

Aurora 2.5

Administration Guide

Condrey Corporation
August 17, 2022

Condrey Corporation makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Condrey Corporation reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Condrey Corporation makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Condrey Corporation reserves the right to make changes to any and all parts of the software at any time, without obligation to notify any person or entity of such revisions or changes. See the Software EULA for full license and warranty information with regard to the Software.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Condrey Corporation assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2022 Condrey Corporation. All Rights Reserved.

No part of this publication may be reproduced, photocopied, or transmitted in any fashion without the express written consent of the publisher.

Condrey Corporation
122 North Laurens St.
Greenville, SC, 29601
U.S.A.
http://condrey.co

CONTENTS

1 APPLICATION OVERVIEW AND STRUCTURE 5

1.1 Aurora 6
1.2 Aurora .Ext 6

2 MANAGING AURORA FOR INTERNAL USER ACCESS 7

2.1 Configure Authentication and Authorization 7
2.2 Configure Automatic Storage Mappings 8
2.2.1 Home Folders 8
2.2.2 Senergy-Managed Paths 8
2.3 Configure Manual Storage Mappings 8
2.4 Manage Internal Users 9
2.4.1 View Registered Users 9
2.4.2 Remove a User 10
2.4.3 Reset Two-Factor Authentication 12

3 MANAGING AURORA .EXT FOR GUEST ACCESS 14

3.1 Enable Sharing 14
3.2 Configure Mail Delivery 14
3.3 Manage Provider Rules 14
3.3.1 Understanding Provider Rules 14
3.3.2 Configuring Provider Rules 15
3.3.3 Provider Rule Path Name Considerations 18
3.3.4 Provider Rule Security Considerations 19
3.4 Configure Proxy Account File System Access 20
3.5 Manage Guest Accounts 20
3.5.1 Create a Guest Account 20
3.5.2 View Guest Accounts 21
3.5.3 Edit a Guest Account 22
3.5.4 Delete a Guest Account 23
3.5.5 Modify the Account Policy 23
3.6 Manage Guest Shares 25
3.6.1 View All Guest Shares 25
3.6.2 Access Share Content 25
3.6.3 Delete a Guest Share 26

4 CONFIGURATION SETTINGS 27

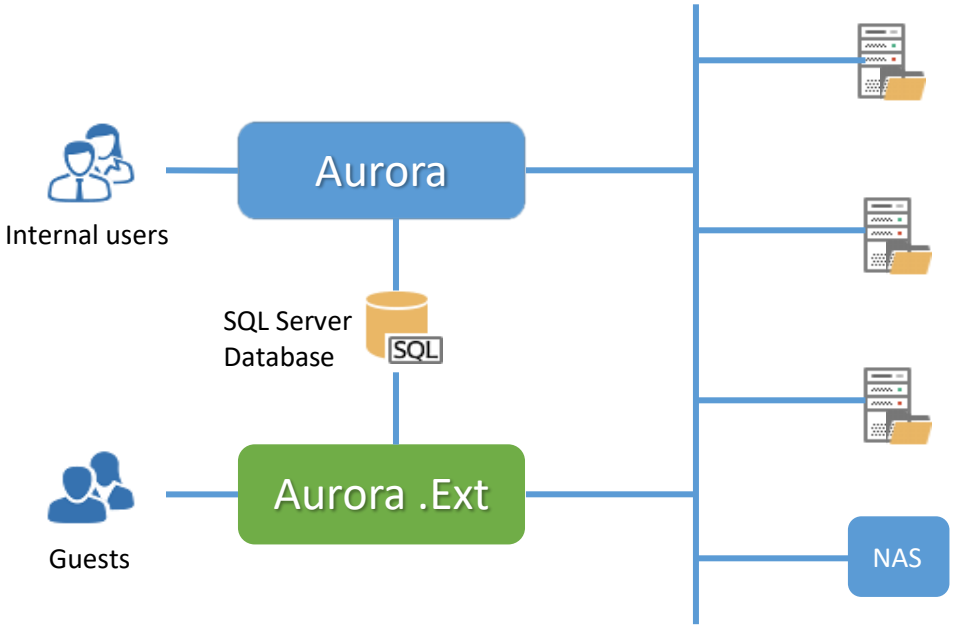
4.1 General Configuration 28
4.1.1 Licensing 29
4.1.2 Basic Integration 30
4.1.3 Senergy Integration 31
4.1.4 Aurora Web Configuration 32
4.1.5 Aurora .Ext Web Configuration 32

4.2 User Access 33
4.2.1 User Authorization *33*
4.2.2 Two-Factor Authentication *34*
4.3 Branding 35
4.4 Storage Map 37
4.4.1 Add a Storage Map Entry *38*
4.4.2 Edit a Storage Map Entry *38*
4.4.3 Delete a Storage Map Entry *38*
4.4.4 Sharing 39
4.4.5 Mail 41
4.5 Mail Templates 43
4.5.1 Placeholder Tokens *44*
4.5.2 Saving a Template *45*
4.5.3 Testing a Template *46*
4.5.4 Recovering the Default Templates *47*
4.6 Logging 48
5 UNDERSTANDING FILE ACCESS 50
5.1 File Access for Internal Users via Aurora 50
5.2 File Access for Guest Users via Aurora .Ext 50
5.2.1 Share Permissions and the Guest Account *52*
5.2.2 File System Permissions and the Proxy Account *52*
6 CUSTOMIZING AURORA 53
6.1 Site Names and Titles 53
6.2 Customized Mail Templates 54
6.3 Sign-in Page Customization 55
6.3.1 Customizing the Background *55*
6.3.2 Adding Custom Help Link *56*
6.4 Customizing other Web Elements 57
APPENDIX A – KNOWN ISSUES 58
APPENDIX B – TROUBLESHOOTING TWO-FACTOR AUTHENTICATION 59
Resetting 2FA for Aurora Admins 59
GLOSSARY 61

1 Application Overview and Structure

The Aurora product suite consists of a set of products working in concert with your enterprise Active Directory environment.

- **Aurora** – The main web application. It is used for the following purposes:
  - Administrative configuration and management
  - End-user remote access for network file systems
  - End-user creation and management of sharing relationships with guest users outside of the organization
- **Aurora .Ext** – The access portal that provides remote file access for Guest users. Self-service account registration and management are provided through the portal as well. This subsystem may be enabled or disabled, and the security is governed by the Aurora administrator.
- **Database** – A Microsoft SQL Server database provides storage for key configuration and management structures as well as storage for Guest accounts and Guest Shares.



1.1 Aurora

When internal users authenticate to Aurora, they are accessing the network file system with their credentials, and their access to files is governed solely by security in NTFS and Active Directory. That is, a user session is created and the user accesses files just as he would on a Windows workstation attached to the domain. As a result, there is no proxy-based access to the file system.

For more information, see sections *2 Managing Aurora for Internal User Access* and *5.1 File Access for Internal Users via Aurora*.

1.2 Aurora .Ext

Guest users always access files through the Aurora .Ext application. A Guest user may register his account as his email address and the account must be confirmed via email before any access to files is allowed.

Guest access is governed by Guest Share records stored in the database. A Guest Share record includes the file system path for access as well as other information such as the internal user that created the share, access rights, and share expiration.

All Guest account access to the file system is performed via a proxy account created specifically for this purpose. All access is logged in the auditing table in the SQL database. Administrators govern what areas of the network file system can be shared and the maximum rights that may be assigned.

For more information, see sections *3 Managing Aurora .Ext for Guest Access* and *5.2 File Access for Guest Users via Aurora .Ext*.

2 Managing Aurora for Internal User Access

Aurora defines **Internal Users** as those users that already exist in your organization and have an account in the Active Directory environment.

Setting up Aurora to work with Internal Users is rather simple:

- Configure authorization for approved Aurora users.
- Configure automatic storage mappings.
- Configure any manually defined storage mappings.
- Optionally enable Sharing and configure Provider Rules so that Internal Users can give access to external Guests.

2.1 Configure Authentication and Authorization

Internal Users are Active Directory user accounts that are configured for Aurora access. When configuring Aurora, an **Authorized Aurora Users** group is defined. Users or other security groups may be added to this group, giving all members authorization to use Aurora.

There may be cases where members of an included group should be denied access from Aurora. For these cases, an **Excluded Users** group may be optionally defined. Members of this group will always be denied access to Aurora, unless they are also included in the **Aurora Administrators** group.

Members of the **Aurora Administrators** group are always granted full access as authorized users and have access to manage Aurora itself.

An optional **Two-Factor Required Users** group may be defined. Aurora always requires members of this group to sign in using two-factor authentication. Users in this group must register a two-factor authentication app and use the associated one-time passcode upon authentication.

Nested group membership is included for each group: Authorized Users, Excluded Users, Two-Factor Required Users, and Aurora Administrators.

To configure the Aurora groups via the *Web Application* component of the **Aurora Configuration Dashboard** utility, see *Aurora Web Application Configuration* in the *Aurora 2.5 Installation and Deployment Guide*.

Refer to section *4.2.1 User Authorization* to modify the Authorized Users, Excluded Users, and Two-Factor Required group references via the Aurora web application.



The Aurora Administrators group may only be configured from the *Web Application* section of the **Aurora Configuration Dashboard** utility.

2.2 Configure Automatic Storage Mappings

Automatic storage mappings include:

- Home Folders
- *Senergy*-managed Collaborative Storage paths
- *Senergy*-managed Auxiliary Storage paths

2.2.1 Home Folders

Internal Users that have the *homeDirectory* attributed populated with a UNC network path in their Active Directory user object can take advantage of the automatic Home Folder storage mapping in Aurora.

To enable Home Folder mapping, refer to section *4.1.2 Basic Integration*.

2.2.2 Senergy-Managed Paths

Senergy is a file system management product from Condrey Corporation that provides automation of user and collaborative storage management. Aurora can take advantage of the following aspects of user and collaborative storage managed by a *Senergy* installation:

- **Home Folders** – home folders managed by *Senergy* update the associated *homeDirectory* attribute of any managed users in Active Directory. This ensures a consistent experience for accessing Home Folders by Aurora.
- **Auxiliary Storage Paths** – users managed by *Senergy* may have other data on their user object identifying Auxiliary Storage paths. These paths are managed by *Senergy* and act as secondary storage mappings in addition to any Home Folder. Aurora can automatically find and present any Auxiliary Storage paths associated with users.
- **Collaborative Storage Paths** – security groups managed by *Senergy* have other data stored in their Active Directory objects identifying associated managed storage paths. Aurora can automatically find and present these associated paths for users that are members or managers of these groups.

To enable *Senergy* integration for automatic storage mappings, refer to section *4.1.3 Senergy Integration*.

2.3 Configure Manual Storage Mappings

In addition to automatic storage mappings, you can configure other manually defined storage mappings. Each of these storage mapping is defined with a network path, an Active Directory security group or user, and a simple alias. Each storage mapping applies to users who are members of the associated group or user.

To setup and manage the Storage Map, refer to section *4.4 Storage Map*.

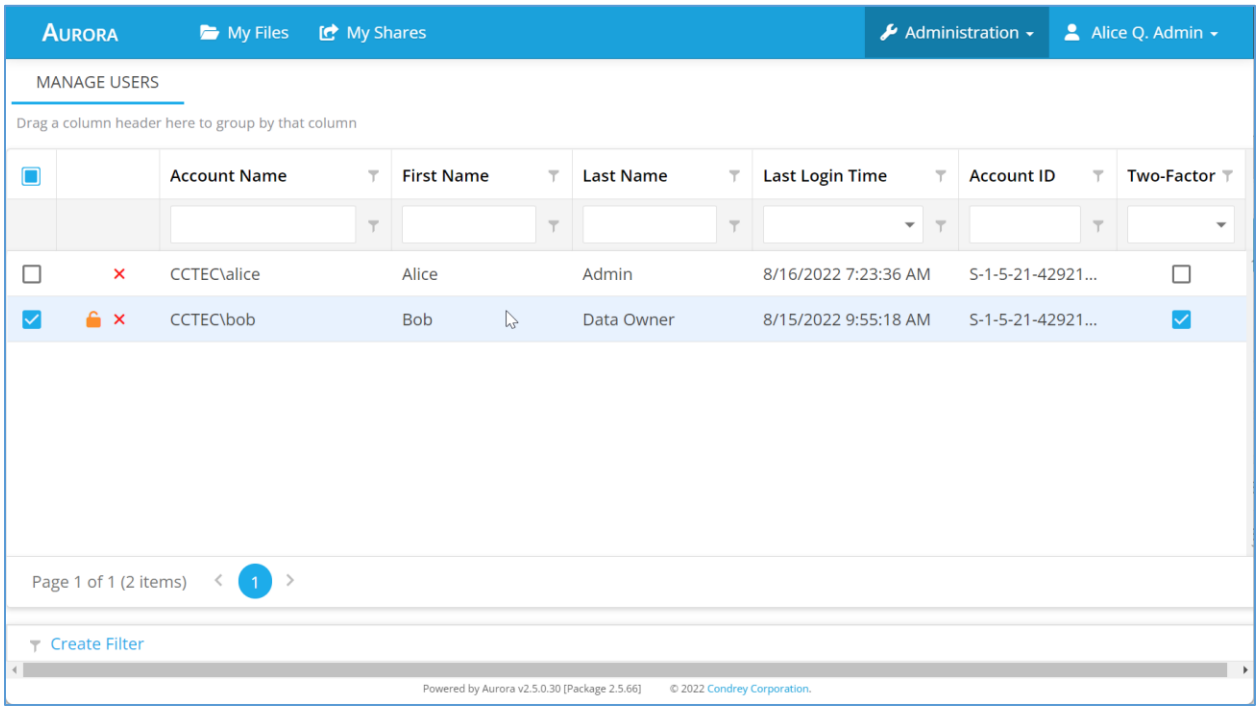
2.4 Manage Internal Users

Aurora maintains a list of Internal Users that sign-in and access Aurora. This list caches a set of user identity information including user account, first and last name, unique identifiers from Active Directory, last sign-in time, and the data necessary to support any two-factor authentication registrations.

2.4.1 View Registered Users

To view the current list of Internal Users:

1. Sign in with an Aurora administrator account.
2. Click the *Administration* menu, then select *Users* from the drop-down list.

