select the relevant **Setup** button and follow the steps to configure 2FA.

5.2. Organisation

When the first user account is created, the organisation is also created and configured.

5.2.1. User Management

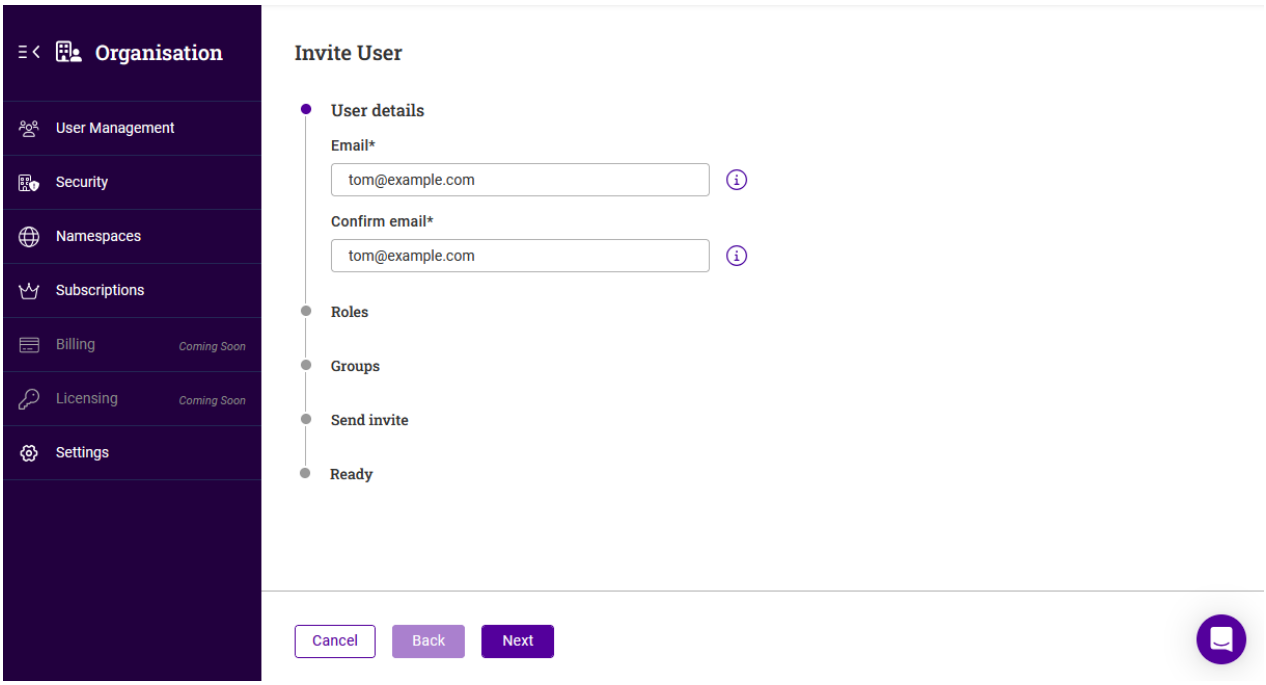
Additional user accounts can be added to the organisation. Permissions granted to each user are based on the role(s) allocated either directly to the user or via group membership and the permissions configured for those role(s).

To add a new user:

1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the Dashboard.
2. In the *Users* panel:

- If this is the first user to be added, click **Invite Users**.
- if users already exist, click **Manage my users**.
    - Click the **Add user** button.

3. The *Add User* form will be displayed:



4. Specify and confirm the *Email address* of the new user, then click **Next**.
5. Select the required *Role(s)* and click **Next**.
6. If any groups have already been configured, select the required *Group(s)* and click **Next**.

> **Note** At least one role or group must be selected.

> **Note** For more information on roles and groups, see Roles & Groups below.

7. Copy the **one-time passcode** as instructed and enable (check) the checkbox to confirm this was done.
8. Click **Next**, then click **Submit**.
9. Enter your password and click **Submit**. An email with an invitation link will be sent to the email address specified.
10. Send the **one-time passcode** to the new user to enable them to complete the enrolment process.

To delete a user:

1. Click the three dots menu next to the user to be deleted.
2. Click **Delete**, then click **Confirm** to delete the user.

> **Note** It's not possible to delete the user that created the first account and the organisation.

5.2.1.1. Roles & Groups

Roles

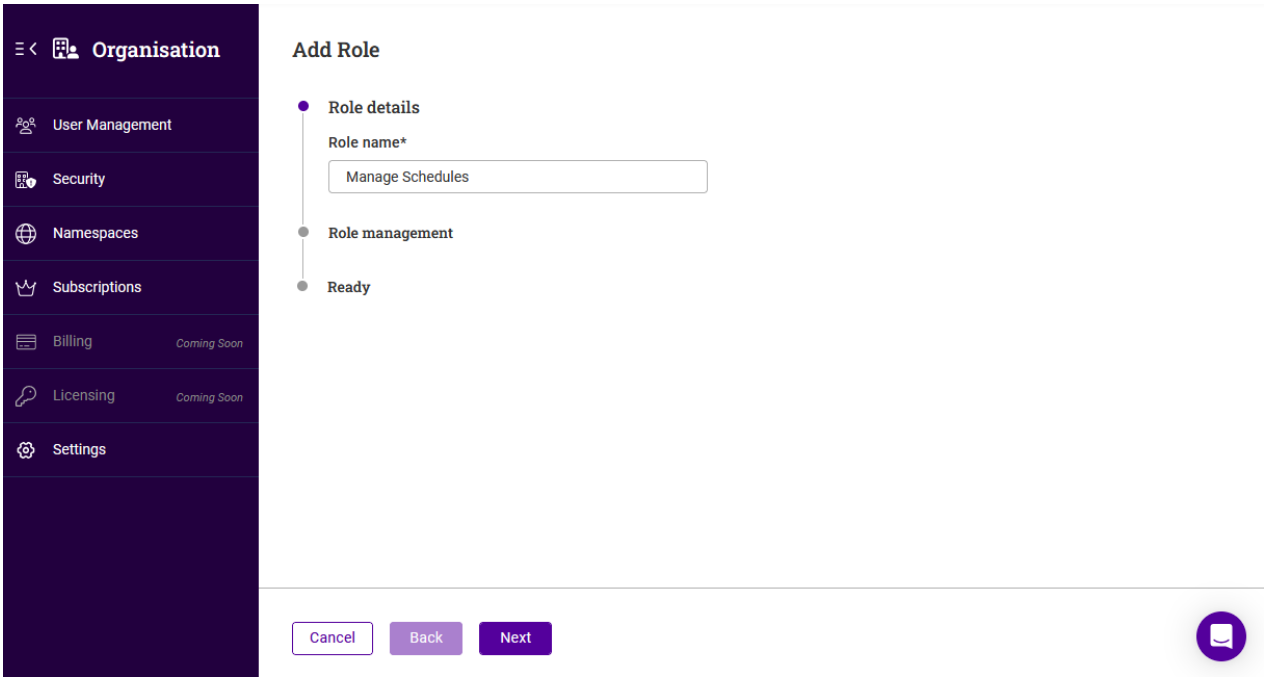
Roles define a set of permissions that can be assigned to users. Three roles are included by default:

- **Owner** - full access to all data and settings.
- **Maintainer** - full access to all data and settings except for user, group, role and account settings where read only access is provided.
- **Viewer** - read only access to all data and settings.

In addition, custom roles can be configured either from scratch or by duplicating one of the default roles and then customizing permissions to suit specific requirements.

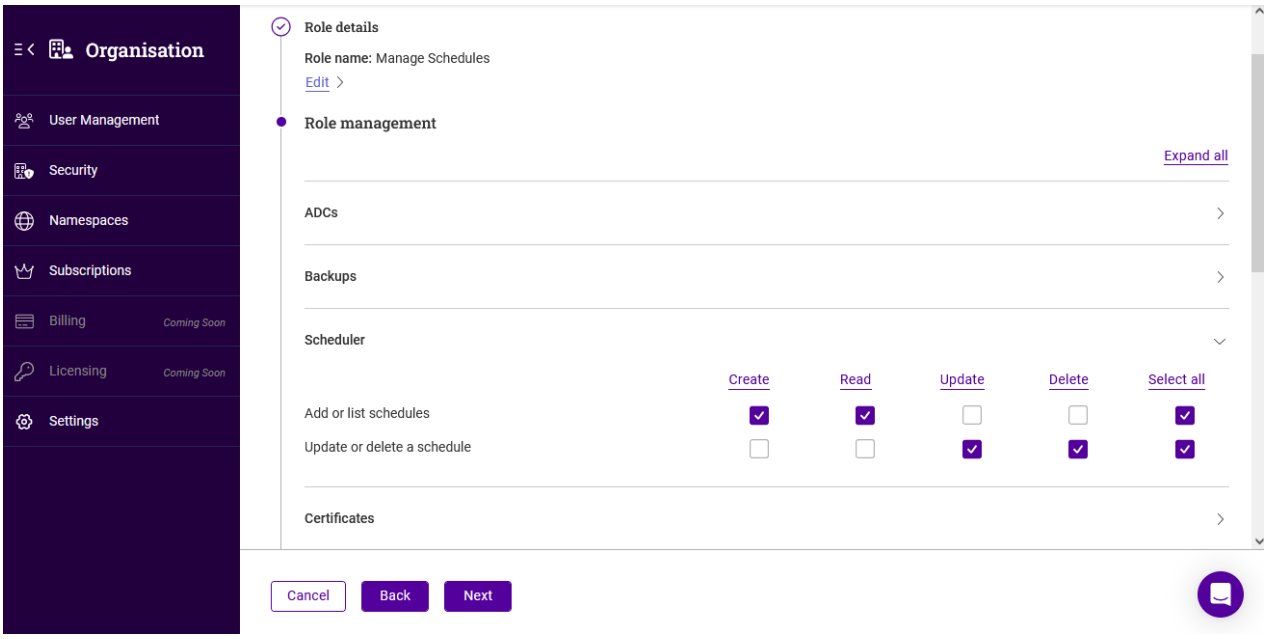
To create a new role from scratch:

1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the Dashboard.
2. In the *Users* panel:
   - If there are currently no users defined, click **Invite Users**.
   - if users already exist, click **Manage my users**.
3. Select the *Roles* tab.
4. Click the **Add Role** button.
5. The *Add Role* form will be displayed:



6. Specify an appropriate *Role name*, e.g. **Manage Schedules** and click **Next**.

7. Under the *Role Management* section either click **Expand all** or expand the relevant section(s) individually.



8. Select the required permissions. In the example above, all permissions related to schedules have been granted.
9. click **Next**, then click **Submit**.

To create a role by duplicating an existing role:

1. In the *User Management* form select the *Roles* tab.
2. Click the three dots menu next to the role to be duplicated.
3. Click **Duplicate**.
4. Specify a name for the new role and click **Next**.
5. Under the *Role Management* section either click **Expand all** or expand the relevant section(s) individually.
6. Customise the required permissions.
7. Click **Next**, then click **submit**.

To delete a role:

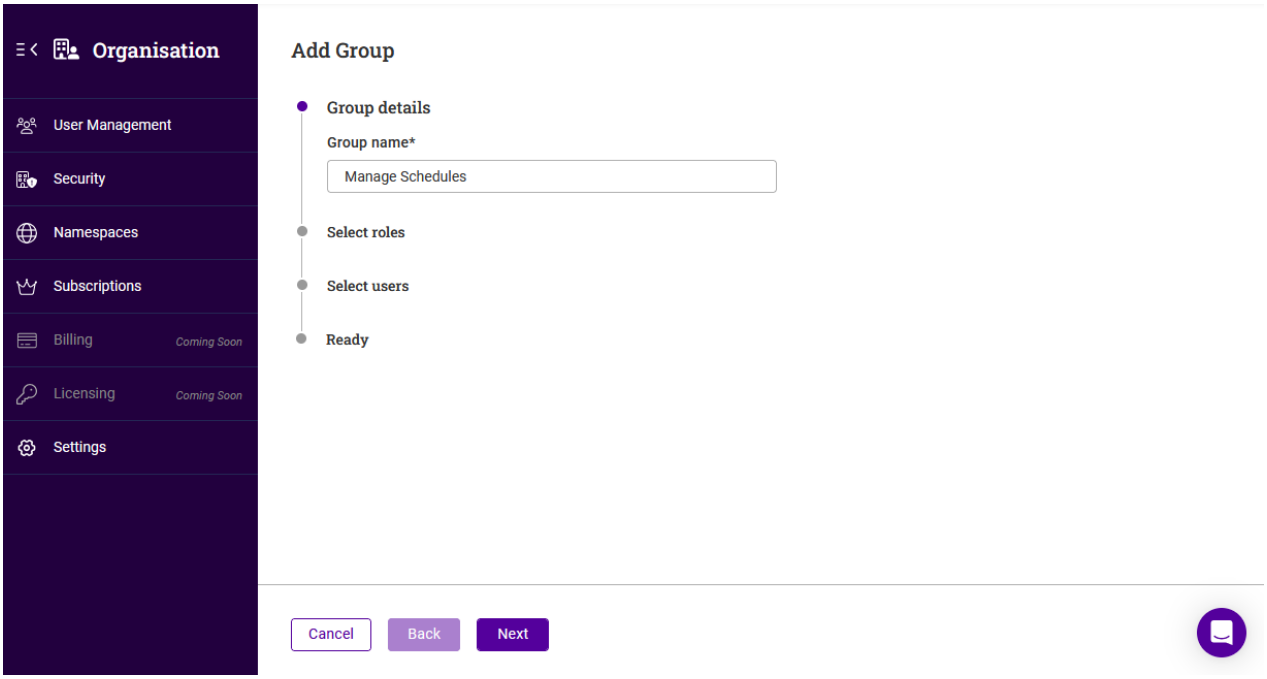
1. Click the three dots menu next to the role to be deleted.
2. Click **Delete**, then click **Confirm** to delete the role.