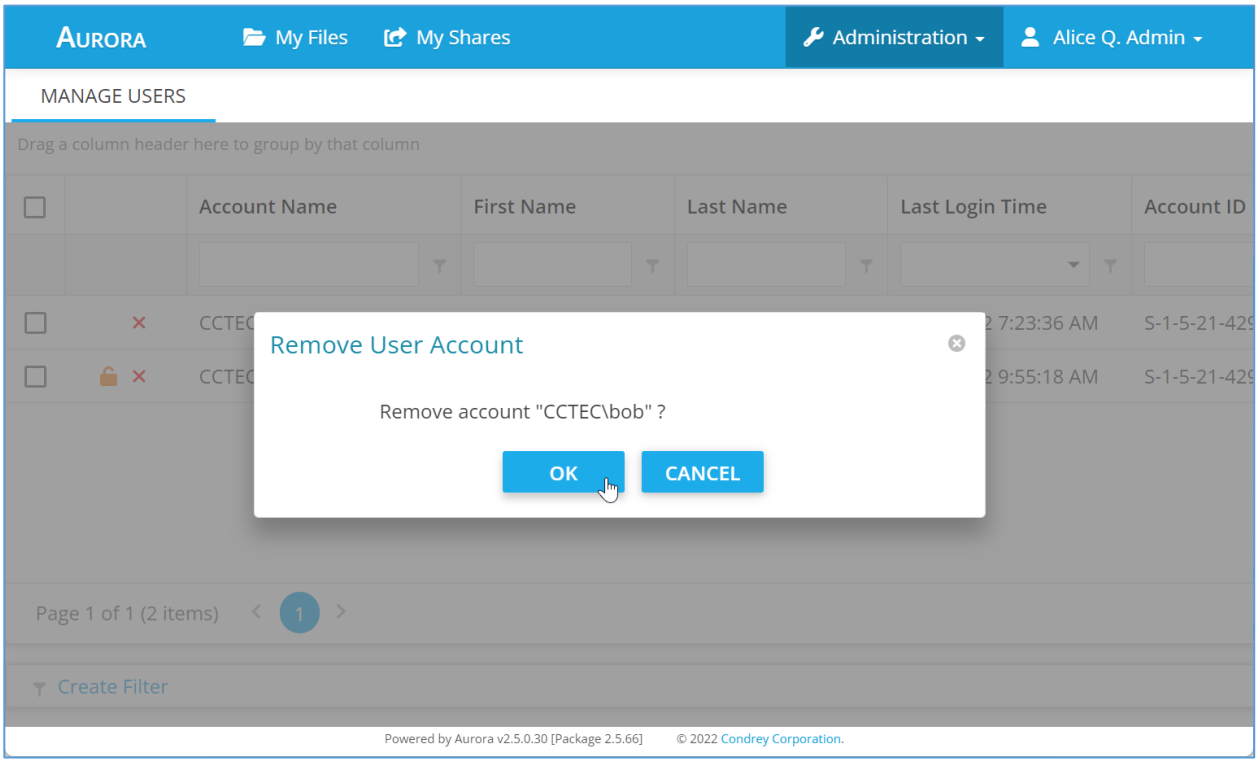


Internal Users management is new with Aurora 2.5. If you have recently upgraded from an earlier version of Aurora, the Internal Users list will not be populated. After upgrading, Aurora will add users to this list as they sign-in.

2.4.2 Remove a User

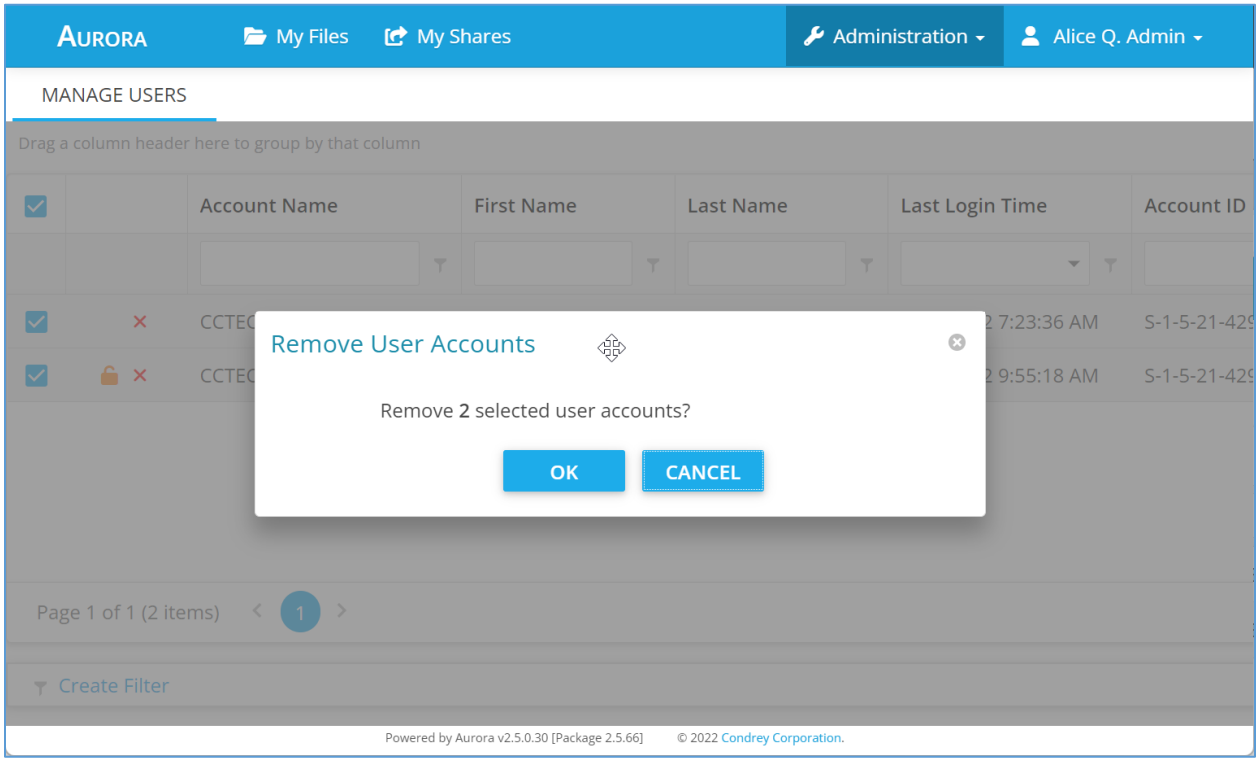
To remove a single user from the list of currently registered accounts:

1. Sign in with an Aurora administrator account.
2. Click the *Administration* menu, then select *Users* from the drop-down list.
3. Click the delete icon ✖ on the User entry you want to remove.
4. Click *OK* in the confirmation dialog to remove the user from the list.



To remove multiple users from the list of currently registered accounts:

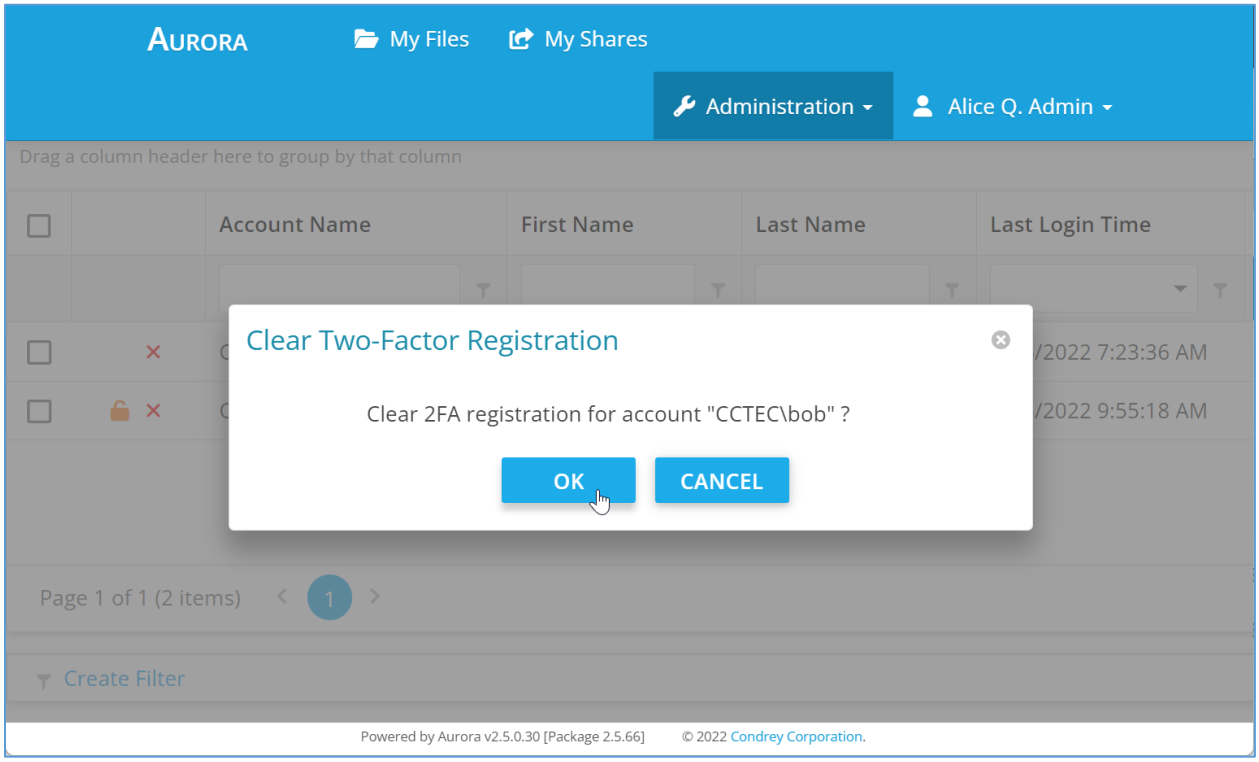
1. Sign in with an Aurora administrator account.
2. Click the *Administration* menu, then select *Users* from the drop-down list.
3. Select the checkbox for each user you wish to remove.
4. Click the delete icon ✖ on any of the selected the user entries.
5. Click *OK* in the confirmation dialog to remove the users from the list.



2.4.3 Reset Two-Factor Authentication

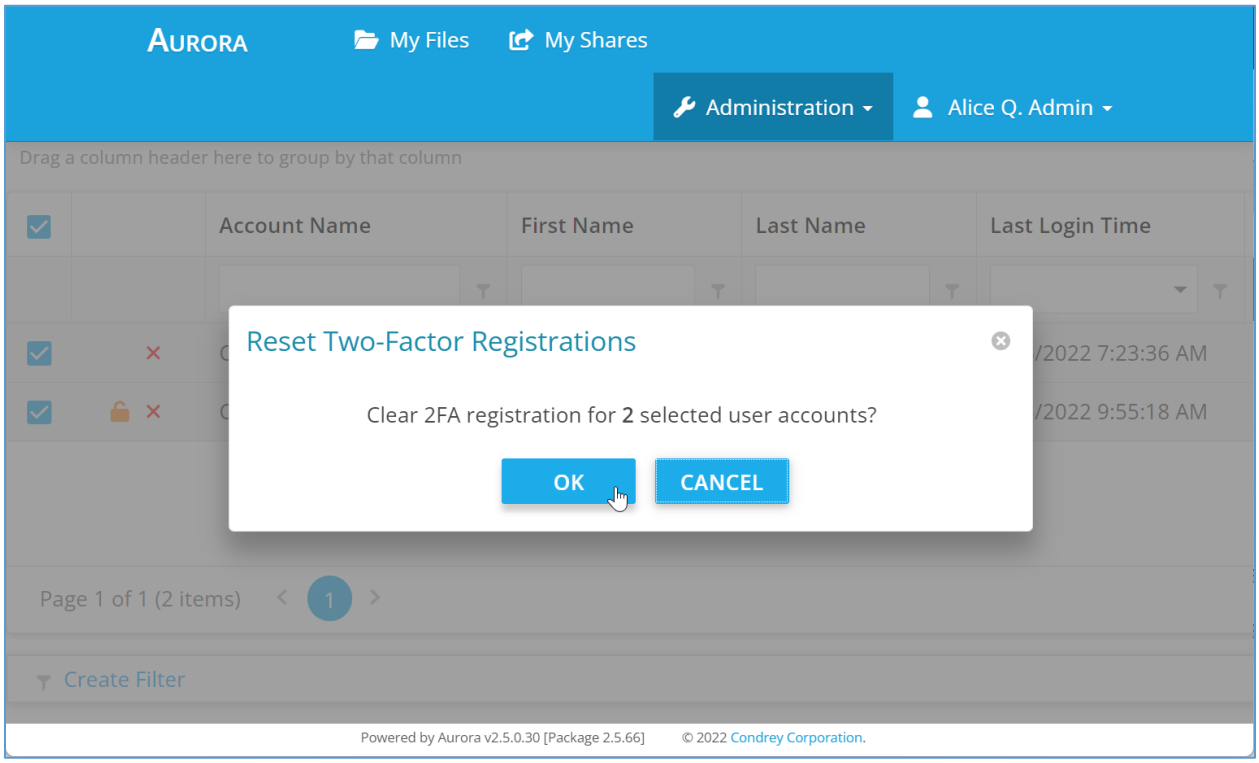
To reset a single user's 2FA registration:

1. Sign in with an Aurora administrator account.
2. Click the *Administration* menu, then select *Users* from the drop-down list.
3. Click the unlock icon for the desired user entry.
4. Click *OK* in the confirmation dialog to unregister that user's 2FA token.



To reset multiple user 2FA registrations:

1. Sign in with an Aurora administrator account.
2. Click the *Administration* menu, then select *Users* from the drop-down list.
3. Click the unlock icon on any of the selected the user entries.
4. Click *OK* in the confirmation dialog to unregister the selected users' 2FA tokens.



3 MANAGING AURORA .EXT FOR GUEST ACCESS

Although Aurora .Ext is installed as a separate web application for Guest access, most management of Guest accounts and Guest Shares takes place in the Aurora web application.

3.1 Enable Sharing

Before any sharing takes place, sharing must be enabled.

To enable sharing:

1. Sign in with an Aurora administrator account.
2. Click the *Administration* menu, then select *Configure* from the drop-down list.
3. Select the *Sharing* tab.
4. Select the *Enable Sharing* checkbox.
5. Save the settings.