Groups

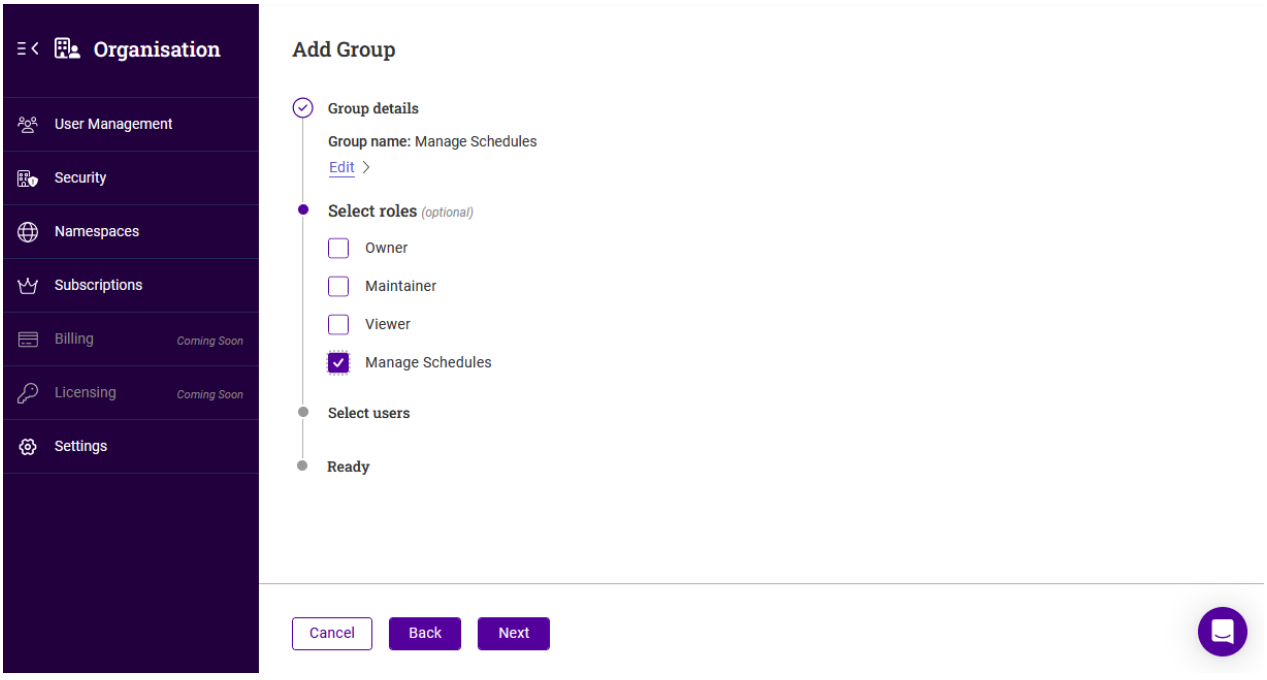
A group can have one or more associated roles and each group can contain multiple users. This enables user permissions to be assigned based on group membership.

To create a group:

1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the Dashboard.
2. In the *Users* panel:
   - If there are currently no users defined, click **Invite Users**.
   - if users already exist, click **Manage my users**.
3. Select the *Groups* tab.
4. Click the **Add Group** button.
5. The *Add Group* form will be displayed:



6. Specify an appropriate *Group name*, e.g. **Manage Schedules** and click **Next**.



7. Select the role(s) to be associated with the group (this can be done later if preferred), then click **Next**.
8. Select the user(s) that will be members of the group (this can be done later if preferred), then click **Next**.
9. Click **Submit**.

As an example, if multiple users were associated with the default Viewer role when first created, they would have read only access to all data and settings. If you wanted to allow those users to configure and manage schedules, they could be made members of the **Manage Schedules** group created above. Since the **Manage Schedules** role created above is associated with this group and provides full permissions to all scheduler related functionality, this would grant the required permissions.

To delete a group:

1. Click the three dots menu next to the group to be deleted.
2. Click **Delete**, then click **Confirm** to delete the group.

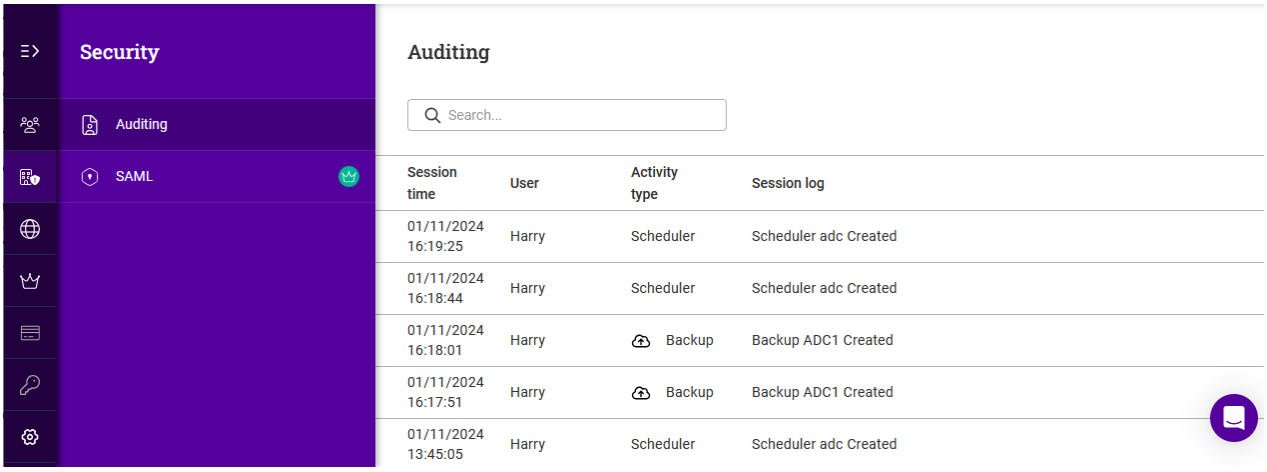
5.2.2. Security

5.2.2.1. Portal Activity Audit Log

Auditing enables Portal admin users to track events occurring on the Portal. Tracked information includes date/time, user, activity type and activity description (session log).

To view the audit log:

1. Click the *Portal* menu icon in the top right corner of the main menu bar and select *Organisation*.
2. Using the menu to the left, select *Security*.



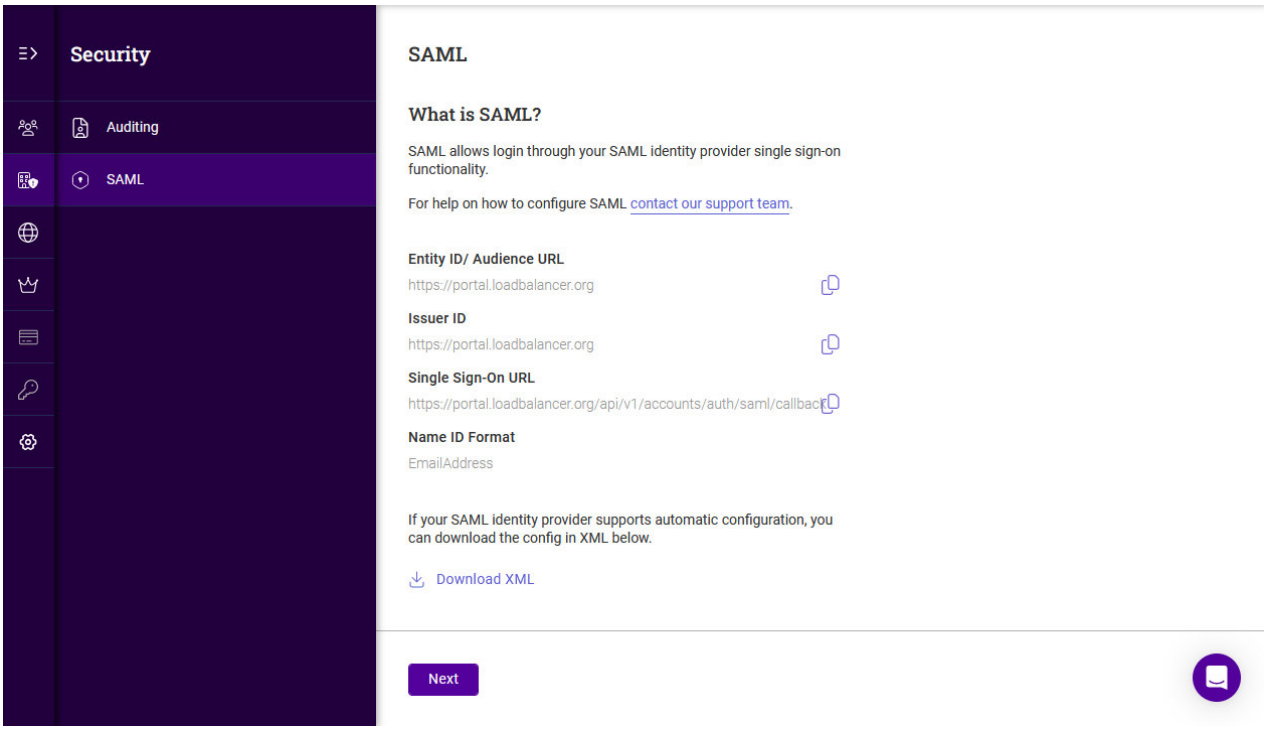
3. In the *Security* menu select *Auditing* to display the audit log.
4. To order by a particular column, click the column heading. The sort order (ascending or descending) is indicated by the arrow. Click the column heading again to change the sort order.

5.2.2.2. Security Assertion Markup Language (SAML)

SAML enables Portal login using a SAML identity provider's single sign-on functionality.

To enable SAML login for the organisation:

1. Click the *Portal* menu icon in the top right corner of the main menu bar and select *Organisation*.
2. Using the menu to the left, select *Security*.
3. In the *Security* menu select *SAML*.



*

4. Copy the data required using the links provided and paste this into the relevant fields in your chosen SAML provider's configuration screen.
5. Click **Next**.
6. Copy the Metadata URL from your SAML provider and paste this into the field provided in the ADC Portal.
7. Click **Submit**.

> **Note** If you need any assistance configuring SAML, please contact our support team.

5.2.3. Namespaces & Tags

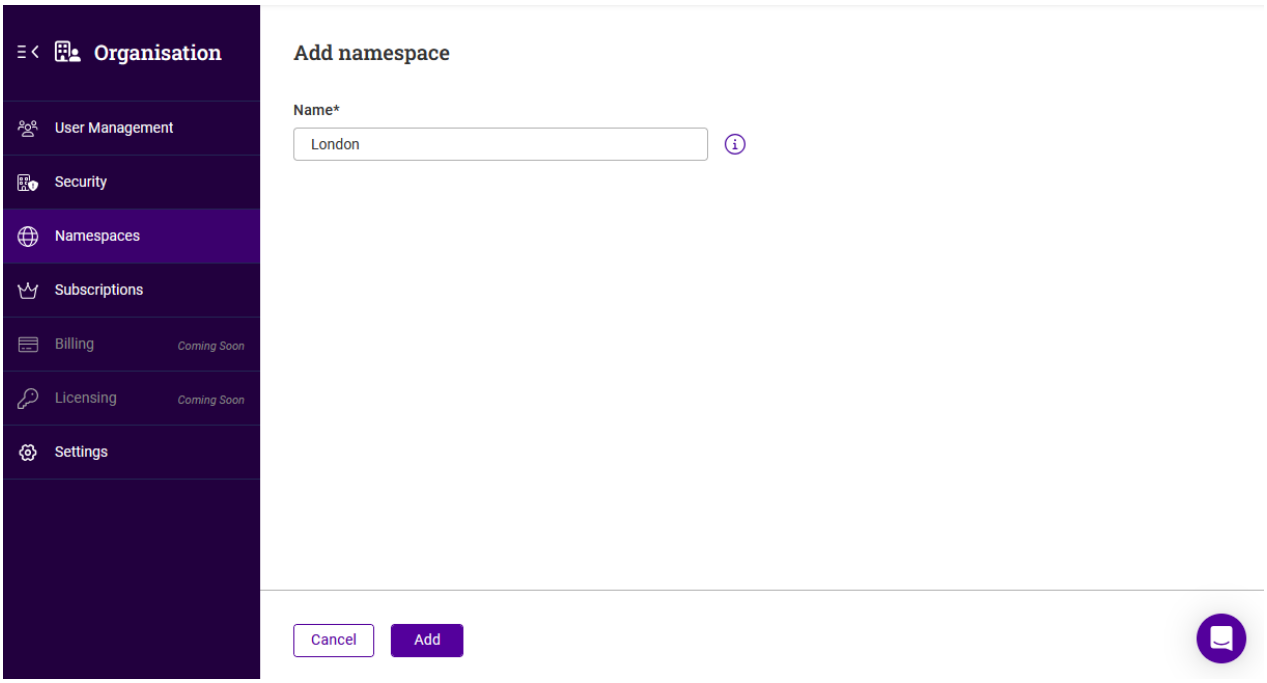
Namespaces allow ADCs to be organised into user-defined groups to simplify management. Each ADC can reside in one Namespace at a time, ensuring a clean and efficient structure. In addition, up to 30 user-defined tags can be added to each ADC to help organize your infrastructure more effectively. Namespaces can be added as detailed below, Tags are specified and created when ADCs are added to the Portal.

For example, Namespaces could be used to indicate where ADCs are located and Tags could be used to indicate which support team is responsible for the ADC. All ADCs in a particular location could then be viewed by selecting the relevant Namespace using the Namespaces dropdown and all ADCs supported by a particular team could be found by specifying the relevant Tag in the ADC search box.

Namespaces and Tags are allocated when ADCs are added to the Portal. They can also be modified later if required by editing the ADC - for more information, see ADC Actions Menu.

To add a new namespace:

1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the Dashboard.
2. In the *Namespaces* panel, click **View my Namespaces**.
3. Click the **Add namespace** button.
4. The *Add Namespace* form will be displayed:



5. Specify a *Name* for the new namespace and click **Add**.

To delete a namespace:

1. Click the three dots menu next to the namespace to be deleted.
2. Click **Delete**, then click **Confirm** to delete the namespace.

5.2.4. Subscriptions

To view the organisation's current ADC Portal subscription:

1. Click the *Subscriptions* menu icon in the top right side of the main menu bar.

All features that are included are listed under each subscription level.

If you want to change your subscription, click the relevant **Contact Sales** button to open a chat window and discuss your requirements. Alternatively, email sales@loadbalancer.org.

5.2.5. Billing

This functionality is coming soon.

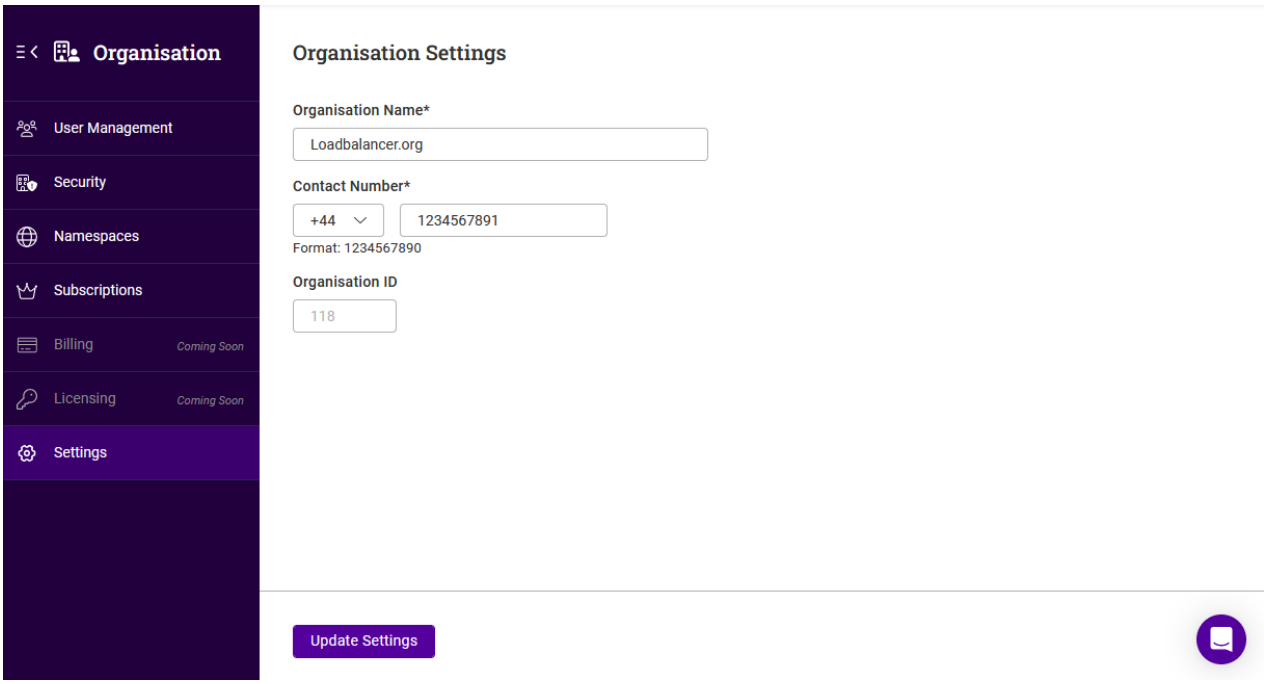
5.2.6. Licensing

This functionality is coming soon.

5.2.7. Settings

To update the organisation's name or telephone number:

1. Click the *Portal* menu icon in the top right corner of the main menu bar and select *Organisation*.
2. Using the menu to the left, select *Settings*.



3. Update the *Organisation Name* and *Contact Number* as required.
4. Click **Update Settings**.

6. Shuttle Management

As mentioned in Technology, a Shuttle is required to enable ADCs to communicate with the ADC Portal.

6.1. Adding a Shuttle

6.1.1. Standalone Shuttle

A standalone Shuttle is a dedicated Linux instance that runs the Shuttle service. The instance requires **wget** and **curl** to be installed to allow the required installation files to be downloaded.

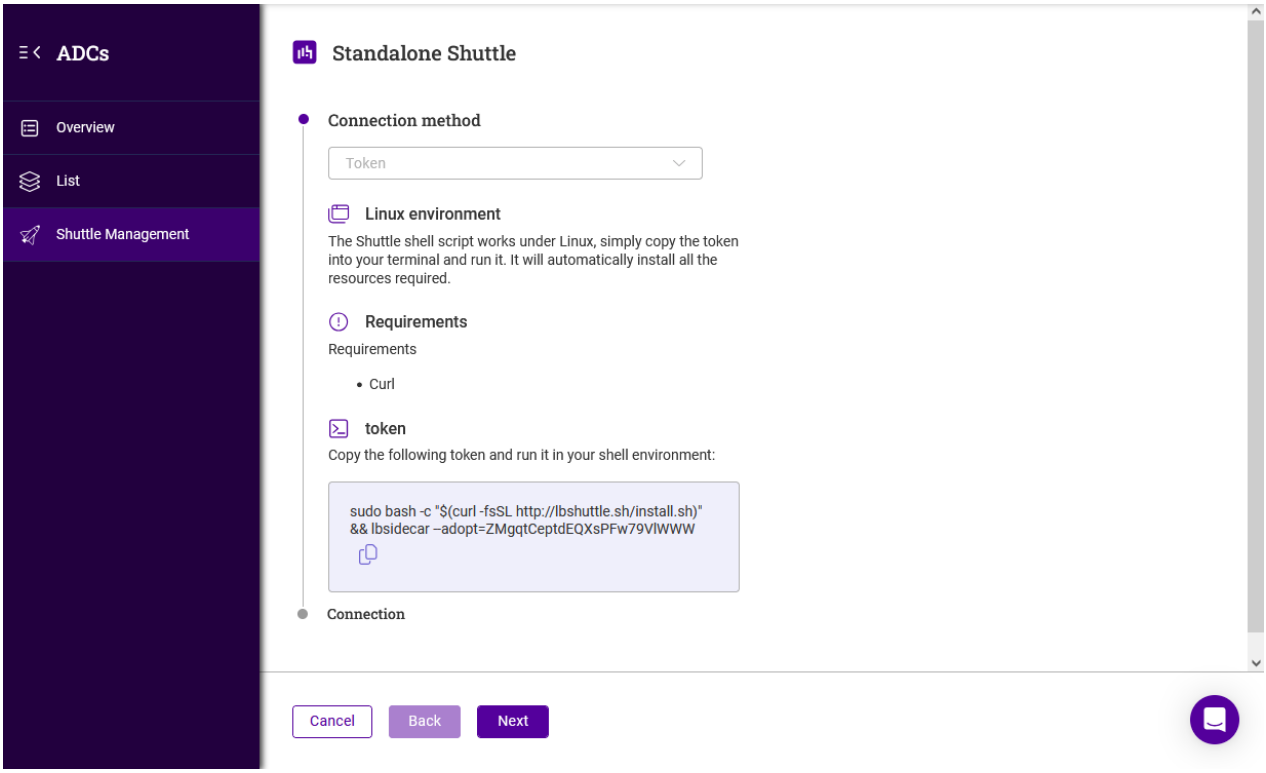
Step 1 - Prepare the Linux instance

1. Deploy a new Linux instance that will be used as the standalone Shuttle.

2. Ensure that **wget** and **curl** are installed.

Step 2 - Configure the Shuttle

1. Click **LOADBALANCER** | PORTAL in the Portal's main menu bar to view the dashboard.
2. In the *ADCs* panel:
   - If there are currently no ADCs, click **Connect an ADC**.
     - Using the menu to the left, select *Shuttle Management*.
   - If ADCs have already been added, click **View my ADCs**.
     - Using the menu to the left, select *Shuttle Management*.
     - Click the **Add Shuttle** button.
3. Click the **Add** button for the **Standalone Shuttle**.



4. Copy the installation command/token as directed using the copy link provided.
5. The Standalone Shuttle form will now display **Waiting for adoption…**
6. Run the copied command/token on the Linux instance via the console or an SSH session.
7. When the command completes successfully, the following message will be displayed:

```
> Installation complete

Successfully initiated adoption process. Please visit the Portal to complete the adoption
process.
```

Step 3 - Adopt the Shuttle

1. In the Shuttle Management form, click the **Adopt** button for the new Shuttle to complete the Shuttle adoption process.
2. Once adopted, the Shuttle name and other attributes can be changed if required. For more information, please refer to Shuttle Actions Menu.

> **Note** To continue and add an ADC to the Portal, please refer to ADC Management.

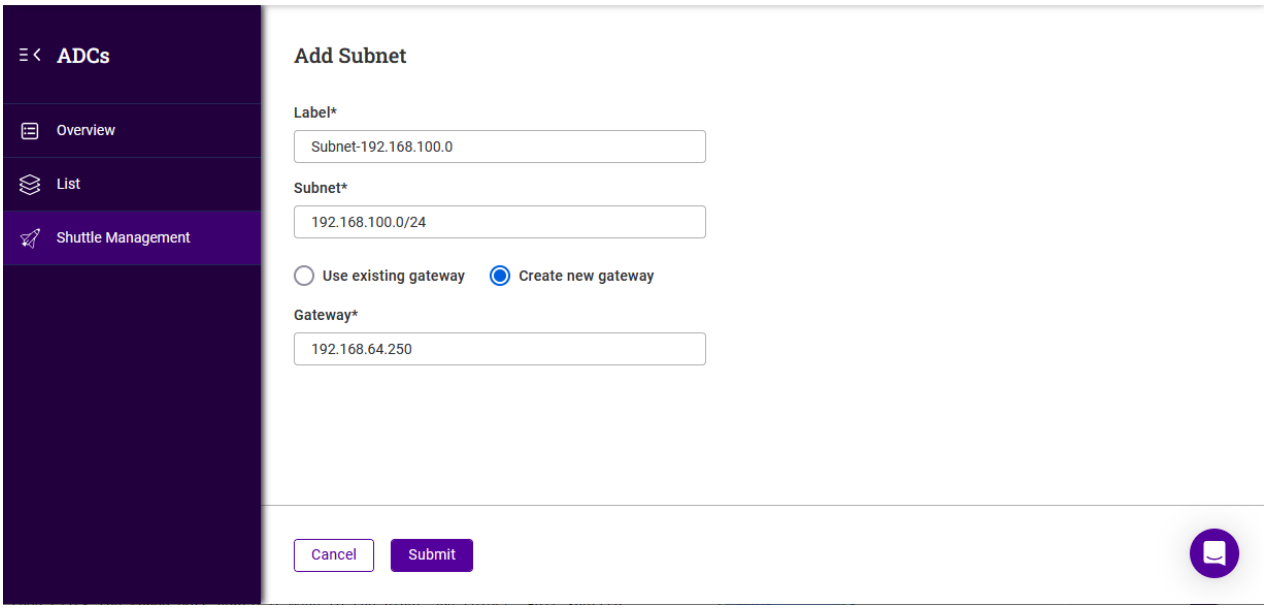
6.1.1.1. Network Topology

As mentioned in Connection Options, if the Shuttle does not have network access to all ADCs, a subnet for each remote ADC must be defined. This configures a static route on the Shuttle to enable access to the remote subnet.