Once sharing has been enabled, the Aurora .Ext application should become available for Guest access, the *My Shares* menu option will become available in Aurora, and the main Aurora file navigation page will display the Sharing panel.

3.2 Configure Mail Delivery

A key part of Guest access is notification email delivery. Email is needed for notifying creation of Guest Shares, as well as alerting Guests when updates occur and supplying a channel for self-service Guest registration and password management.

To configure the mail delivery subsystem, refer to section *4.4.5 Mail*.

3.3 Manage Provider Rules

Provider Rules decide which Internal Users are allowed to share which storage paths and with what permissions to Guest users.

As an administrator, it is important to understand that unless a Provider Rule has been defined for a given storage path, no one can share any content from that path with Guest users.

Additionally, it is important to understand what a configured Provider Rule grants to Internal Users, and the security implications that go with that delegation.

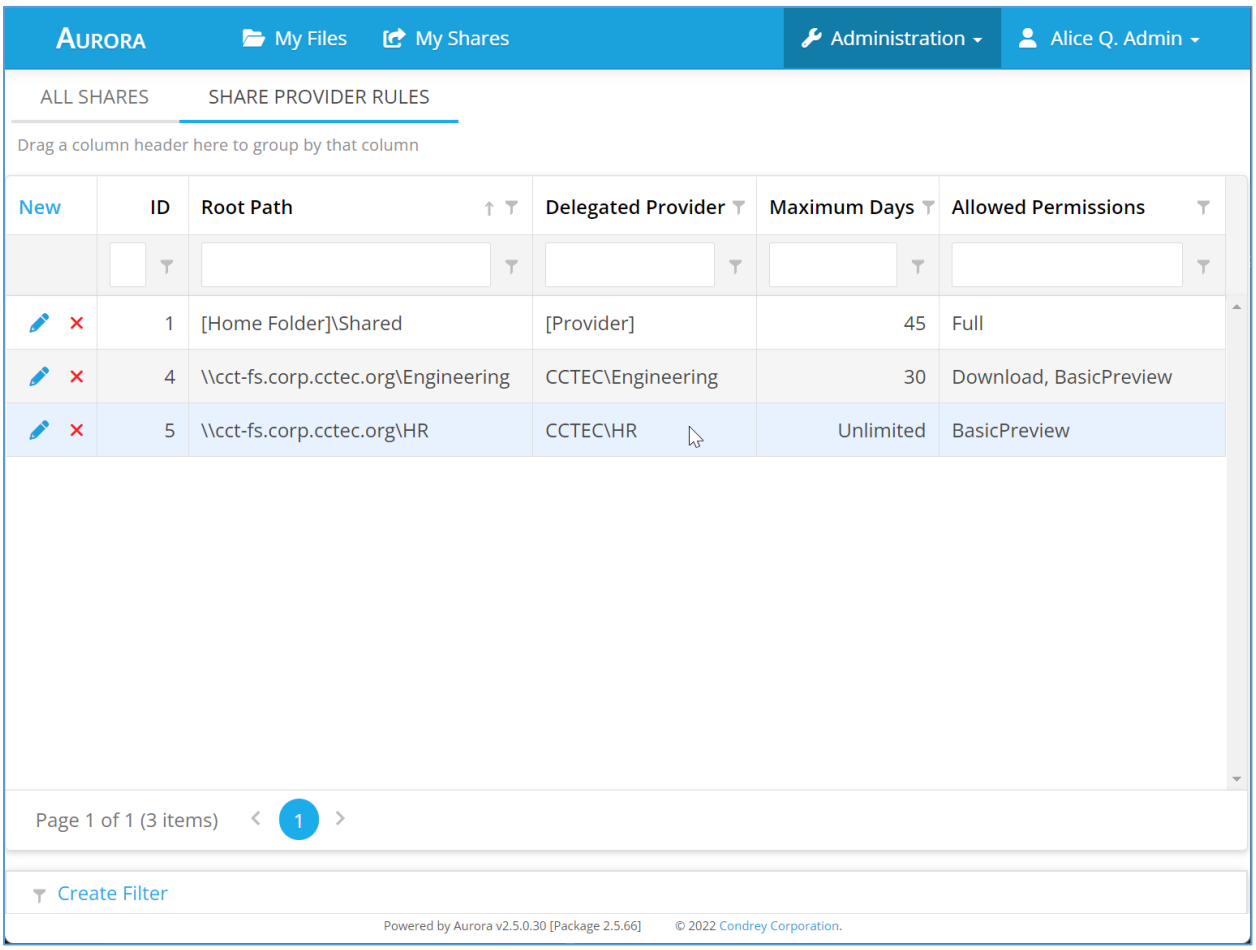
3.3.1 Understanding Provider Rules

Defining Provider Rules is essentially delegating file system sharing management to trusted Internal Users within the organization.

A single Provider Rule includes a *Root Path*, a trusted Internal User or user group as the *Designated Provider*, and a set of allowed permissions that may be delegated. By defining a Provider Rule, you are implicitly saying that you trust one or more organizational users (Internal Users) to become *Providers* who may give managed access to appropriate users outside the organization (Guest users).

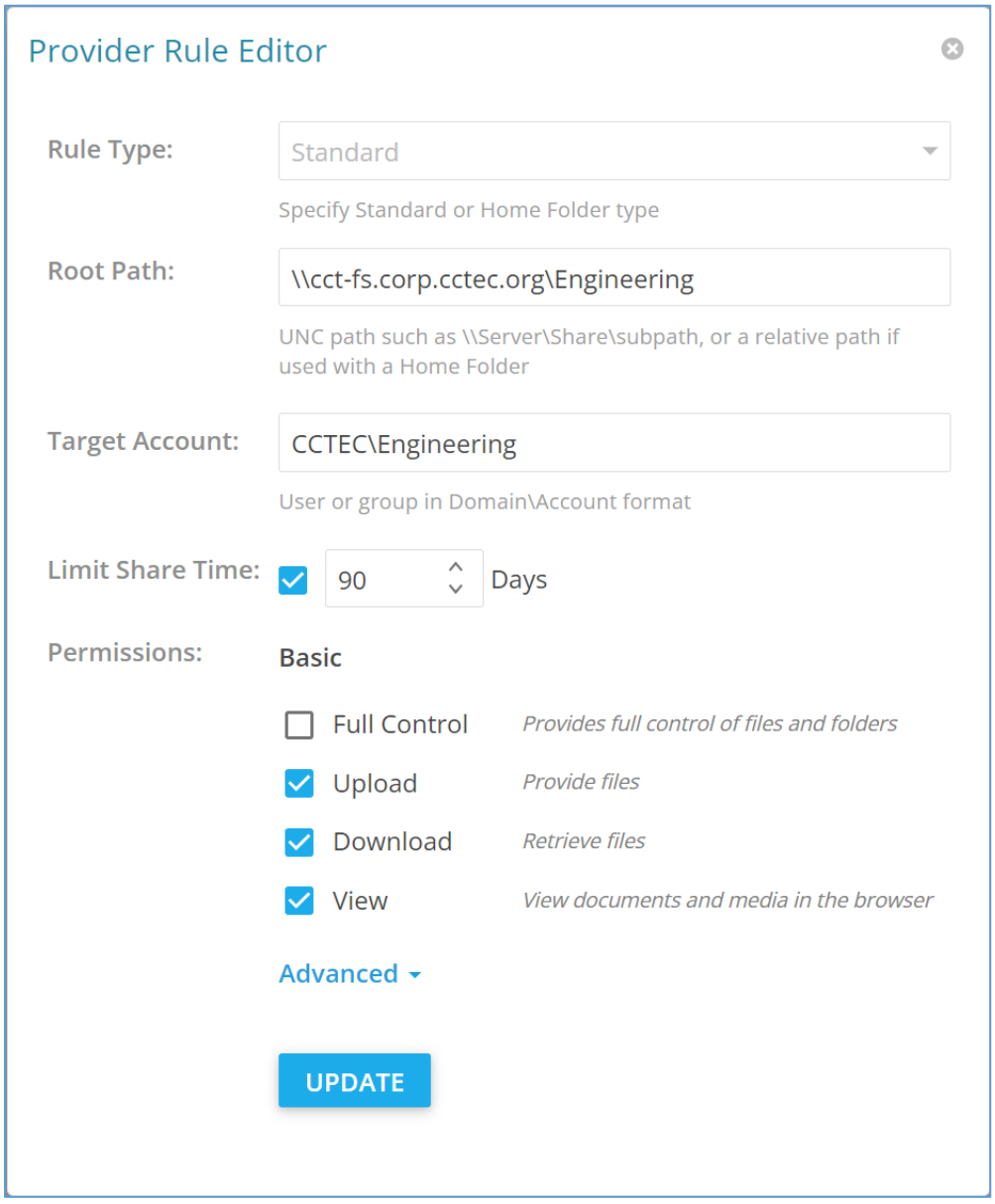
3.3.2 Configuring Provider Rules

By default, no Provider Rules are defined, and no Internal Users can act as Share Providers for Guests.



For each Windows file share or path where Aurora sharing is to be allowed, at least one Provider Rule must exist. Multiple Provider Rules may be defined for the same *Root Path* so long as each specified *Provider* is unique.

3.3.2.1 Add a Provider Rule



To add a Provider Rule:

1. Click *New* in the column header.
2. Select the *Rule Type*.

   Home Folder – only applies to automatically mapped Home Folders

   Standard – applies to all other paths
3. Specify a *Root Path*
   a. For **Standard** rule types, specify a *Root Path* in UNC format. Please note that the full UNC path prefix must match exactly (case insensitive) with the mapped path. See *3.3.3 Provider Rule Path Name Considerations* for more details.
   b. For a **Home Folder** rule type, optionally specify a relative path.

      If specified, the Home Folder rule only applies to sub-paths in home folders that match or are found beneath the relative path.

      If empty, the rule applies to the entire Home Folder.
4. Specify a *Target Account* in *Domain\Name* format. The target account may be either a user or a security group.
5. Select the allowed *Permissions*.
6. Optionally select *Limit Share Time* and specify a maximum number of days a share may be provided.
7. Click *Update* when complete to save the rule.



The **Home Folder** Provider Rule is a special rule that may only occur once in the Provider Rules list. If defined, this rule dynamically applies to any discovered Home Folder associated with the current user.

Processing of this rule is also dependent on the *Home Folder Storage* setting being enabled in *Basic Integration*. See *4.1.2 Basic Integration* for details on setting this flag.



The *Limit Share Time* property of Provider Rules only applies to the rule with the closest matching path.

3.3.2.2 Edit a Provider Rule

To edit a Provider Rule:

1. Click the pencil icon next to the desired Provider Rule or double-click the row.
2. [Optional] – change the *Root Path* in UNC format. Please note that for Standard rule types, the full UNC path prefix must match exactly (case insensitive) with the mapped path. See *3.3.3 Provider Rule Path Name Considerations* for more details.
3. [Optional] – change the *Target Account* in *Domain\Name* format. The target account may be either a user or a security group.
4. [Optional] – change the allowed *Permissions*.

Click *Update* when complete to save the rule.

3.3.2.3 Delete a Provider Rule

To delete a Provider Rule:

1. Click the delete icon on the Provider Rule entry you want to remove.
2. Click *OK* in the confirmation dialog to delete the rule.

3.3.3 Provider Rule Path Name Considerations

Since Provider Rules perform simple path matching against existing Home Folder, Storage Map paths, and *Senergy* managed paths, the same UNC paths must be used.

As a best practice, it is recommended that server DNS names are used instead of NetBIOS names. For example, a server with a DNS name such as **cctms1.cctec.org** may have just **CCTMS1** as its NetBIOS name. When evaluating a Provider Rule, the entire UNC path prefix must match case-insensitively. If a Storage Map entry, for example, is defined as \\cctms1\Share but the associated Provider Rule specifies a *Target Path* of \\cctms1.cctec.org\Share, the rule will not match.

\\cctms1\Share ≠ \\cctms1.cctec.org\Share

This issue lies primarily with manually defined Storage Map entries: *Senergy* records all its managed paths using server DNS naming by default, and the special Home Folder mapping with its associated Home Folder Provider Rule automatically handles path matching for its discovered paths.

3.3.4 Provider Rule Security Considerations

Provider Rule management should include careful consideration of the following security implications. Disregarding these considerations could lead to incorrectly escalated privileges or at the least, unexpected permissions.

- Provider Rules are inherited – the settings for a Provider rule defined on a parent path are inherited by all sub-paths.
- Provider Rules are attached to shares – when a Guest Share is created, the effective provider rules are stamped onto the share itself. Changes to a matching Provider Rule do not affect a share after it has been created, even if the share is changed.
- Provider Rule Permissions are allow-only –to keep rule management simple, only “Allow” permissions are available. If a permission is set by a rule on a parent path for a given user or group, there is no way to override or deny that permission on a sub-path.
- Provider Rule Permissions are additive – a Provider Rule’s permissions on a sub-path do not “override” any Provider Rule permissions from a parent path, but instead, add to them. For example, if a Provider Rule allows **Upload** for a parent path, and another one gives **Download** to a sub-path, the effective permissions available for delegation by that user on the sub-path are **Upload** *and* **Download.**
- Provider Rule Permissions do not account for existing File System permissions – if an Internal User only has read access to a given NTFS path via existing ACEs but is delegated Full Control sharing permissions via a Provider Rule, there is potential for that user to elevate his access by simply sharing that path (or a sub-path) with himself. It is important to understand that the Provider Rules and the rule calculation subsystem do not currently have any knowledge of Internal Users’ file system access.
  This consideration also extends to scenarios where Deny ACEs may be in place for delegated Providers on sub-paths in the file system.

  The following two rules sum this up:

- Do not assign Internal Users as Providers for a path where Deny ACEs are in place on sub-paths.
- Do not assign Internal Users as Providers for a path where the set of delegated share permissions exceeds what they currently have for the specified path or one of its sub-paths.

3.4 Configure Proxy Account File System Access

Guest access is managed by two layers of security, the first being the share permissions defined in the Guest Share itself, and the second being the proxy account access at the Windows share and file system levels.

Essentially, for every storage location that could be shared with Guest accounts, the Aurora proxy rights account must have at least the same level of access.