> **Note** You'll also need to ensure that routing for the remote subnet(s) allows traffic to return to the Shuttle.

To add a new subnet:

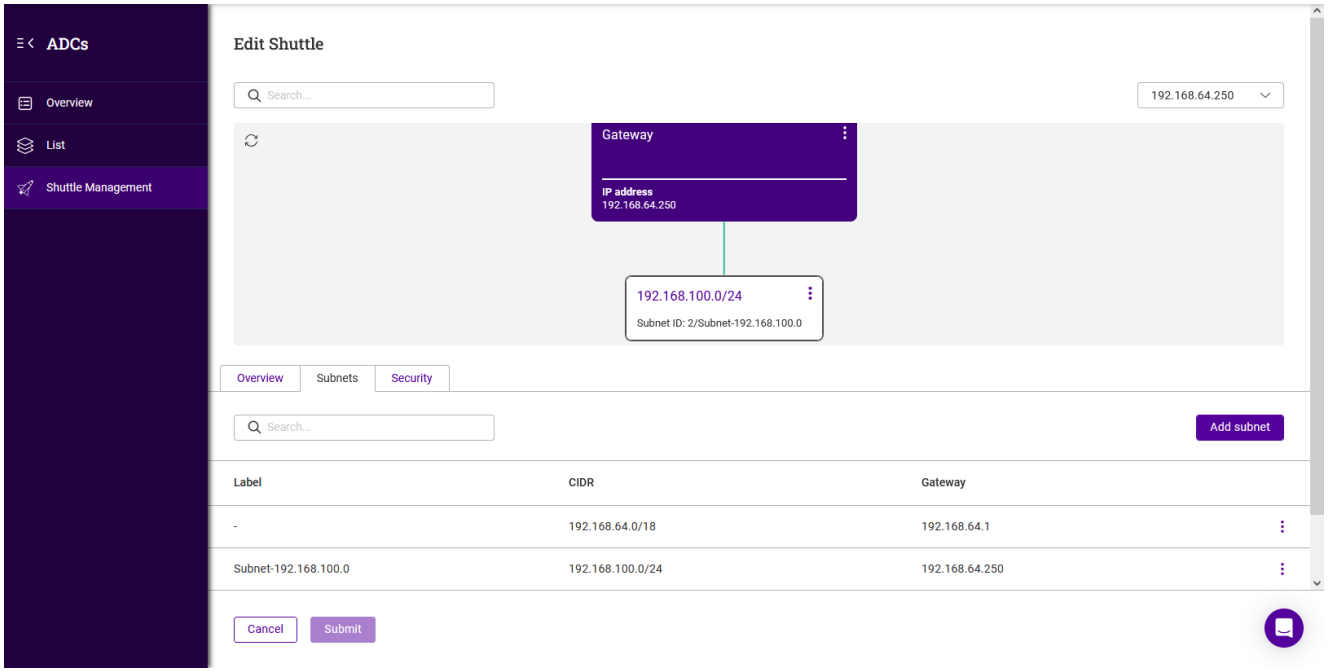
1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the dashboard.
2. In the *ADCs* panel, click **View my ADCs**.
3. Using the menu to the left, select *Shuttle Management*.
4. Click the three dots menu to the right of the relevant standalone shuttle and select *Edit Shuttle*.
5. Ensure that the *Subnets* tab is selected, then click the **Add Subnet** button.



6. Specify a suitable label (name) for the subnet, e.g. **Subnet-192.168.100.0**.
7. Enter the subnet address, e.g. **192.168.100.0/24**.
8. To create a new gateway, select *Create new Gateway* and specify the *Gateway* IP address.

9. Click **Submit**.

Once created, a graphical representation of the subnet and associated gateway will be displayed:



Repeat these steps to add additional subnets as required.

To delete a subnet:

1. Click the three dots menu next to the subnet to be deleted.
2. Click **Delete**, then click **Confirm** to delete the subnet.

6.1.2. Loadbalancer Enterprise

A Loadbalancer.org Enterprise ADC with the Shuttle service enabled can also be used as a Shuttle.

> **Note** For more details, please refer to Connection Options.

Step 1 - Prepare the Enterprise Appliance

1. If required, deploy a new Loadbalancer.org Enterprise Appliance that will be used as the Shuttle.
2. Using the Enterprise appliance's WebUI, navigate to ***Local Configuration > Portal Management***.
3. Enable (check) the ***Shuttle Enabled*** checkbox.

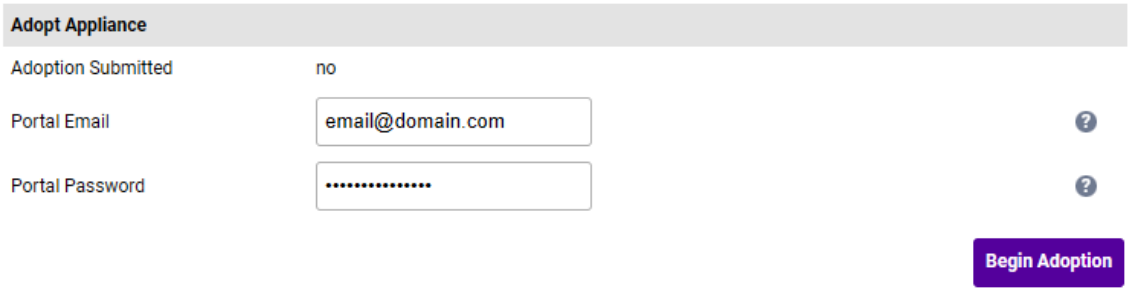
> **Note** If this appliance will also handle load balancing workload and you wish to monitor the appliance via the Portal, you should also enable (check) the ***Gateway Enabled*** checkbox to allow it to be added to the ADC Portal.

4. Click **Update**.

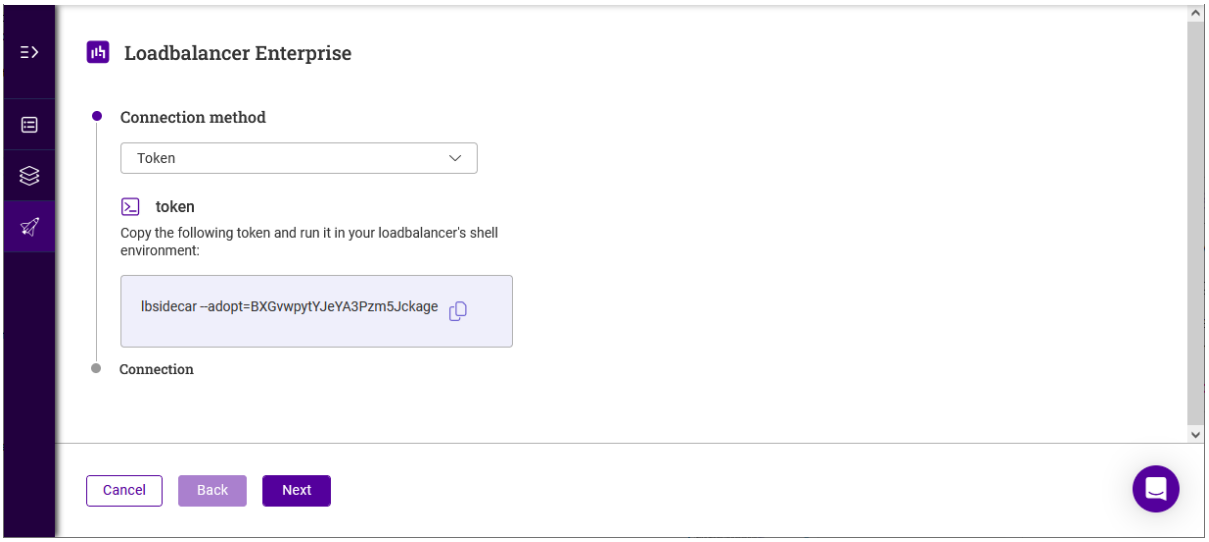
5. Restart the Gateway and Shuttle services using the buttons in the "Commit changes" box at the top of the screen.
6. Using the Enterprise appliance's WebUI, navigate to *Local Configuration > Security*.
7. Set the *Appliance Security Mode* to **Custom** and click **Update**. This will enable shell commands via the WebUI.

Step 2 - Configure the Shuttle

1. Click **LOADBALANCER** | PORTAL in the Portal's main menu bar to view the Dashboard.
2. In the *ADCs* panel:
   - If there are currently no ADCs, click **Connect an ADC**.
     - Using the menu to the left, select *Shuttle Management*.
   - If ADCs have already been added, click **View my ADCs**.
     - Using the menu to the left, select *Shuttle Management*.
     - Click the **Add Shuttle** button.
3. Click the **Add** button for the **Loadbalancer Enterprise**.
4. Select the required *Connection Method*.
   - If **Credentials** is selected:
     - Click **Next**.
     - The Loadbalancer Enterprise Portal form will now display **Waiting for adoption...**.
     - Using the Enterprise appliance's WebUI, navigate to *Local Configuration > Portal Management*.



     - Enter the *Portal Email* and *Portal Password* for the Portal account.
     - Click **Begin Adoption**.
     - "Adoption Initiated" will be displayed in the blue information box.
   - If **Token** is selected:



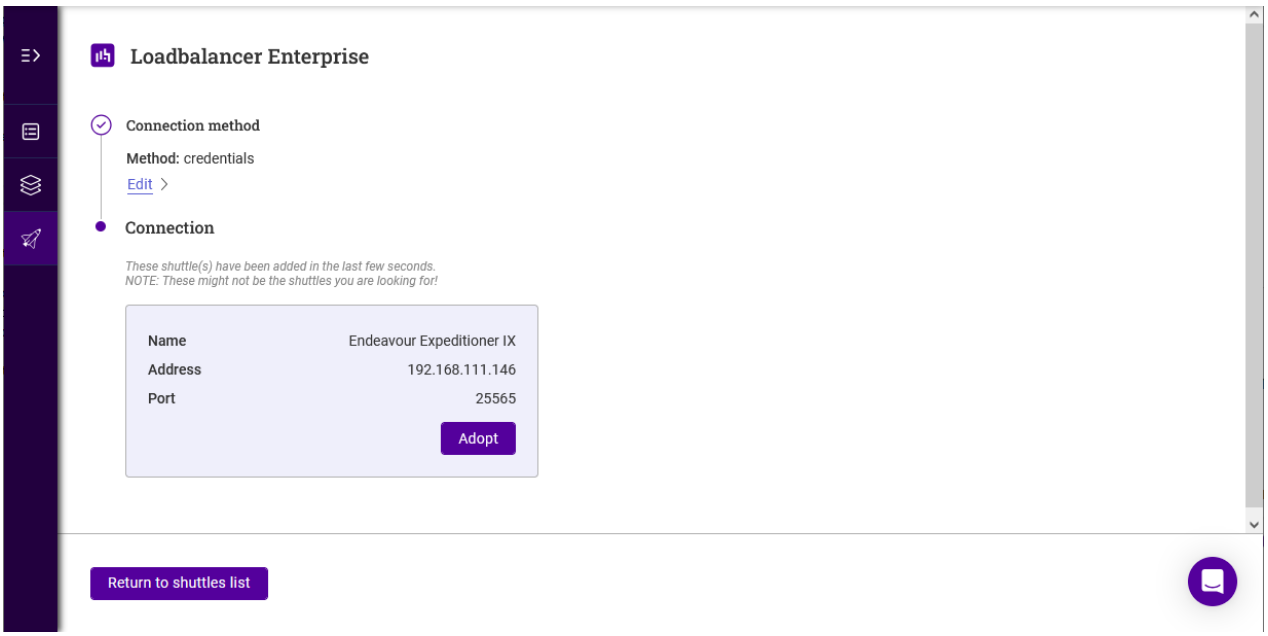
- Copy the installation command/token as directed using the copy link provided.
- The Loadbalancer Enterprise Shuttle form will now display **Waiting for adoption…**.
- Using the Enterprise appliance's WebUI, navigate to *Local Configuration > Execute Shell Command*.
- Paste the installation command/token into the execute shell command field as shown below.

- Click **Execute shell command**.
- Once the command has executed successfully, the following message will be displayed on the appliance WebUI:

```
Successfully initiated adoption process. Please visit the Portal to complete the
adoption process.
```

Step 3 - Adopt the Shuttle

1. Return to the ADC Portal.



> **Note** Multiple Shuttles may be displayed if others have been configured but not yet adopted.

2. Click the **Adopt** button for the Shuttle. The Shuttle will be displayed in the ***Shuttle Management*** list.
3. Once adopted, the Shuttle name and other attributes can be changed if required. For more information, please refer to Shuttle Actions Menu.

> **Note** To continue and add an ADC to the Portal, please refer to ADC Management.

6.1.3. Loadbalancer Endurance

The ability to use a Loadbalancer.org Endurance appliance as a Shuttle is coming soon.

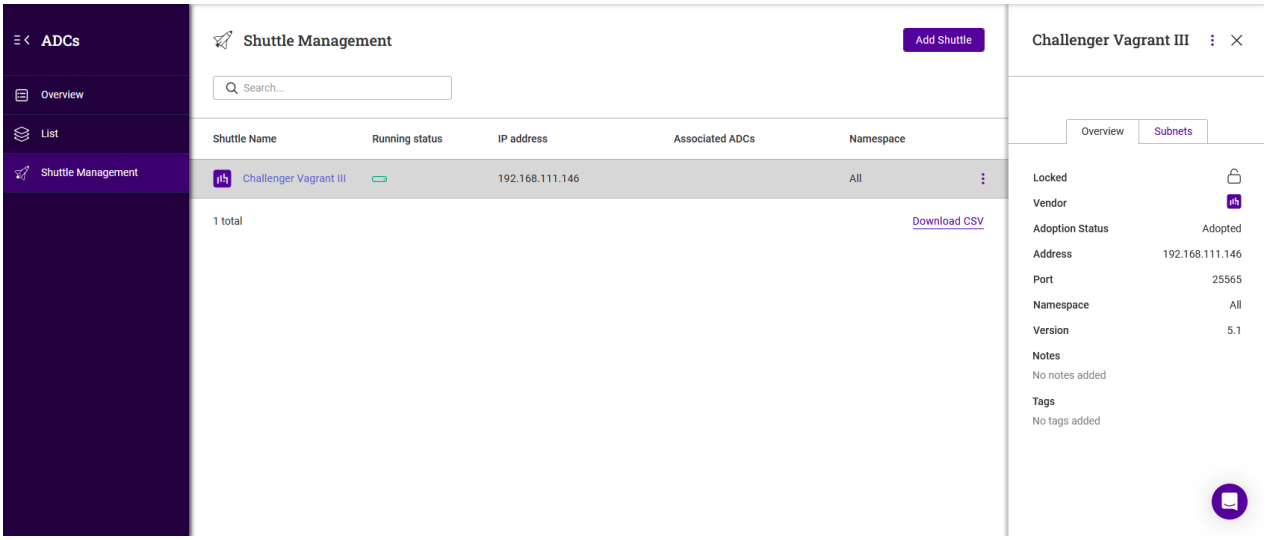
6.2. Viewing & Managing Shuttles

To view all shuttles:

1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the Dashboard.
2. In the ***ADCs*** panel, click **View my ADCs**.
3. Using the menu to the left, select ***Shuttle Management***.
4. All existing Shuttles will be listed.

To view/manage a particular shuttle:

1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the Dashboard.
2. In the ***ADCs*** panel, click **View my ADCs**.
3. Using the menu to the left, select ***Shuttle Management***.
4. Click the Label (name) of the Shuttle to be viewed, a new information panel will be displayed to the right.

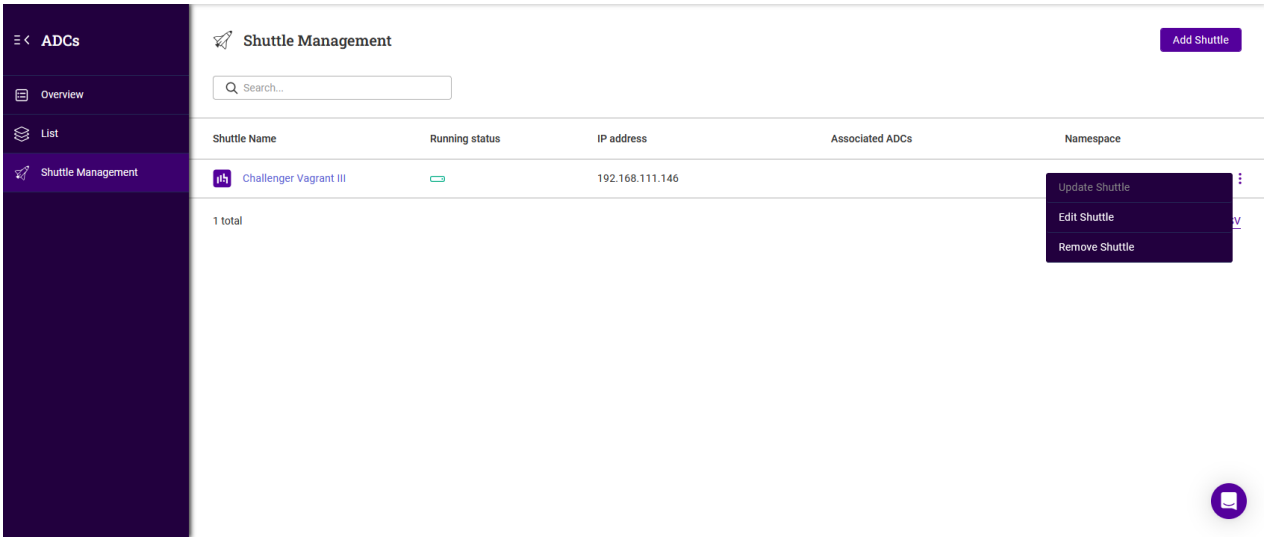


- The *Overview* tab provides a summary of the Shuttle.
- The *Subnets* tab lists the subnets that the Shuttle is associated with.

> **Note** For more information on subnets, please refer to Standalone Shuttle.

6.2.1. Shuttle Actions Menu

1. Click the three dots menu for the Shuttle, the actions menu will be displayed.



2. Select the required action:

   - **Update Shuttle**
     - Update the Shuttle service to the latest version.

     > **Note** This option will be greyed out if there are no updates available.

   - **Edit Shuttle**

- The *Edit Shuttle* screen will be displayed. Update the settings as required and click **Submit** to save.

- **Remove Shuttle**
  - Remove the Shuttle from the Portal. You'll be prompted to confirm that you want to proceed, click **Confirm** to delete the Shuttle.

> **Note** This option will be greyed out if any ADCs are using the Shuttle to communicate with the ADC Portal.

7. ADC Management

7.1. Multi Vendor Support

ADCs from multiple vendors can be adopted (added to the ADC Portal). The table below lists which ADCs are currently supported.

Vendor	Software Versions Supported	Notes
Loadbalancer.org	v8.11.4 & later	
F5	v17.0.0.1 & later	Previous versions may be supported but have not been verified
Kemp	v7.2.55.0.21071 & later	Previous versions may be supported but have not been verified
Citrix	v13.1-48.47 & later	Previous versions may be supported but have not been verified

7.2. Adding an ADC to the Portal

> **Important** There must already be an accessible Shuttle available before an ADC can be added. To add a Shuttle, please refer to Shuttle Management.

Step 1 - Prepare the ADC for Adoption

Loadbalancer.org ADC Appliances:

1. Using the WebUI, navigate to *Local Configuration > Portal Management*.
2. Ensure that the *Gateway Enabled* checkbox is enabled (checked).
3. Click **Update**.
4. Restart the Gateway and Shuttle services using the restart buttons in the "Commit changes" box at the top of the screen.

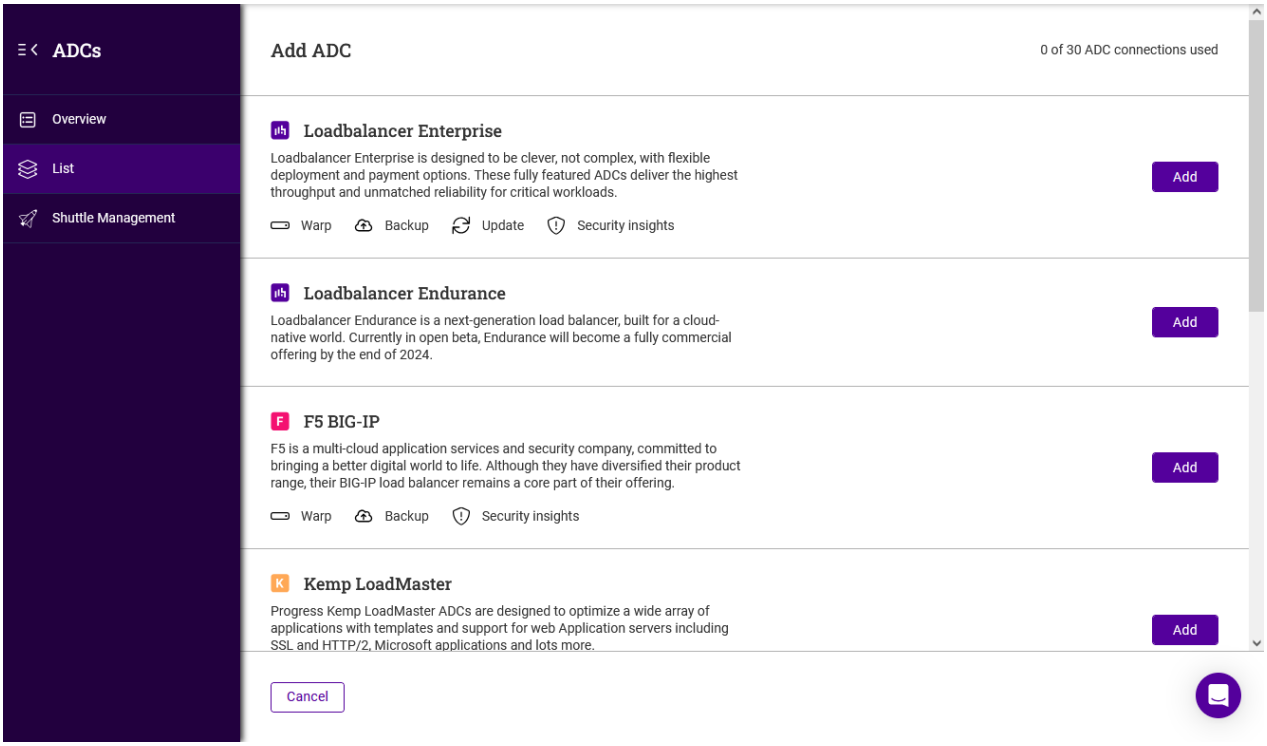
All other ADC Appliances:

1. Follow the manufacturers instructions to add a user account that has permissions to make API calls.

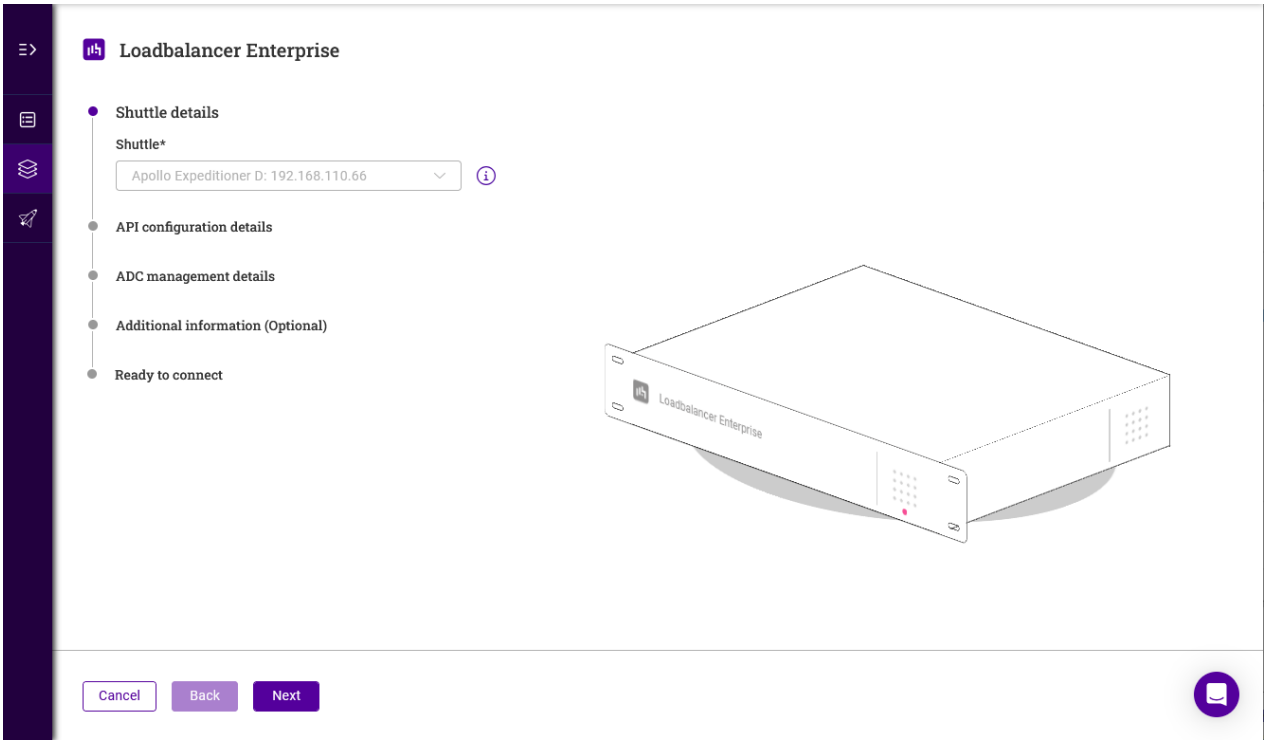
2. Note the user credentials as these will be needed when adopting the appliance in the ADC Portal.