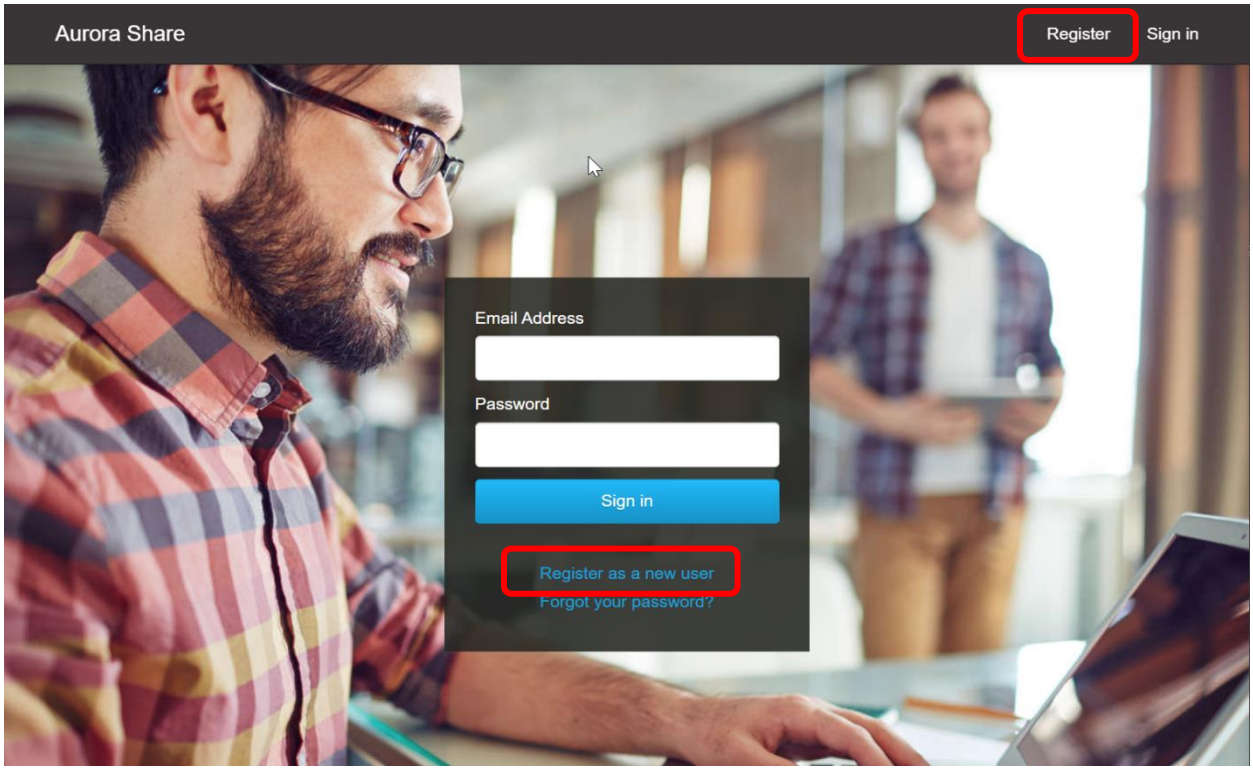
For more details on considerations around file system access for Aurora .Ext refer to section *5 Understanding File Access*.

3.5 Manage Guest Accounts

Guest accounts are users who are typically external to your organization. Since external users do not have an identity of their own within the organization's Active Directory, Aurora manages its own set of identities by which Guest users may identify themselves and authenticate to Aurora.

3.5.1 Create a Guest Account

Guest accounts are created when a Guest self-registers via the Aurora .Ext web application interface:

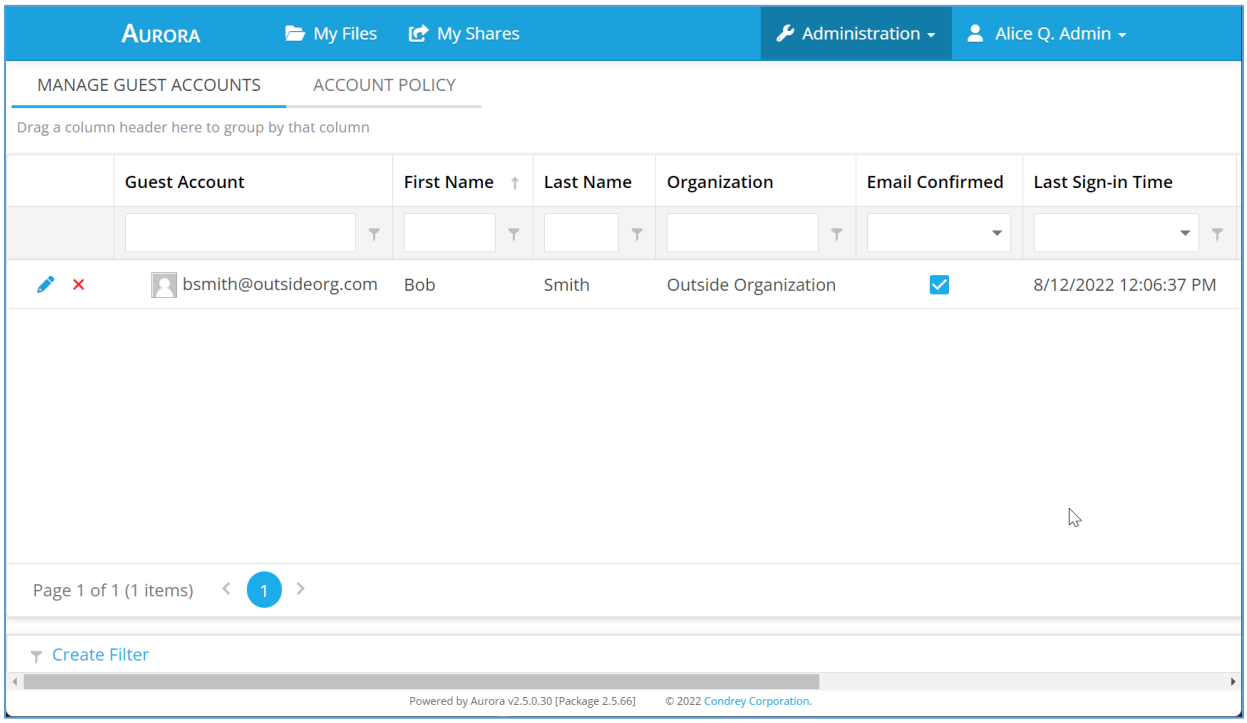


For instructions on completing the self-registration process, see *Aurora .Ext for Guest Users* -> *Registering an Account* in the *Aurora 2.5 User Guide*.

3.5.2 View Guest Accounts

To view the list of current Guest accounts:

1. Sign in to the Aurora web application with a user who is a member of the **Aurora Administrators** group.
2. Click the *Administration* menu, then select *Guest Accounts* from the drop-down list.
3. Select the *Manage Guest Accounts* tab.

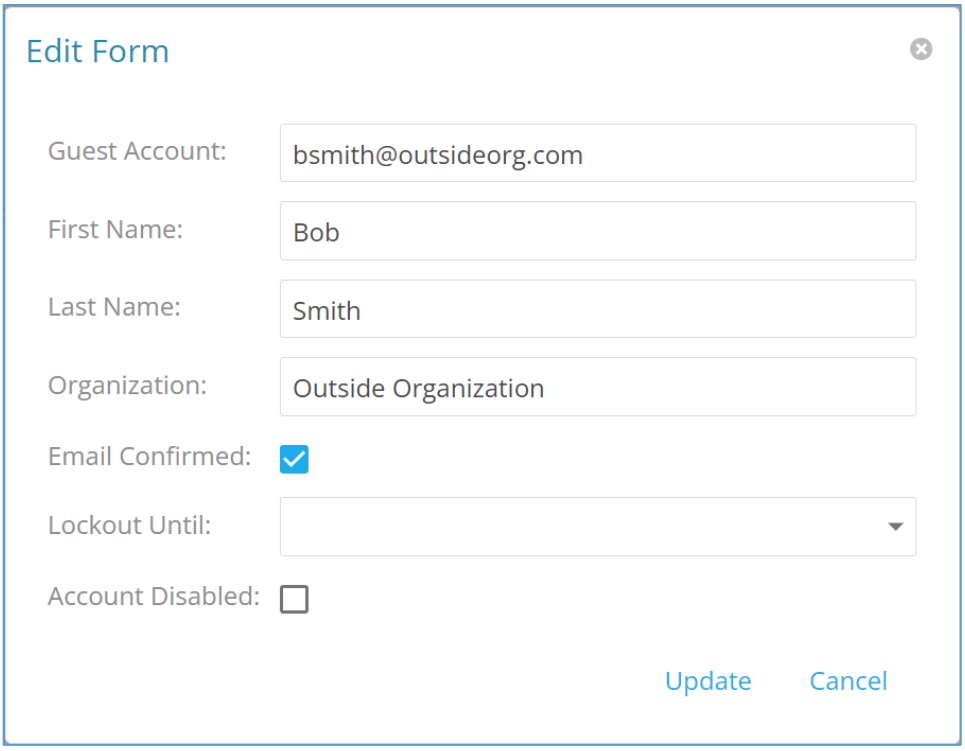


Columns may be sorted, and column headers may be dragged to the top for grouping.

3.5.3 Edit a Guest Account

To edit a Guest account:

1. Click the *Administration* menu, then select *Guest Accounts* from the drop-down list.
2. Select the *Manage Accounts* tab.
3. Click the pencil icon next to the desired Guest account or double-click the row.



The following fields are available for editing in Guest accounts:

- *Guest Account* – change the username (email address) of the account.
- *First Name, Last Name, Organization* – change the name and associated organization of the account.
- *Email Confirmed* – confirm or revoke email confirmation for this account. If revoked, the user will be prompted at the next sign-in to confirm.
- *Account Disabled* – enable or disable the account.
- *Lockout Until* -- set the date and time when the account is active.

Click *Update* to save any changes.

3.5.4 Delete a Guest Account

To delete a Guest account:

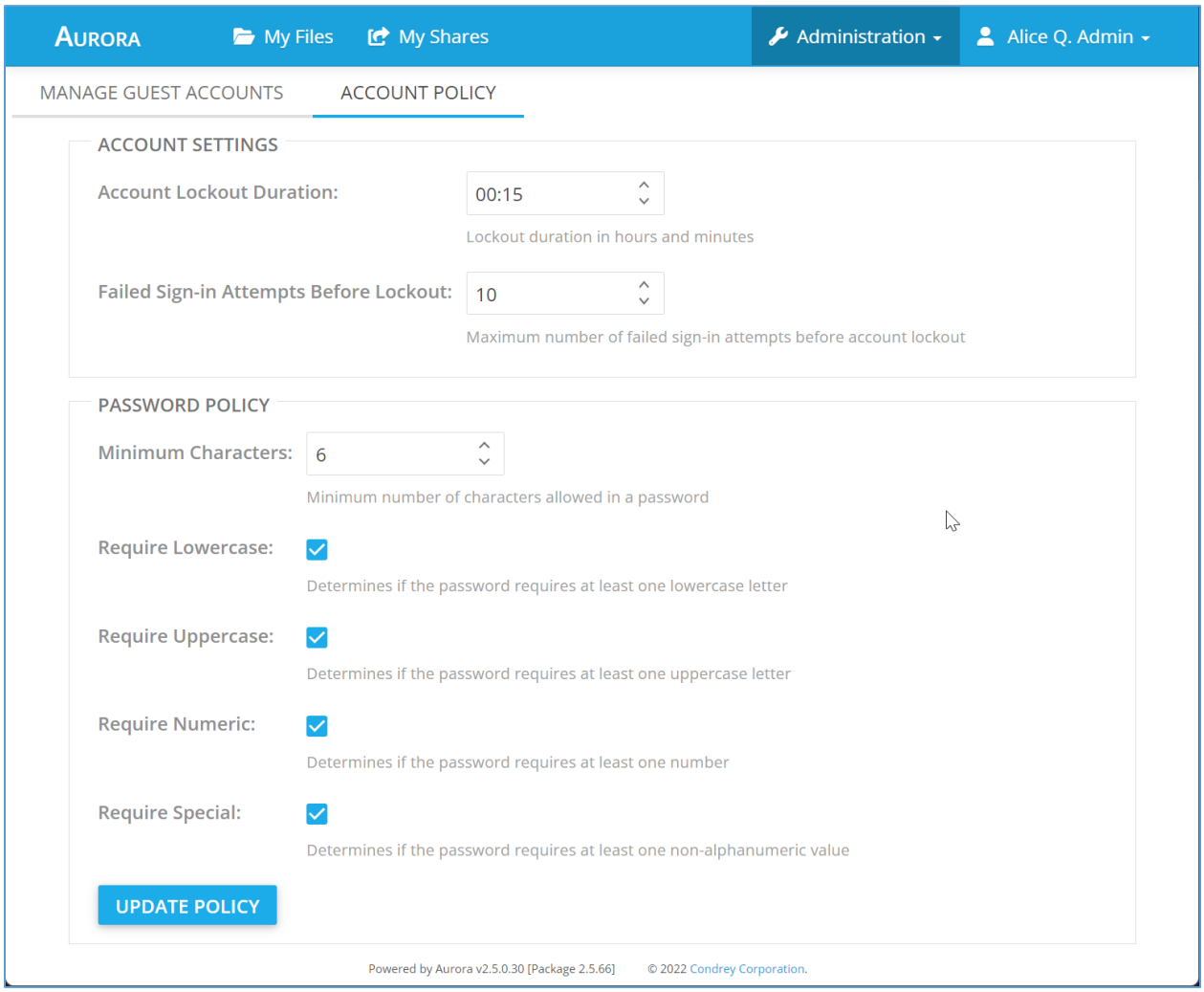
1. Click the *Administration* menu, then select *Guest Accounts* from the drop-down list.
2. Select the *Manage Guest Accounts* tab.
3. Click the delete icon ✖ on the Guest account entry you want to remove.
4. Click *OK* in the confirmation dialog to delete the Guest account.

3.5.5 Modify the Account Policy

Guest accounts are managed by a single account policy. To access the Guest account policy:

1. Click the *Administration* menu, then select *Guest Accounts* from the drop-down list.
2. Select the *Account Policy* tab.