Step 2 - Adopt the ADC

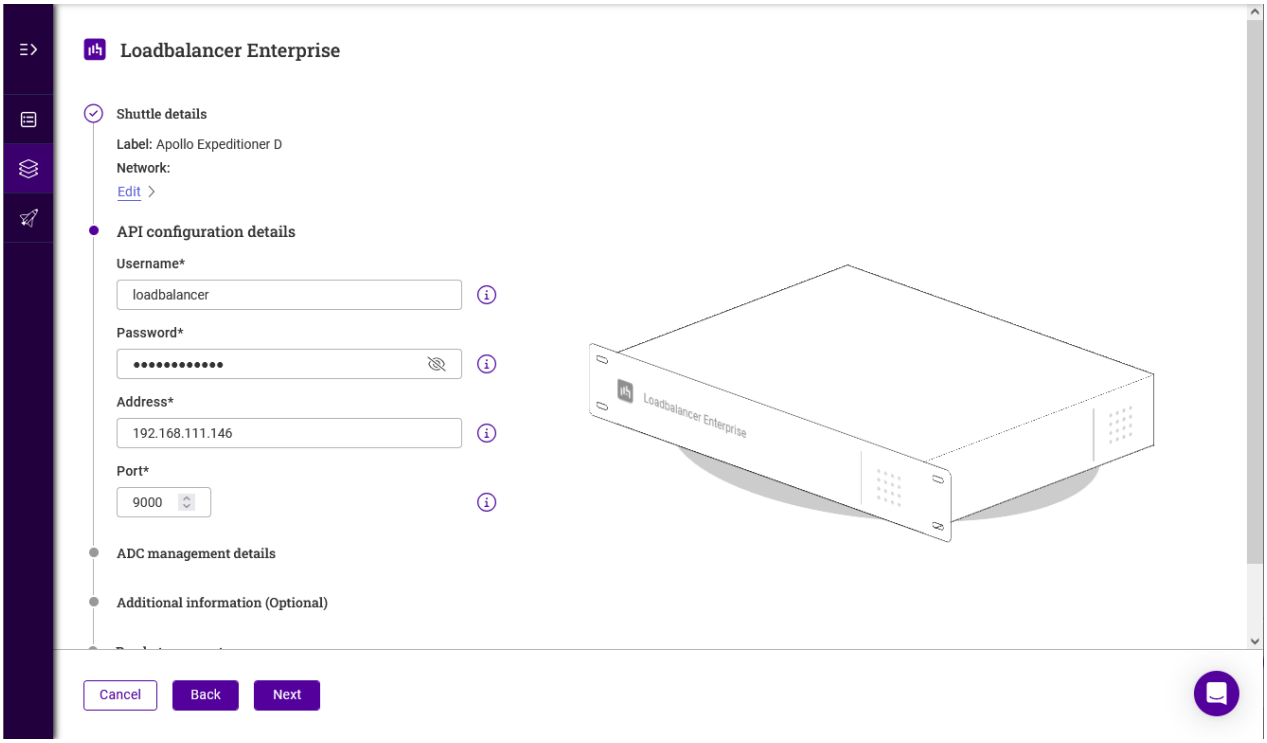
1. Click **LOADBALANCER** | PORTAL in the Portal's main menu bar to view the Dashboard.
2. In the *ADCs* panel:
   - If there are currently no ADCs, click **Connect an ADC**.
     - In the menu to the left, select *List*.
   - if ADCs have already been added, click **View my ADCs**.
3. Click the **Add ADC** button.



4. Click the **Add** button for the type of ADC to be added, for example **Loadbalancer Enterprise**.

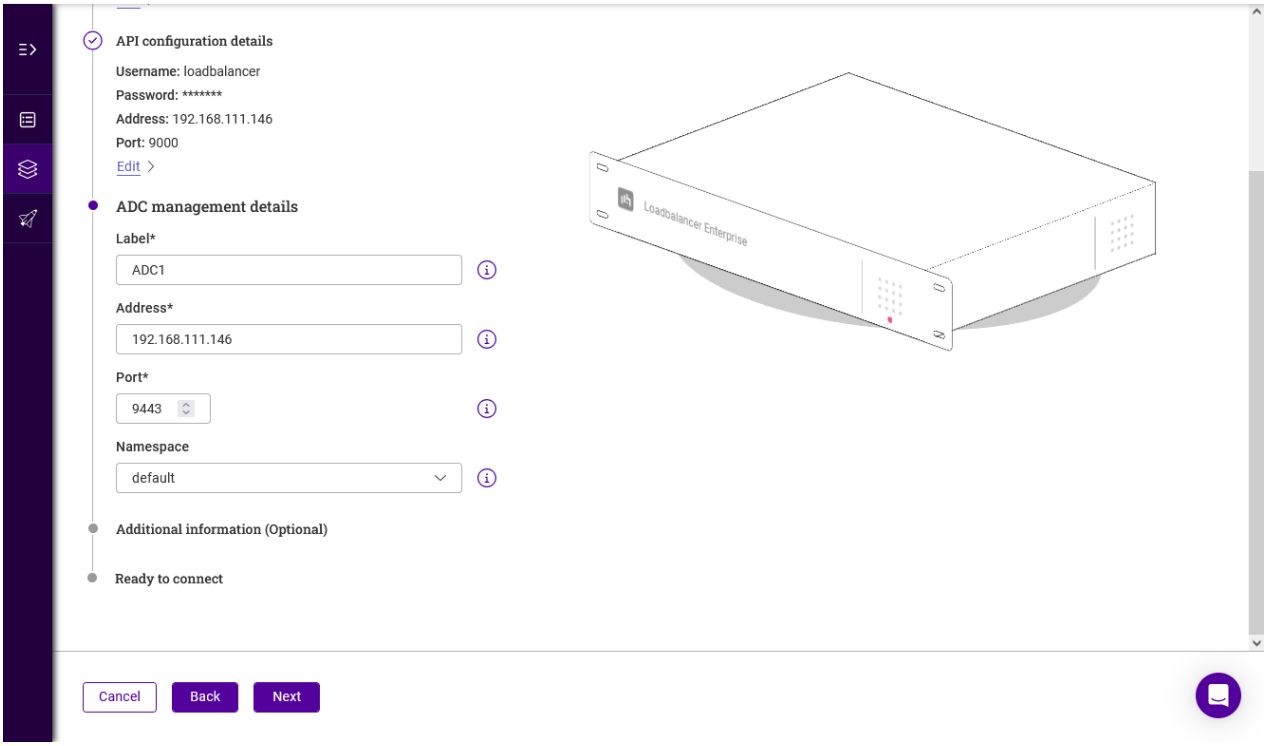


5. Using the ***Shuttle*** dropdown, select the required shuttle. If there is only one shuttle available, it will be greyed out and selected automatically as shown above.
6. Click **Next**.



7. Enter the ***Username*** and ***Password*** for a user account that has permissions to make API calls. For an Enterprise appliance, the "loadbalancer" account can be specified.
8. Enter the ***IP address*** of the appliance being added.

9. Leave the *Port* set to the default value (**9000**).
10. Click **Next**.



11. Enter an appropriate *Label* (name) for the appliance.
12. Ensure that the *IP Address* is correct.
13. Leave the *Port* set to the default value (**9443**).
14. Select the required *Namespace*.
15. Click **Next**.
16. Enter any required *Notes* and *Tags* to describe the appliance and click **Next**.

> **Note** To create a tag, enter the required name and hit <ENTER>. The tag will appear colored blue under the *Tags* field. Repeat to specify multiple tags (up to 30).

17. Verify all settings, these can be changed if needed using the relevant *Edit* option.
18. Click **Submit** - if the details have been specified correctly, the adopted appliance will appear in the list.

7.3. Viewing & Managing ADCs

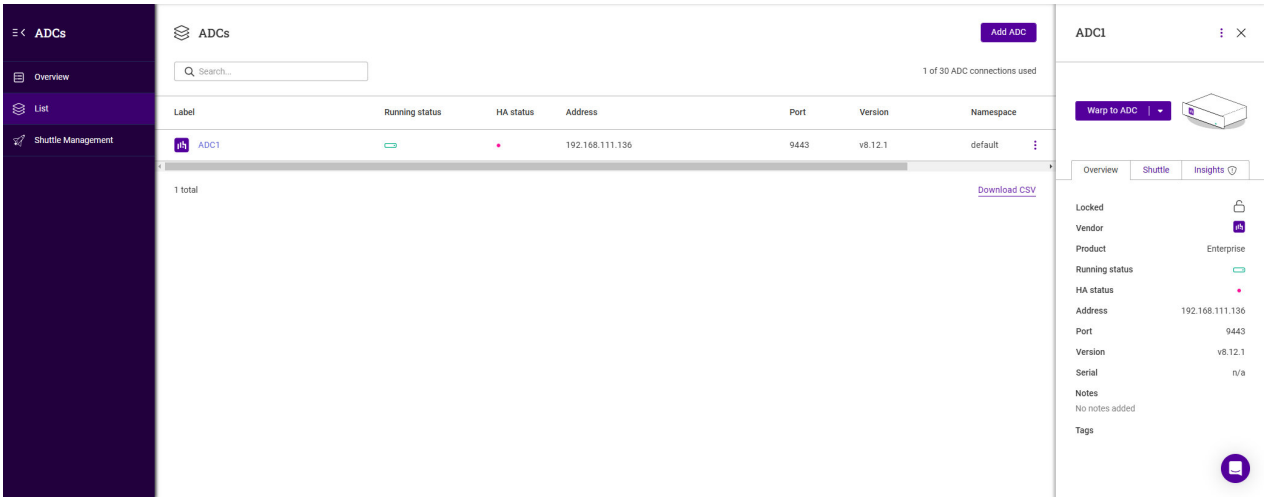
To view all ADCs:

1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the Dashboard.
2. A summary of the ADCs already added to the Portal will be displayed in the *ADCs* panel.
3. Click **View my ADCs** to see details of all ADCs.

4. All existing ADCs will be listed.

To view/manage a particular ADC:

1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the Dashboard.
2. In the *ADCs* panel, click **View my ADCs**.
3. Click the Label (name) of the ADC to be managed, a new information panel will be displayed to the right.



- The *Overview* tab provides a summary of the ADC.
- The *Shuttle* tab details which Shuttle is being used to connect to the Portal.
- The *Insights* tab details any security issues (CVEs) found.

7.3.1. Connect to an ADC's WebUI

The Portal enables instant, one-click access to any ADC's WebUI - for ADCs located in connected networks direct access can be used, for ADCs located in other networks WARP (not available with the Free Portal subscription level) can be used.

Using WARP

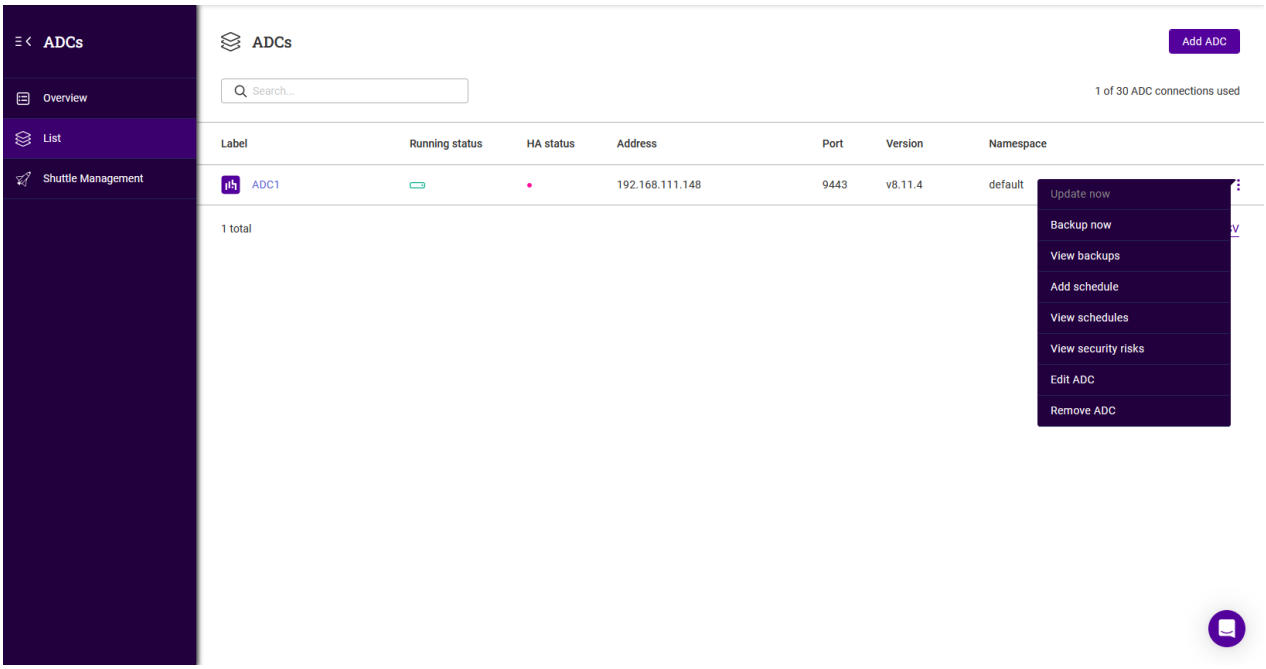
1. Click the Label (name) of the ADC to be viewed, a new panel will be displayed to the right.
2. Click **Warp to ADC** to securely connect to the ADC.
3. A new browser tab will open and display the WebUI.

Using Direct Access

1. Click the Label (name) of the ADC to be viewed, a new panel will be displayed to the right.
2. Click the down arrow on the **Warp to ADC** button and select **Direct access**.
3. A new browser tab will open and display the WebUI.

7.3.2. ADC Actions Menu

1. Click the three dots menu for the ADC, the actions menu will be displayed.



2. Select the required action:

   - **Backup now**
     - A backup of the ADC will be created.
   - **View backups**
     - All backups for this ADC will be listed.
     - To order by a particular column, click the column heading. The sort order (ascending or descending) is indicated by the arrow. Click the column heading again to change the sort order.
     - To download a backup:
       - Click the three dots menu to the right and click **Download**.
       - Enter your password and click **Submit**.
     - To delete a backup:
       - Click the three dots menu to the right and click **Delete**, then click **Confirm** to proceed.
   - **Add schedule**
     - The *Create Schedule* screen will be displayed.
     - The *Product Name* is set to the name of the ADC and *Schedule Type* is set to **Backup**.
     - Specify the required *Date*, *Time* and *Occurrence* and click **Save Schedule**.
   - **View schedules**
     - The *Schedules* screen will be displayed. Any schedules created for the ADC will be listed.
   - **View security risks**

- The *Security Insights* screen will be displayed. Any CVEs for the ADC will be listed.

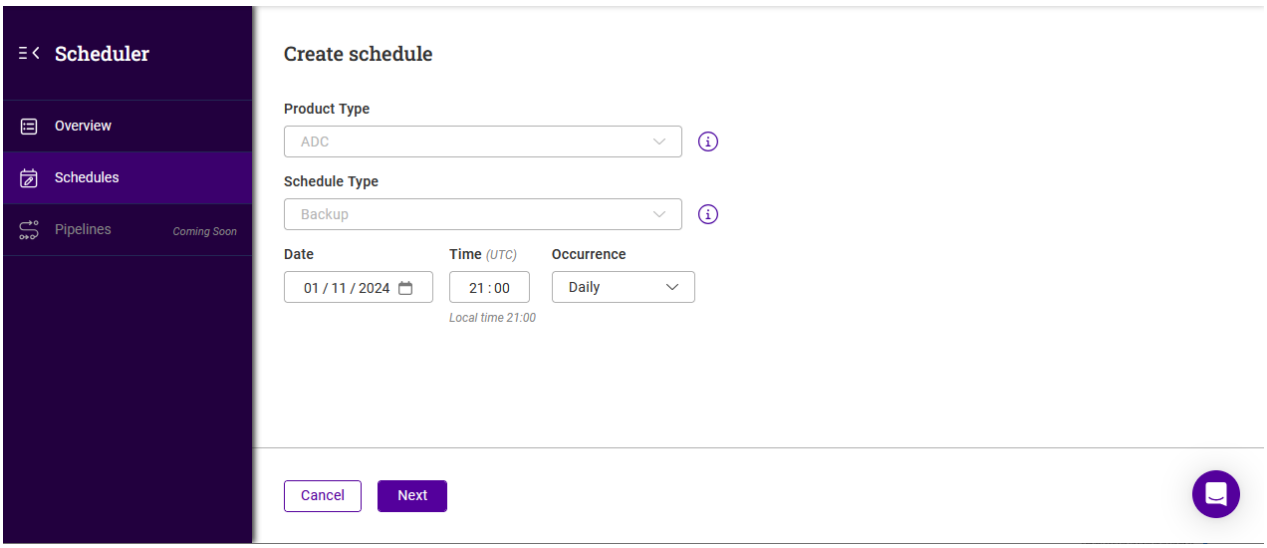
- **Edit ADC**
  - The *Edit ADC Details* screen will be displayed. Update the settings as required and click **Submit** to save.
- **Remove ADC**
  - Remove the ADC from the Portal. You'll be prompted to confirm that you want to proceed, click **Confirm** to remove the ADC.

8. Task Scheduler

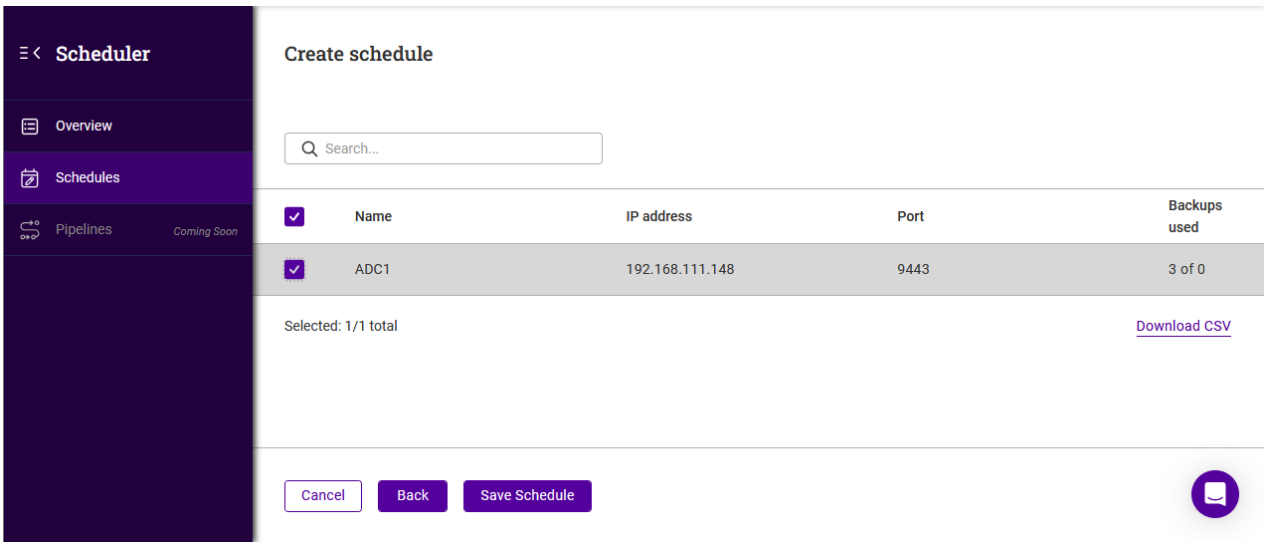
The task scheduler allows multiple tasks to be configured and scheduled. Currently, ADC backups can be scheduled. Other tasks including software updates are coming soon. Backups are securely stored in the Portal and can be easily viewed and either restored, downloaded or deleted.

To add a new schedule:

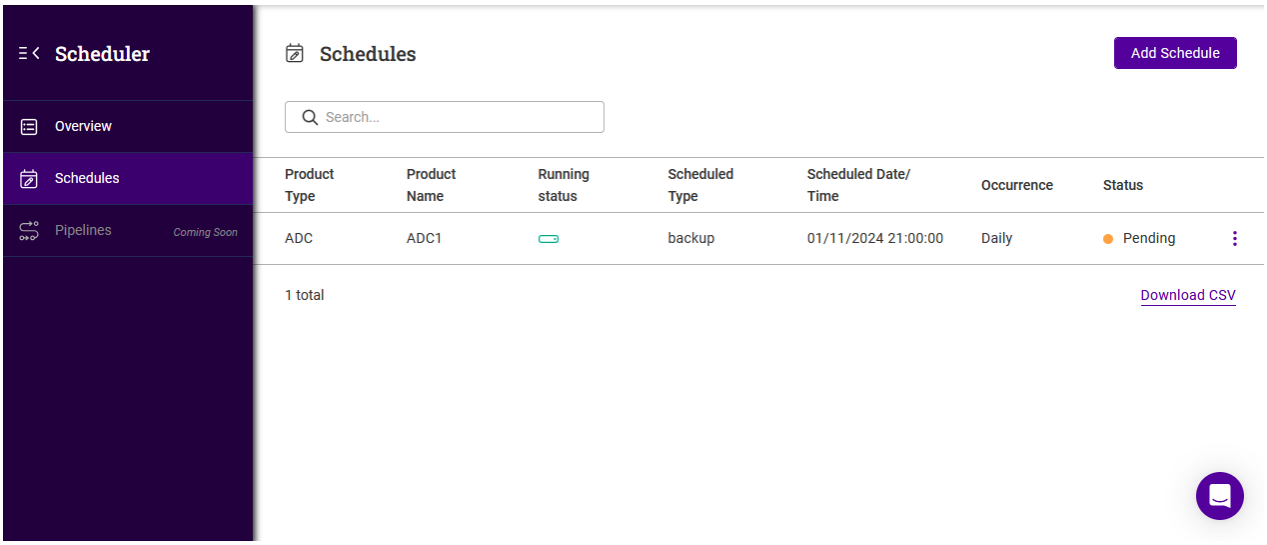
1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the Dashboard.
2. In the *Scheduler* panel:
   - If this is the first schedule to be added, click **Create a schedule**.
   - If schedules already exist, click **View my Schedules**.
     - Click the **Add Schedule** button.
3. The *Create Schedule* form will be displayed:



4. Specify the required *Date*, *Time* and *Occurrence*.
5. Click **Next**.



6. Using the checkboxes, specify which ADC(s) the schedule should apply to.
7. Click **Save Schedule**, the new schedule will appear in the Schedules list.



To delete a schedule:

1. Click the three dots menu next to the schedule to be deleted.
2. Click **Delete Schedule**, then click **Confirm** to delete the schedule.

9. Storage

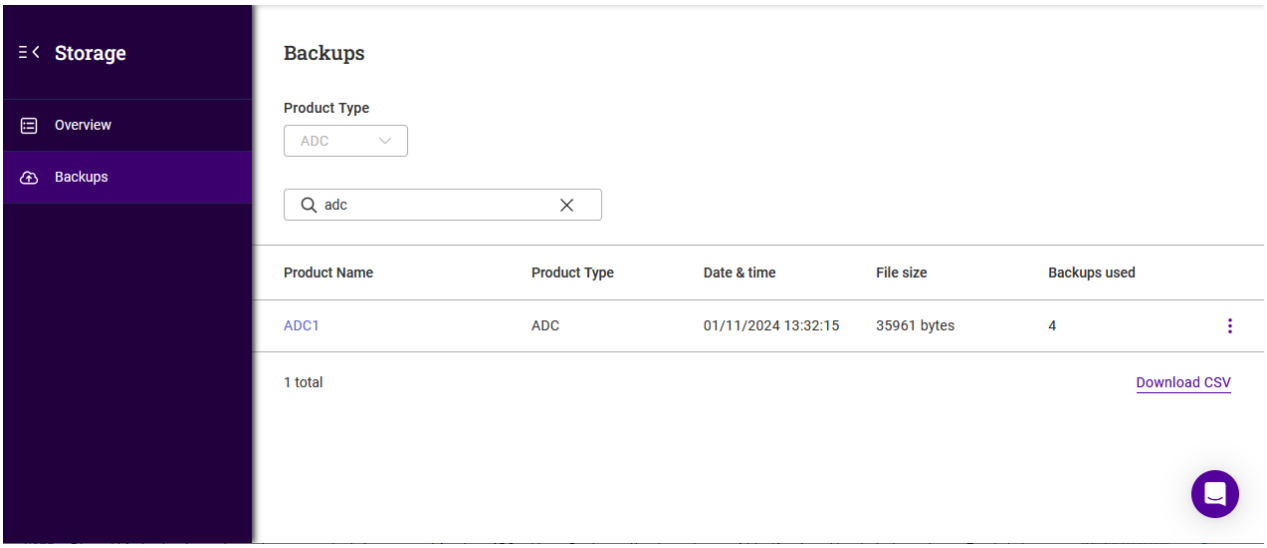
Backups can be easily viewed and either restored, downloaded for storage elsewhere, or deleted. All backups are encrypted and securely stored in the Loadbalancer.org ADC Portal.