The Account Policy consists of *Account Settings* and the *Password Policy*.



3.5.5.1 Guest Account Settings

The *Guest Account Settings* include:

- *Account Lockout Duration* – the amount of time that a locked-out account stays locked. This value is displayed in hours and minutes.
- *Failed Sign-in Attempts Before Lockout* – number of bad password attempts for a given account before the account is locked out.

Click *Update Policy* to save any changes.

3.5.5.2 Guest Account Password Policy

The *Password Policy* for Guest accounts includes:

- *Minimum Characters* – smallest password length
- *Require Lowercase* –requires passwords to have at least one lowercase character
- *Require Uppercase* –requires passwords to have at least one uppercase character
- *Require Numeric* – requires passwords to have at least one number
- *Require Special* – requires passwords to have at least one non-alphanumeric character

Click *Update Policy* to save any changes.

The password policy changes are enforced the next time a new account is created, or a current account's password is changed.

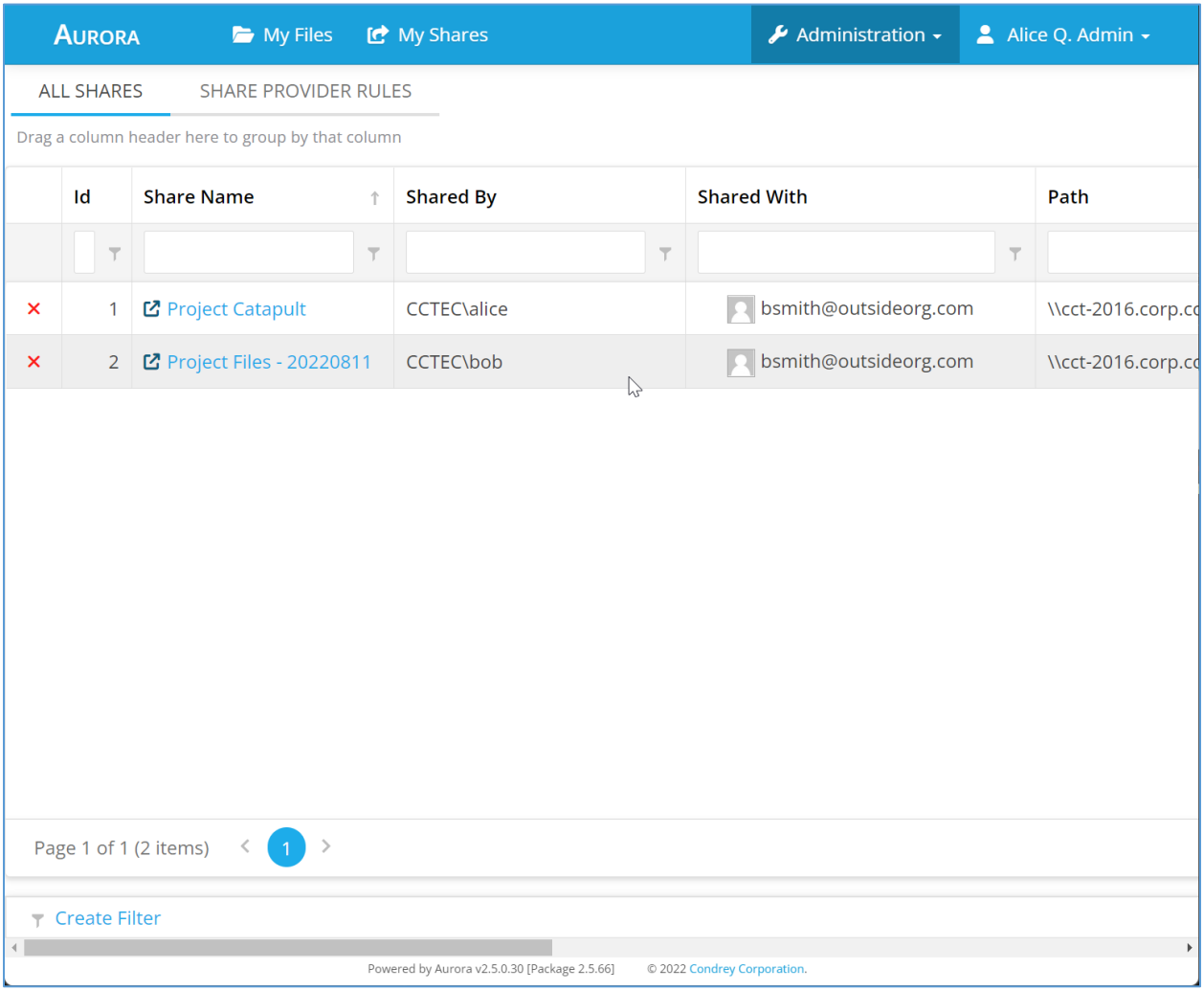
3.6 Manage Guest Shares

An Aurora administrator has access to view and remove existing Guest Shares.

3.6.1 View All Guest Shares

To view the list of all current Guest Shares:

1. Click the *Administration* menu, then select *Shares* from the drop-down list.
2. Select the *All Shares* tab.



Columns may be sorted, and column headers may be dragged to the top for grouping.

3.6.2 Access Share Content

To access the content of an existing share, click the link represented by the Share Name, which opens the share in a limited pop-out window.

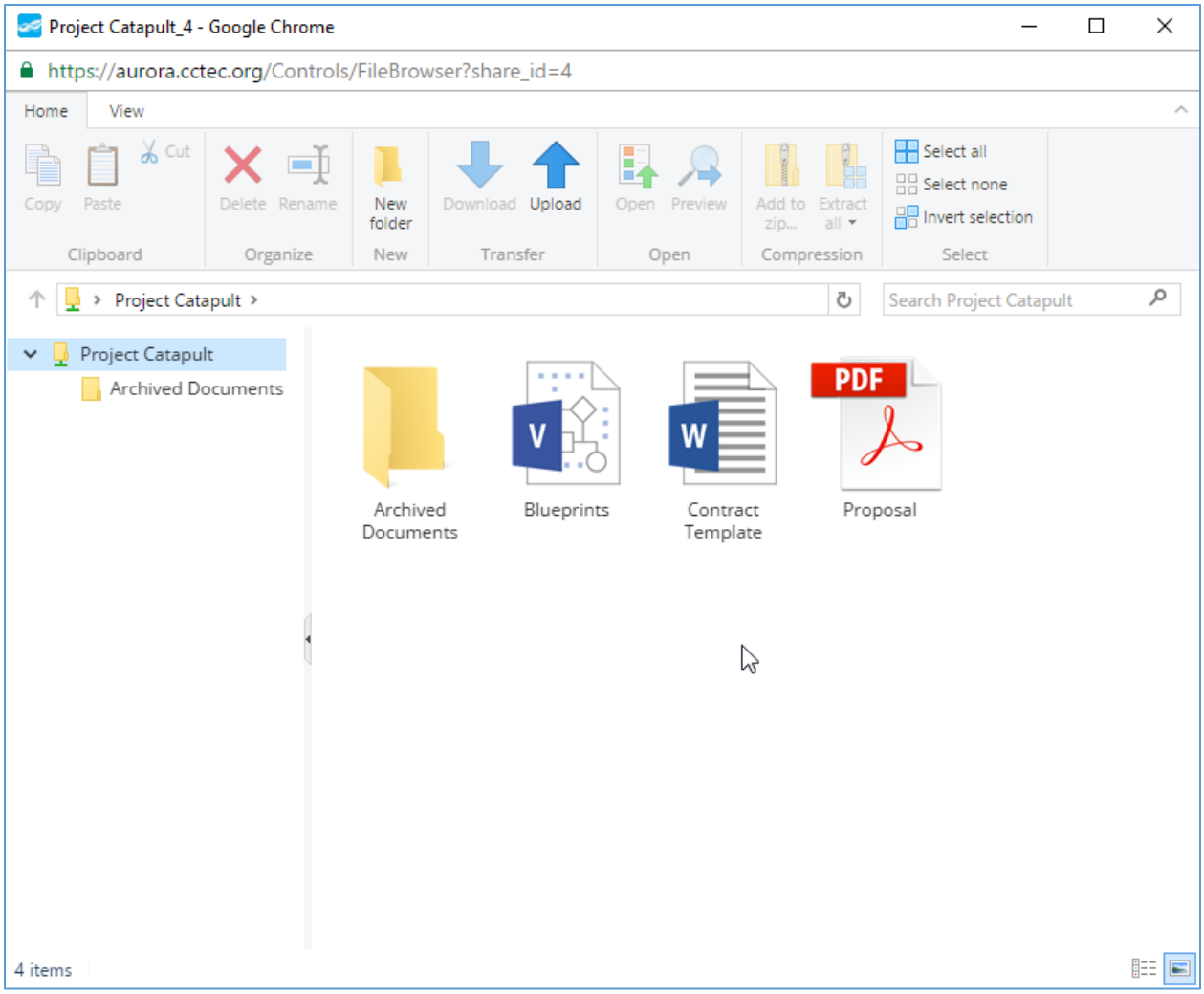


Figure 1 - Pop-out View of a Share

Multiple shares may be accessed simultaneously, enabling the administrator to see the provided content for each.

Note that the rules defined in the Guest Share are not represented in this view.

3.6.3 Delete a Guest Share

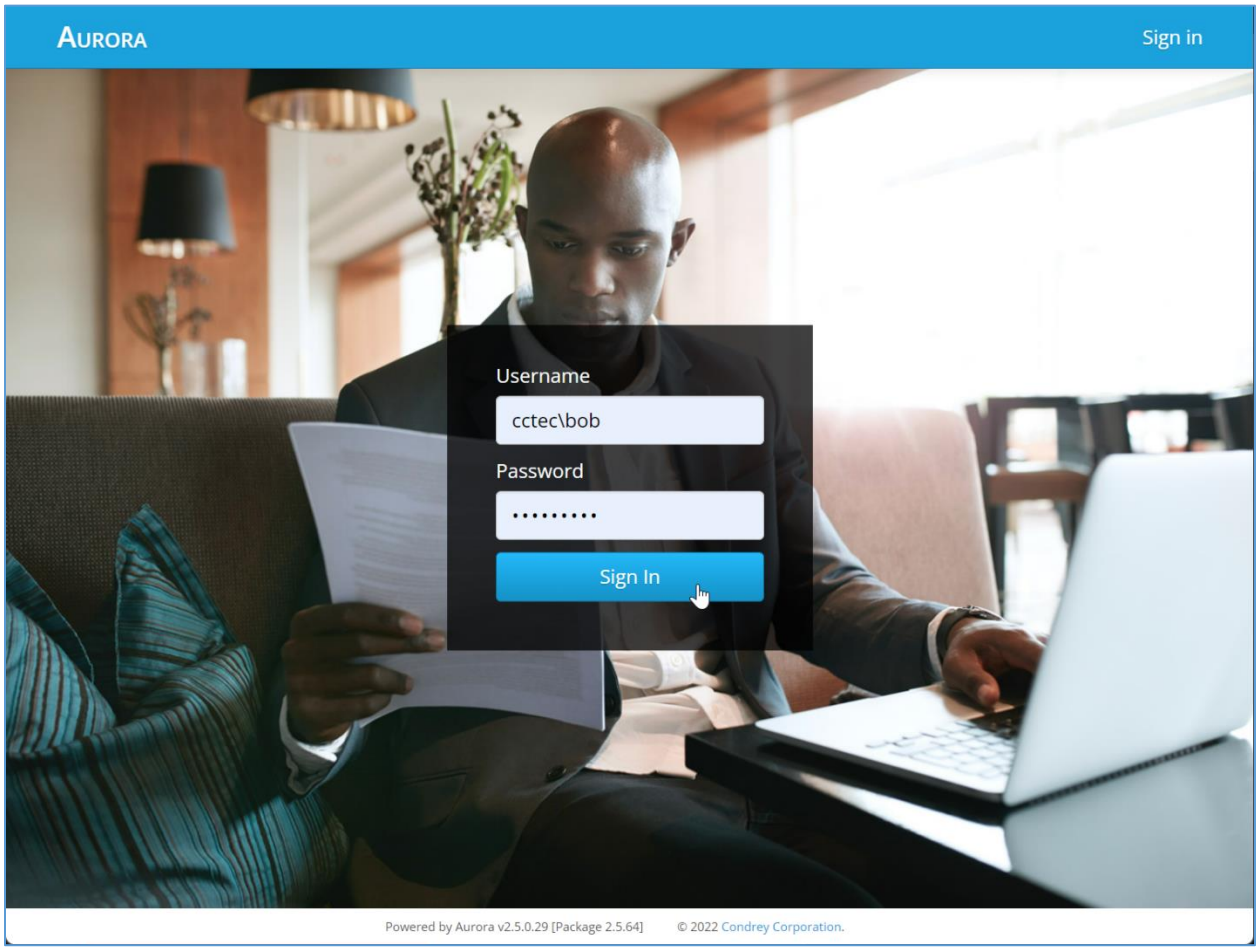
To delete a Guest Share:

1. Click the *Administration* menu, then select *Shares* from the drop-down list.
2. Select the *All Shares* tab.
3. Click the delete icon ✖ on the Guest account entry you want to delete.
4. Click *OK* in the confirmation dialog to delete the Guest account.

4 CONFIGURATION SETTINGS

Both Aurora and Aurora .Ext have several runtime configuration settings that may be accessed from within the Aurora web application itself.

To access the Aurora configuration settings, sign in to Aurora with a user who is a member of the **Aurora Administrators** group. (The Aurora Administrators group is defined using the Web Application section of the Aurora Configuration Dashboard utility.)