To access storage:

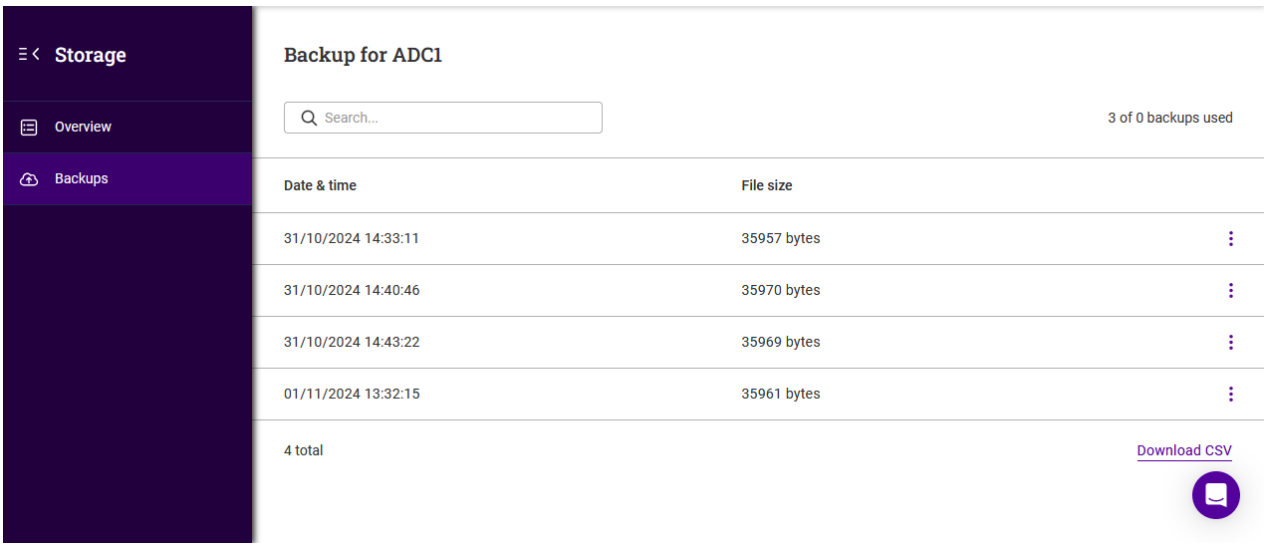
1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the Dashboard.
2. In the ***Storage*** panel:

- If there are currently no backups, click **Create a backup**.
  - The Create Schedule form will be displayed. For more details, see Task Scheduler.
- If backups already exist, click **View my Backups**.

3. Existing backups will be listed:



4. In this example, 4 backups have been created for ADC1.
5. To view all backups, click on the *Product name*, is this case **ADC1**.
6. Details of all backups will be displayed.



To download a backup:

1. Click the three dots menu next to the backup to be downloaded.
2. Select *Download*.
3. Enter your password in order to decrypt and download the backup and click **Submit**.
4. Note the **Backup Archive Password** (ADC appliance ID) that is displayed on screen. This is required as a

password for the encrypted file.

To delete a backup:

1. Click the three dots menu next to the backup to be deleted.
2. Click **Delete**, then click **Confirm** to delete the backup.

10. Security

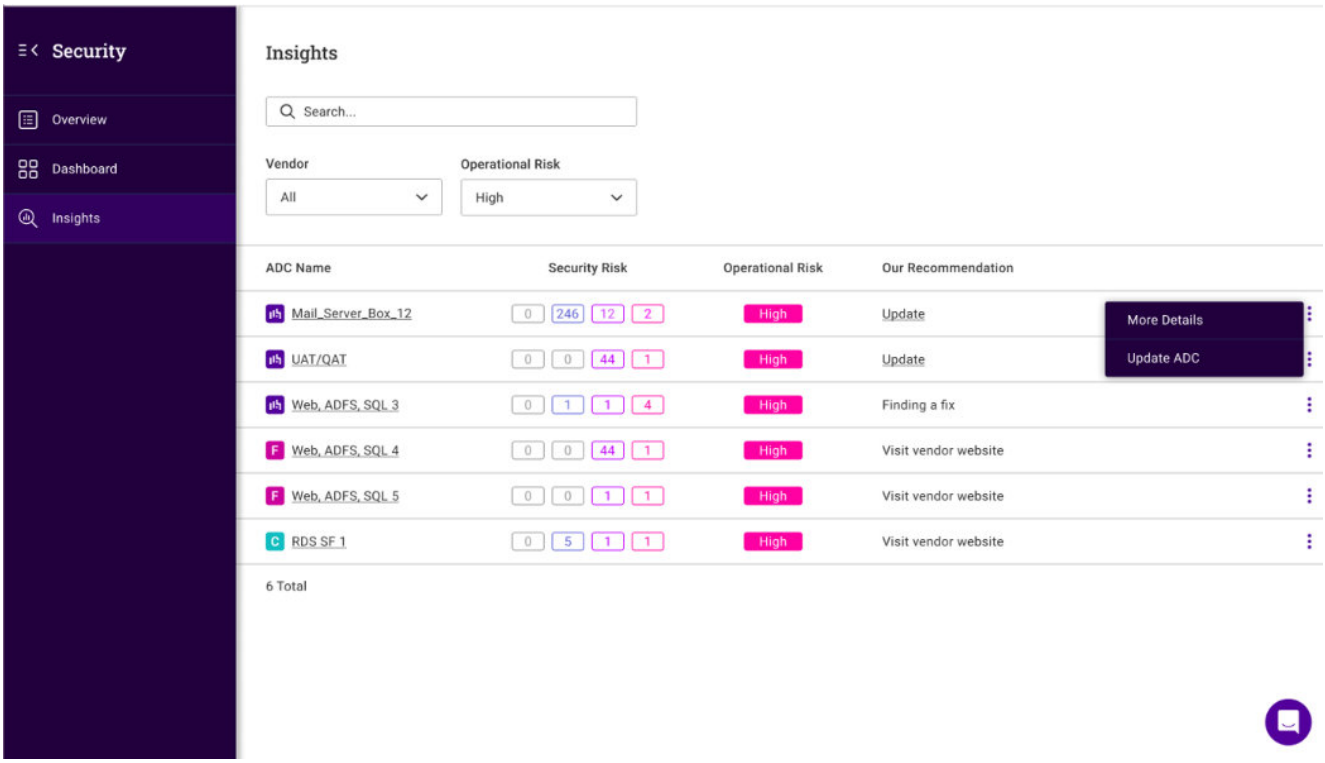
10.1. Security Insights

The ADC Portal provides continuous, real-time CVE (Common Vulnerabilities and Exposure) monitoring of all ADCs and ensures that any issues found are highlighted so that swift action can be taken.

To view security insights for all ADCs:

1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the Dashboard.
2. The number of risks detected is displayed in the ***Security Panel***.
3. Click **View my Security insights** to view details of any risks found.

Details of all CVEs complete with a recommendation of what action should be taken will be displayed as shown in the example below:



To view security insights for a particular ADC:

1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the Dashboard.

2. In the *ADCs* panel, click **View my ADCs**.
3. Click the three dots menu next to the ADC to be viewed and select **View security risks**.

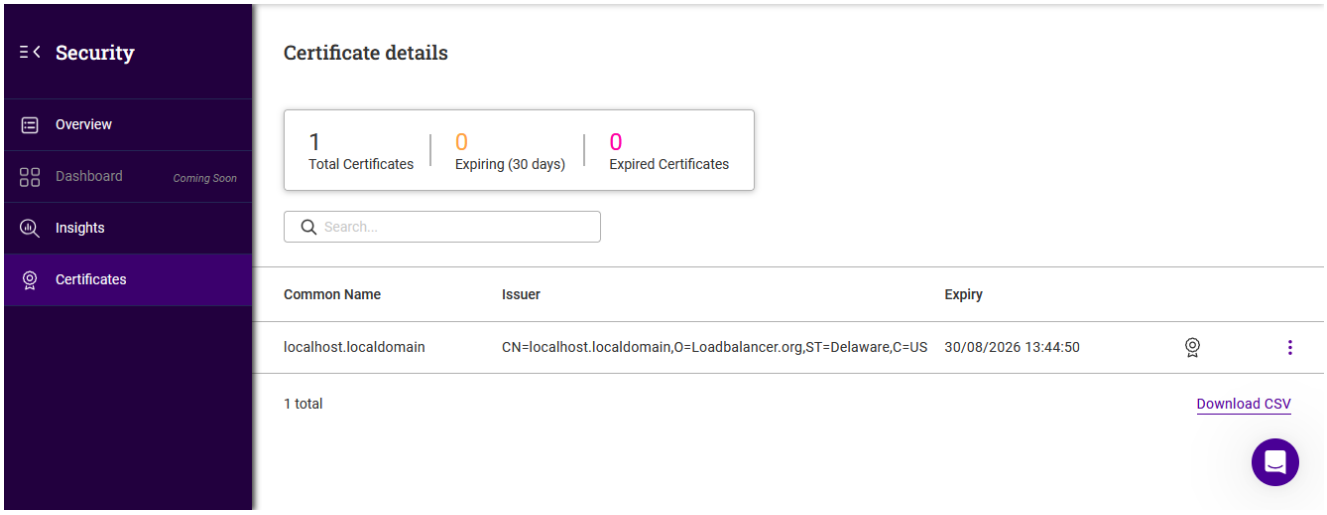
10.2. SSL Certificates

All SSL/TLS certificates installed in each ADC can be viewed from the Portal (not available with the Free Portal subscription level). This enables proactive monitoring to help ensure that expiring certificates are renewed or replaced before they expire.

To view all certificates for a particular ADC:

1. Click **LOADBALANCER** | PORTAL in the main menu bar to view the Dashboard.
2. In the *Security* panel, click **View my Security insights**.
3. In the menu to the left, select *Certificates*.
4. Select the ADC you'd like to view.

A summary of all installed certificates is displayed at the top and full details of each is displayed below as shown in the example below:



11. Governance & Compliance

Loadbalancer.org is an ISO 13485:2016, ISO 9001:2015, and ISO 27001:2022 certified company, adhering to the principles of security, availability, processing integrity, confidentiality, and privacy.

We hold our Quality Management System (QMS) in high regard and carry out regular security audits and penetration tests internally and with independent third parties.

12. Loadbalancer.org Technical Support

12.1. Accessing Technical Support

If you need assistance or have any questions, please don't hesitate to contact us.

12.1.1. Using Online Chat from the Portal

Click the Intercom icon in the bottom right-hand corner to use the online chat function to communicate with our support team.

12.1.2. Create a Support Ticket from the Portal

To create a support ticket:

1. Click the *Support* menu icon in the top right corner of the main menu bar and select *Get Support*.
2. Click the **Create Ticket** button.
3. Select the *Ticket Type* and *Product*.
4. Specify the *Subject* and enter your question in the box provided.
5. Click **Submit** to create the ticket.
6. Using the menu to the left, select *All Tickets* to view, update or close the ticket.

12.1.3. Email Us

To raise a support ticket via email, send a message to the support team : support@loadbalancer.org.

12.2. Service Status

To view the current status of all portal services:

1. Click the *Support* menu icon in the top right corner of the main menu bar and select *Service Status*.

12.3. Send Feedback

We always welcome your feedback and suggestions.

To provide feedback:

1. Click the *Support* menu icon in the top right corner of the main menu bar and select *Send Feedback*.
2. Click **Next**.
3. Provide your comments and click **Submit**.

12.4. Documentation

To access this documentation:

1. Click the *Support* menu icon in the top right corner of the main menu bar and select *Documentation*.

LOADBALANCER

Visit us: www.loadbalancer.org

Phone us: +44 (0)330 380 1064

Phone us: +1 833 274 2566

Email us: info@loadbalancer.org

Follow us: @loadbalancer.org

About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.