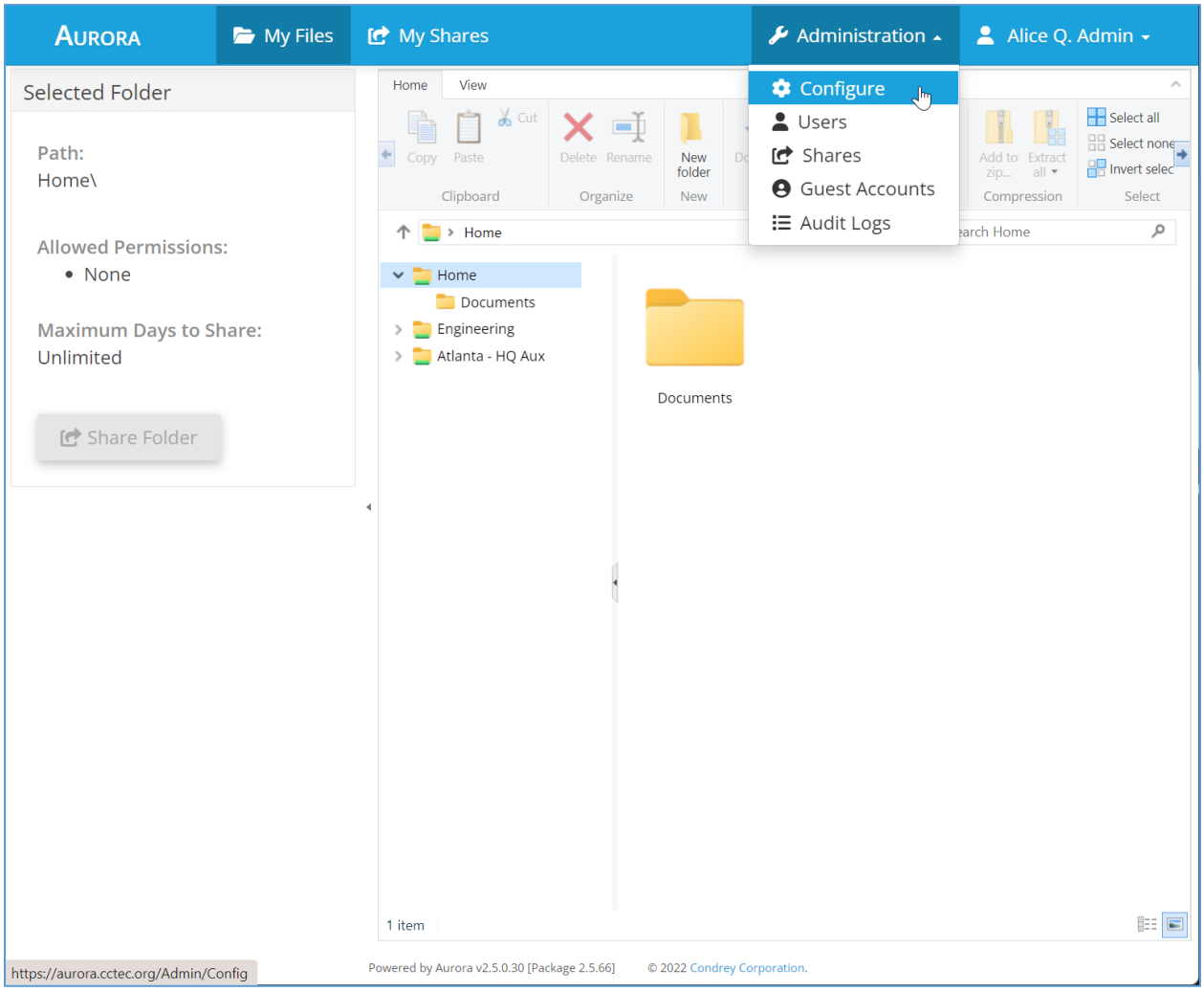
User names may be entered in the following formats:

- Domain\Name CCTEC\ajames
- User Principal Name ajames@cctec.org
- Unqualified ajames (user must be in the same domain as the Aurora server)

4.1 General Configuration

To access the *General* configuration section of Aurora

1. Click the *Administration* menu, then select *Configure* from the drop-down list.



2. Select the *General* tab.

The following options are available:

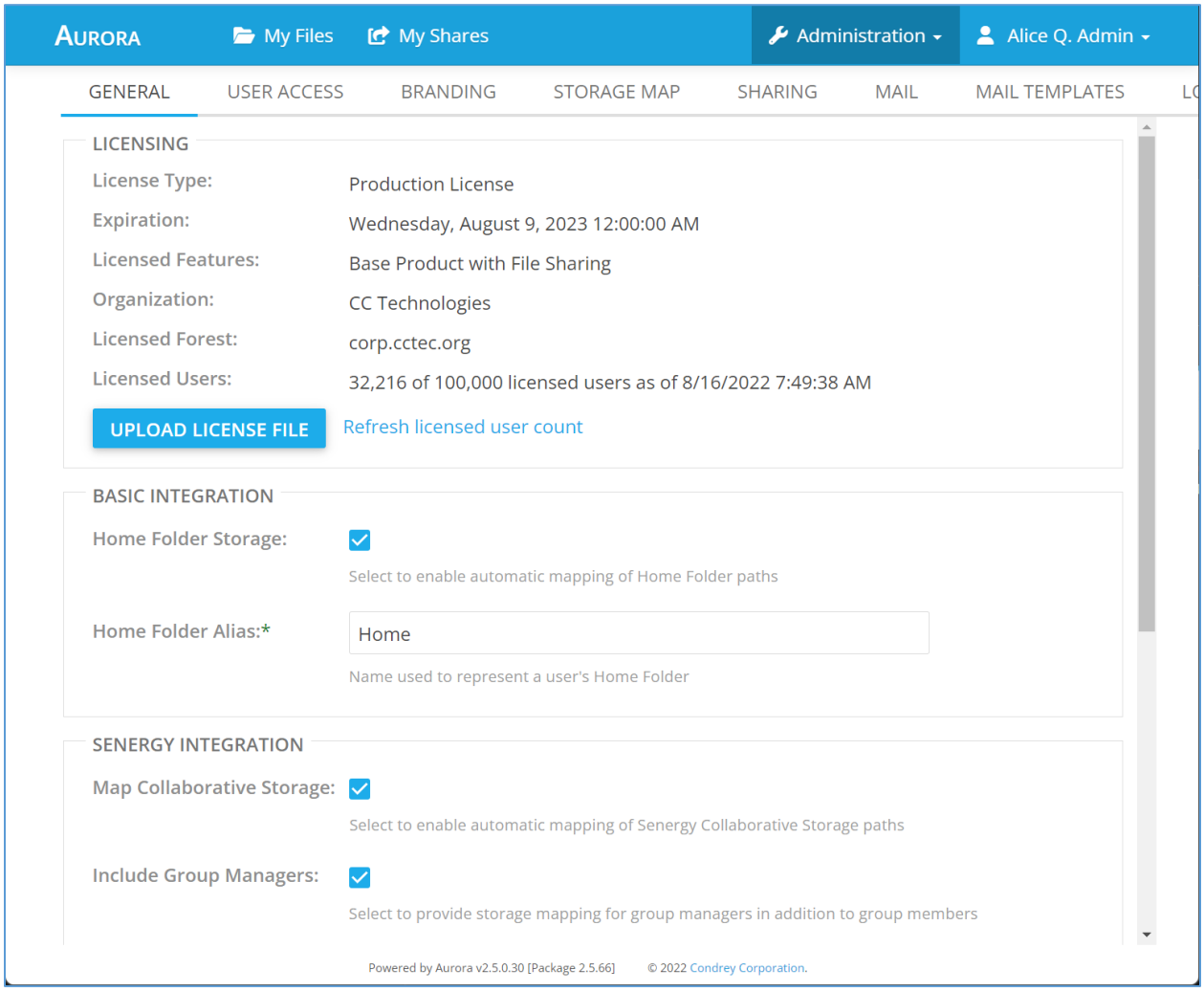


Figure 2 - Aurora Configuration Options

4.1.1 Licensing

This section displays the various aspects of the current license, including:

- License type
- Expiration date
- Licensed user count
- Licensed features list
- Licensed Active Directory forest
- Registered organization

The *Licensed Users* entry displays the number of actively licensed users based on membership in the **Aurora Authorized Users** and **Aurora Administrators** groups. (Users in the **Aurora Excluded Users** group are removed from this tally, unless they are also in the **Aurora Administrators** group.) This membership is checked each time the Aurora Application Pool is restarted, and once each night at 12:00 AM local time.

To update the assigned license, click *Upload License File* then select a new license.

Any errors or issues with the currently assigned license are displayed in this section as well.



When a license is expired or is not valid, the Aurora and Aurora .Ext sites may display the “Site Unavailable” error message. To update the license, either run the **Aurora Configuration Dashboard** utility or access the Aurora *Configuration -> Licensing* section using a web browser to access Aurora on the local server where Aurora is installed.

4.1.2 Basic Integration

The *Home Folder Storage* checkbox determines whether Aurora will automatically include a user’s Home Folder in the list of available storage mappings when that user signs in to Aurora.

Unselecting the *Home Folder Storage* checkbox prevents any automatic inclusion of a **Home Folder** storage entry and disables the special Home Folder rule in the *Provider Rules* from being calculated for sharing rule processing.

The *Home Folder Alias* allows an administrator to specify alternate wording to show the Home Folder storage mapping in the *My Files* page.

Click *Save Settings* to save the parameters.

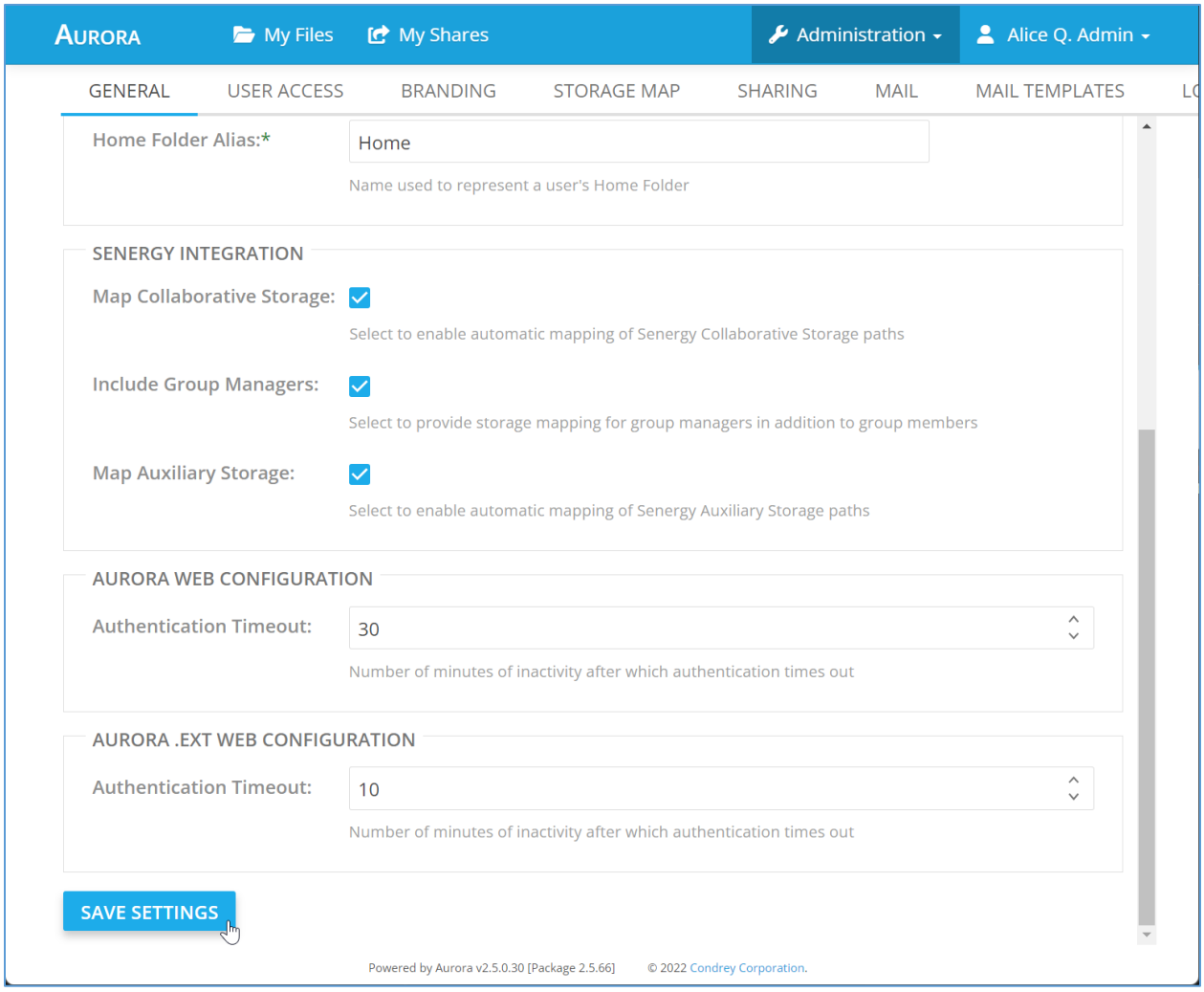


Figure 3 - Aurora Configuration Options, continued

4.1.3 Senergy Integration

Senergy Integration options include automatic storage entry processing for Collaborative and Auxiliary storage.

When *Map Collaborative Storage* is selected, all the user's groups that are managed by *Senergy* and have a corresponding managed path will be displayed as a storage entry in Aurora. In addition, any groups for which the user is a designated *manager* may also be displayed as a storage entry.

When *Map Auxiliary Storage* is selected, all the user's managed Auxiliary paths will be displayed as a storage entry in Aurora.

Click *Save Settings* to save the parameters.

4.1.4 Aurora Web Configuration

Specify the *Authentication Timeout* in minutes for a user's session in the Aurora web application. This specifies the largest interval of inactivity, after which the user must authenticate again.

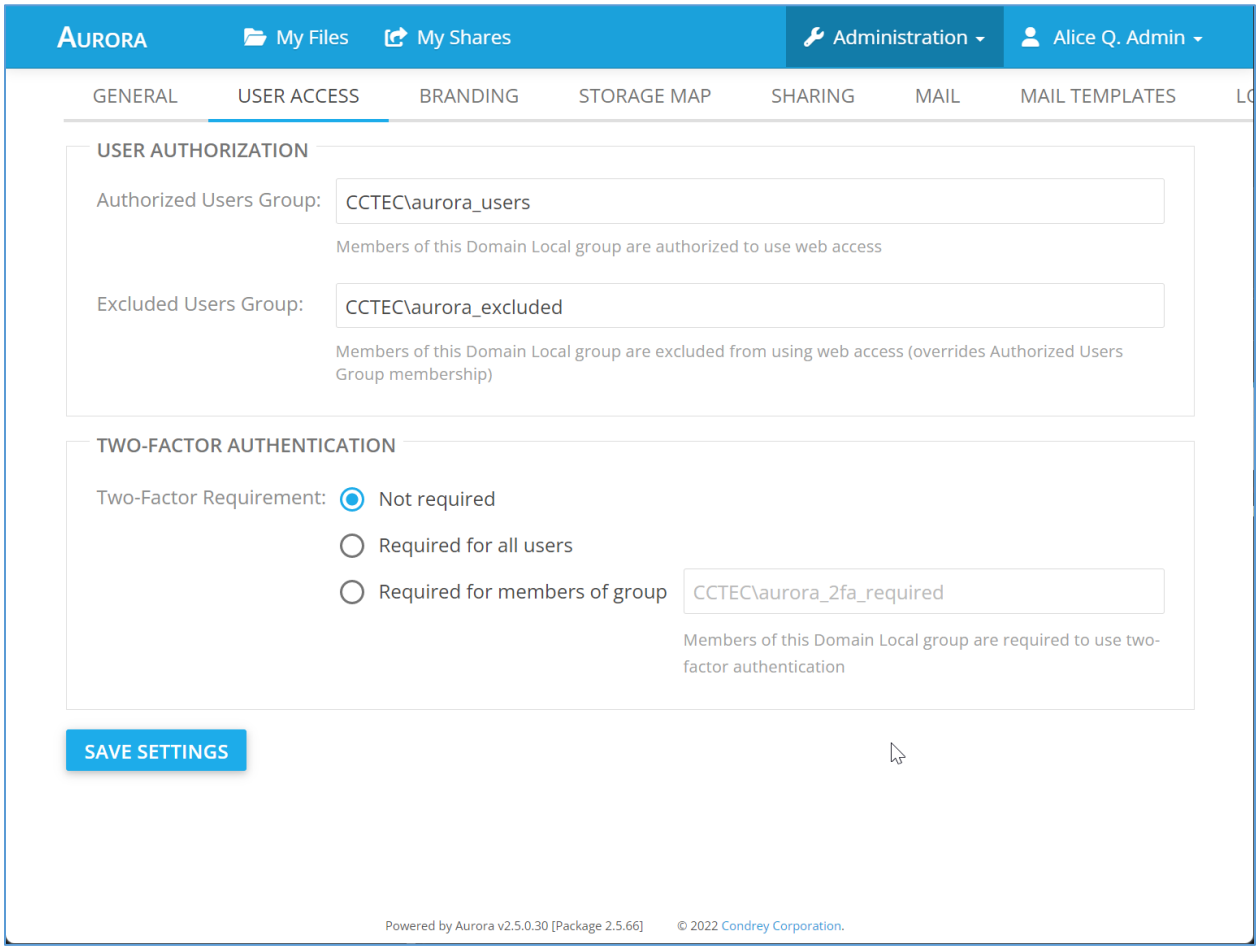
Click *Save Settings* to save the parameters.

4.1.5 Aurora .Ext Web Configuration

Specify the *Authentication Timeout* in minutes for a user's session in the Aurora .Ext web application. This specifies the largest interval of inactivity, after which the user must authenticate again.

Click *Save Settings* to save the parameters.

4.2 User Access



4.2.1 User Authorization

The *User Authorization* section includes the specification for the **Aurora Authorized Users** group and the **Aurora Excluded Users** group.

- Authorized Users Group – specify an Active Directory security group whose members grant access to use Aurora web access
- Excluded Users Group – specify an Active Directory security group whose members are restricted from accessing Aurora web access services. This is an optional group and is especially useful in cases where an all-inclusive group, such as **Domain Users** may have been specified as the **Aurora Users Group**, but certain users should be restricted from Aurora's services.

To save changes to the specified groups, click *Save Settings* at the bottom of the page.

If a group is specified that already exists, it will be validated first before saving the change. If a specified group does not exist, Aurora will create the group as a *Domain Local* group.

Any errors met while processing validation or creation of the specified groups will display an error.

Membership in each of the Authorization, Administrators, Two-Factor Required, and Excluded Users groups may be managed using standard management tools such as the *Active Directory Users and Computers* utility provided with Active Directory.

Nested group membership is always processed for each of the *User Access* groups.

It is strongly recommended to use *Domain Local* security groups for both the **Aurora Authorized Users** and **Aurora Excluded Users** groups. This is especially true for installations in a multi-domain AD forest.

4.2.2 Two-Factor Authentication

The *Two-Factor Authentication* section includes options for two-factor authentication requirements.

Two-factor authentication (2FA) may be:

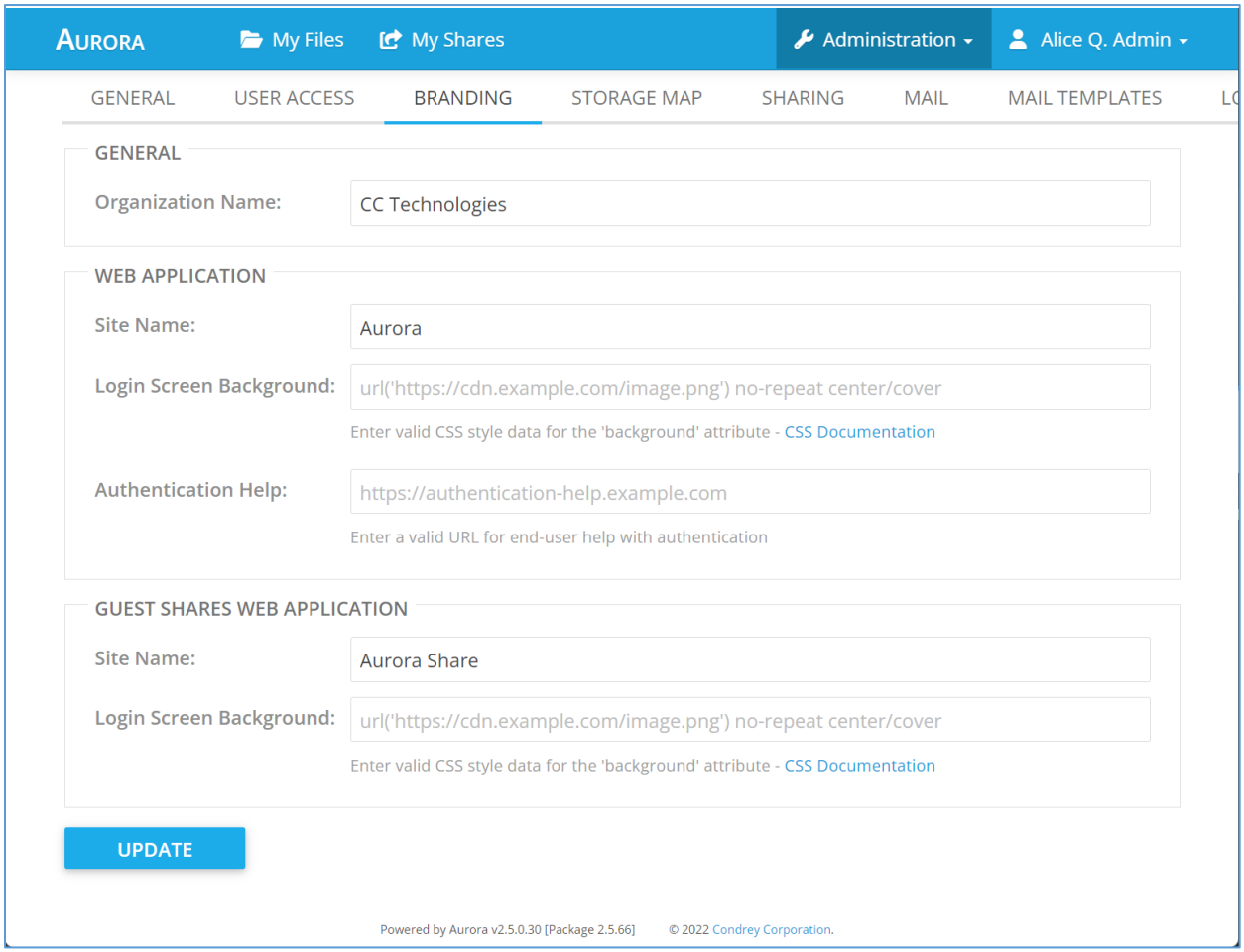
- Not required – configuration of 2FA registration is optional per-user.
- Required for all users – all internal users must register and use two-factor authentication to access Aurora.
- Required for members of group – only the members of the specified group must register and use two-factor authentication. All other users may optionally register for two-factor authentication on a per-user basis.

Users who must use two-factor authentication but have not yet registered will be prompted to do so at the next sign-in before access to Aurora is granted.

4.3 Branding

To access the *Branding* configuration section of Aurora

1. Click the *Administration* menu, then select *Configure* from the drop-down list.
2. Select the *Branding* tab.



The *General* section includes:

- Organization Name – optionally referenced in mail templates

The *Web Application* section includes:

- Site Name – displayed in the main title of the Aurora web application, and optionally referenced in mail templates
- Login Screen Background – specifies an optional CSS value for the *background* CSS style property.
  See https://developer.mozilla.org/en-US/docs/Web/CSS/background for details on this property.
- Authentication Help – specifies an optional URL for help when signing in to Aurora

The *Guest Shares Web Application* section includes:

- Site Name – displayed in the main title of the Aurora .Ext web application, and optionally referenced in mail templates
- Login Screen Background – specifies an optional CSS value for the *background* CSS style property.
  See https://developer.mozilla.org/en-US/docs/Web/CSS/background for details on this property.

Make any changes, then click *Update* to save the changes.

Changes affecting mail template processing take place immediately.

Changes to the Aurora Site Name take effect immediately and are seen in the current session when the current page changes.

Changes to the Aurora .Ext Site name requires a restart of the Aurora .Ext Application Pool to take effect.

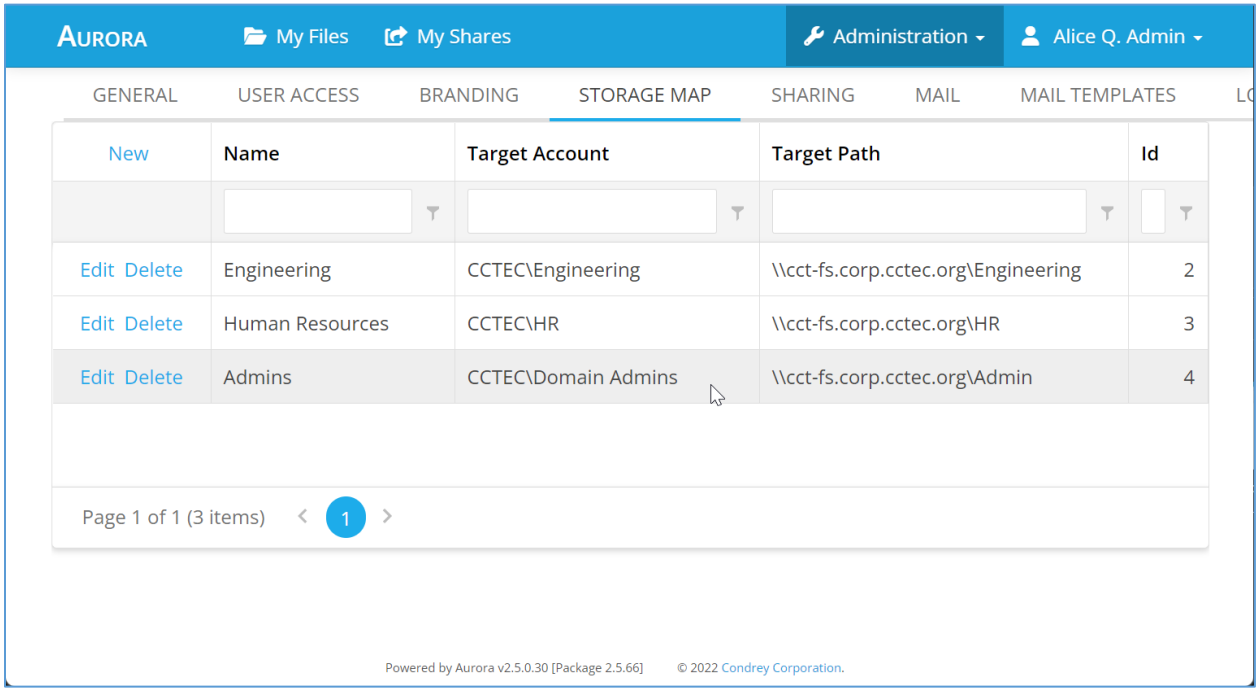
For other branding options including web styles and background images, refer to section *6 Customizing Aurora*.

4.4 Storage Map

To access the *Storage Map* configuration section of Aurora

1. Click the *Administration* menu, then select *Configure* from the drop-down list.
2. Select the *Storage Map* tab.

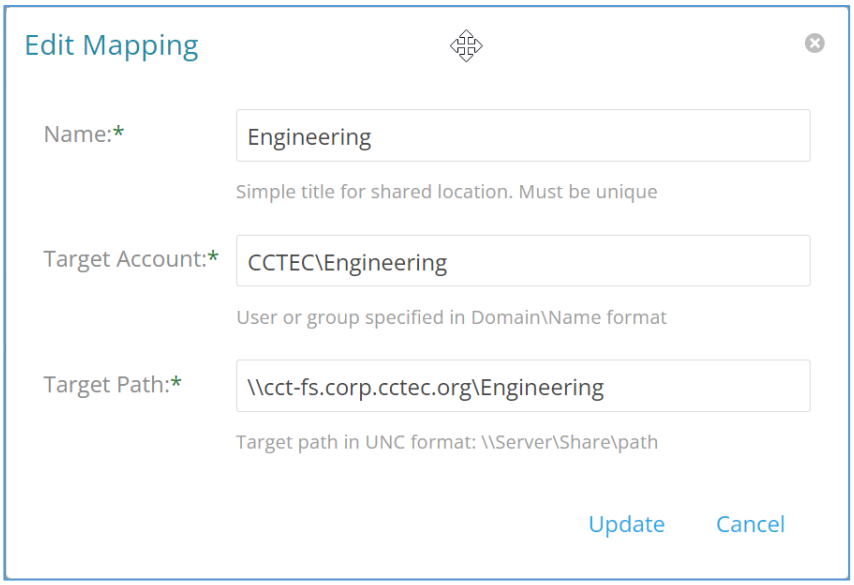
The *Storage Map* includes a list of manually defined storage entries to be displayed when a user signs in to the Aurora web application. These entries are in addition to any automatically mapped entries from Home Folder or Senergy-integrated storage mappings.



4.4.1 Add a Storage Map Entry

To add a new Storage Map entry:

1. Click *New* in the column heading.
2. Specify a *Name.* This name must be unique.
3. Specify a *Target Group* using *Domain\Name* format.
4. Specify a *Target Path* in UNC format.
5. Click *Update* to save the Storage Map entry.



It is recommended that *Target Paths* use the DNS name of servers and not the simple NetBIOS name. Name consistency is important when staging *Provider Rules* for path sharing. Refer to section *3.3.3 Provider Rule Path Name Considerations* for details.

4.4.2 Edit a Storage Map Entry

1. Click *Edit* on an existing Storage Map entry.
2. Modify any of the *Name, Target Group*, or *Target Path* fields.
3. Click *Update* to save the changes.

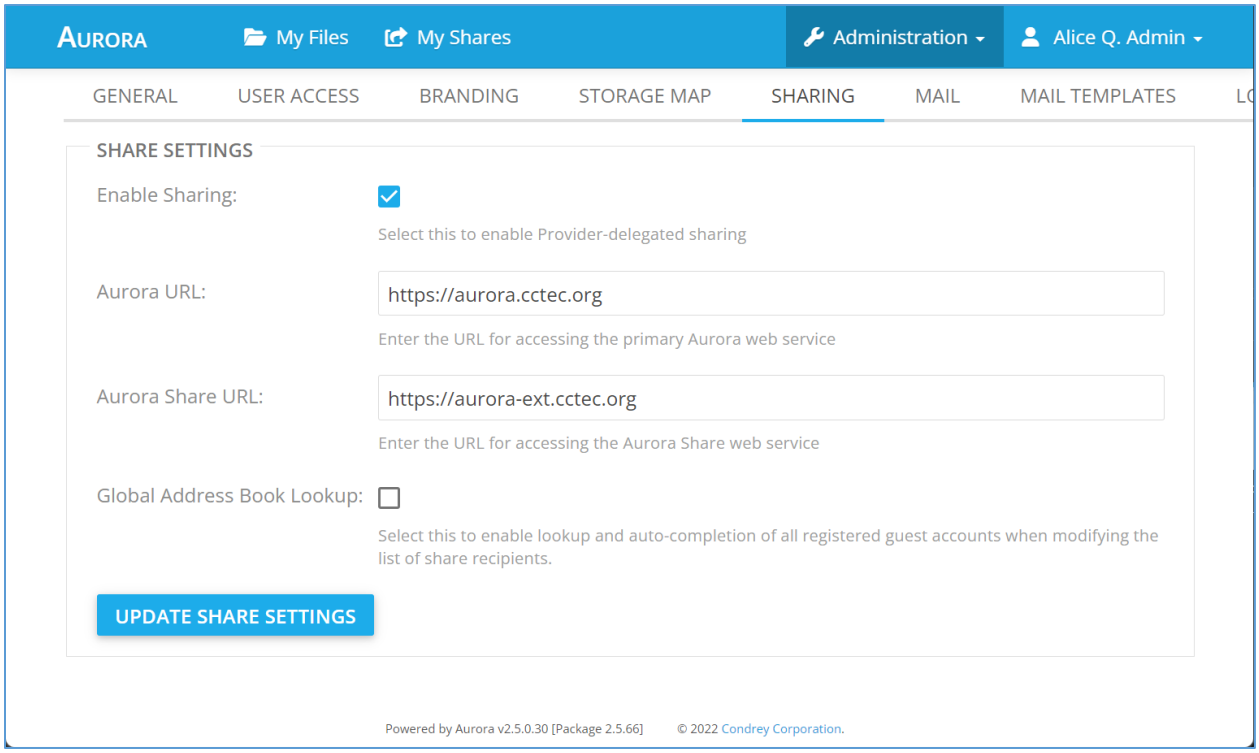
4.4.3 Delete a Storage Map Entry

1. Click *Delete* on an existing Storage Map entry.
2. Click *OK* in the confirmation dialog.

4.4.4 Sharing

To access the *Sharing* configuration section of Aurora

6. Click the *Administration* menu, then select *Configure* from the drop-down list.
7. Select the *Sharing* tab.



The *Share Settings* include:

- *Enable Sharing* – select to enable sharing with Guest Users
- *Aurora Site URL* – specifies the URL used in mail templates for accessing the Aurora web application.
- *Aurora .Ext URL* – specifies the URL used in mail templates for accessing the Aurora .Ext web application
- *Global Address Book Lookup* – when enabled, the list of currently registered guest accounts supplies an auto-complete option when creating shares for target guest users.

The two URLs do not define the address itself but are used as references, primarily in mail templates, for accessing the existing sites. These addresses have default values based on the initial configuration of the Aurora web application but may need to be changed to reflect the actual URLs needed.

Note that in the case of reverse proxy integration, the URLs needed here could be significantly different than what is configured in the IIS website bindings, from which these parameters are initially derived.

Click *Update Share Settings* to save any changes to these parameters.

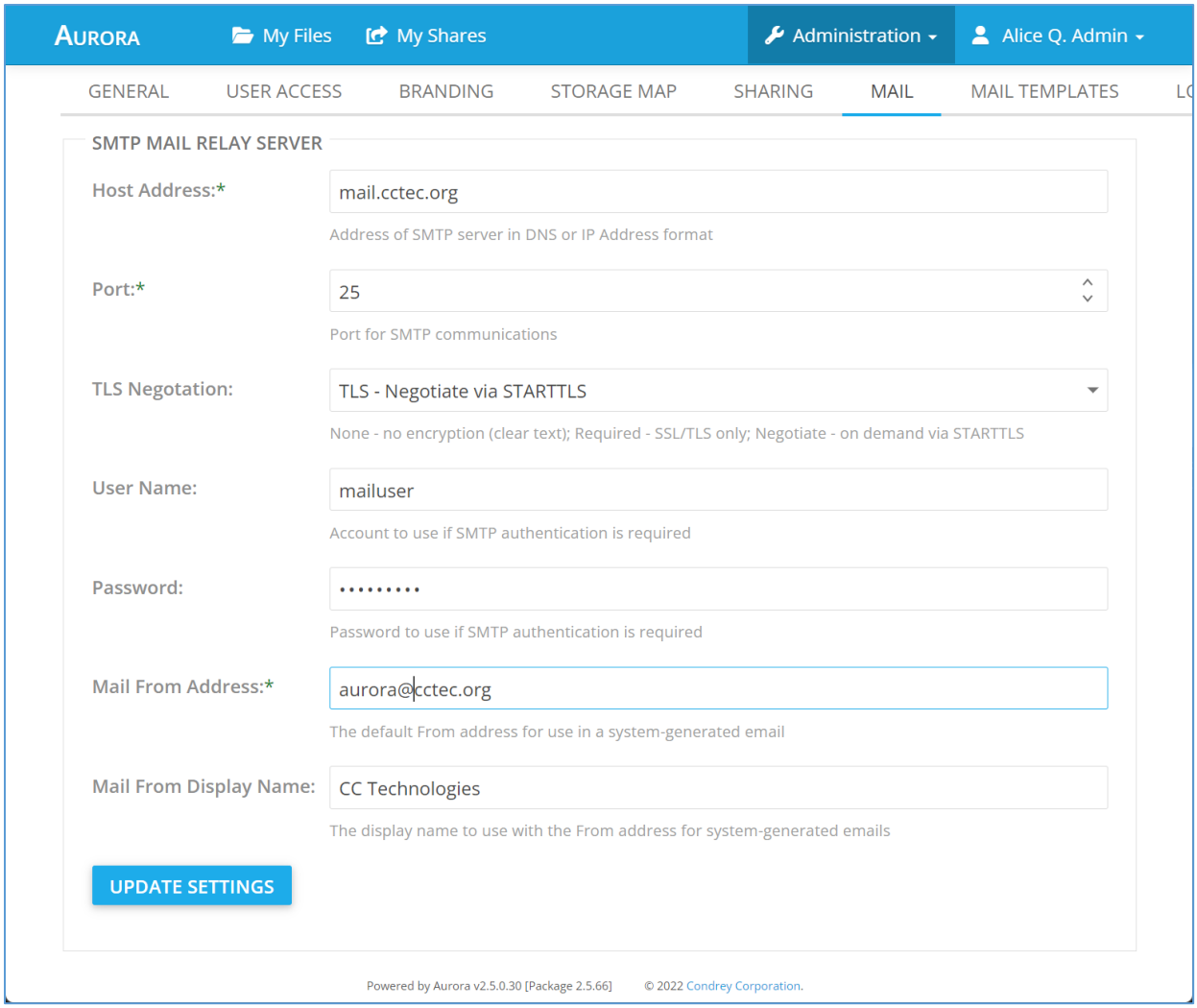


Since some organizations may consider an auto-completion list from all registered guest accounts to be a security or privacy issue, the *Global Address Book Lookup* option is disabled by default.

4.4.5 Mail

To access the *Mail* configuration section of Aurora

1. Click the *Administration* menu, then select *Configure* from the drop-down list.
2. Select the *Mail* tab.



This section is primarily concerned with the integration of an SMTP mail relay service. This service is crucial for communication with Guest users concerning Guest Share notifications and account self-service.

The *SMTP Mail Server* settings include:

- *Host Address* – IP address or DNS name of an SMTP mail relay
- *Port* – port used to access the SMTP mail relay, typically 25 or 587
- *TLS Negotiation*
    - None – clear text communication only
    - TLS Negotiate via STARTTLS – use TLS communication
- *User Name* – the account for use with SMTP authentication; this is optional
- *Password* – the password for use with SMTP authentication; this is needed only if User Name is present
- *Mail From Address* – a required field used as the source address for outgoing mail
- *Mail From Display Name* – display name to use with the source address for outgoing mail

Click *Update Settings* to save any changes made to these parameters.

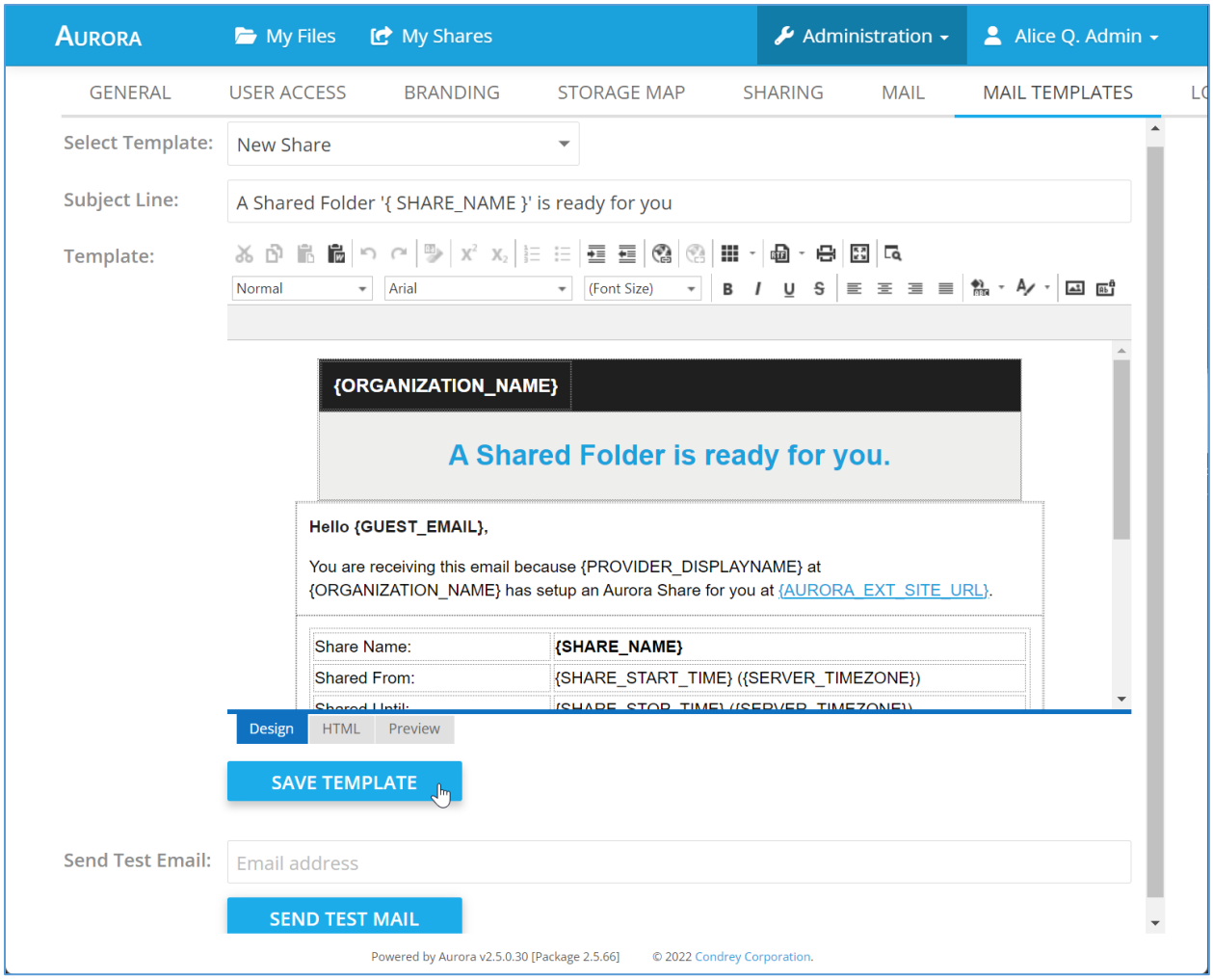


The SMTP configuration parameters can be tested by sending a test email from the *Mail Templates* configuration page.

4.5 Mail Templates

To access the *Mail Templates* configuration section of Aurora

1. Click the *Administration* menu, then select *Configure* from the drop-down list.
2. Select the *Mail Templates* tab.



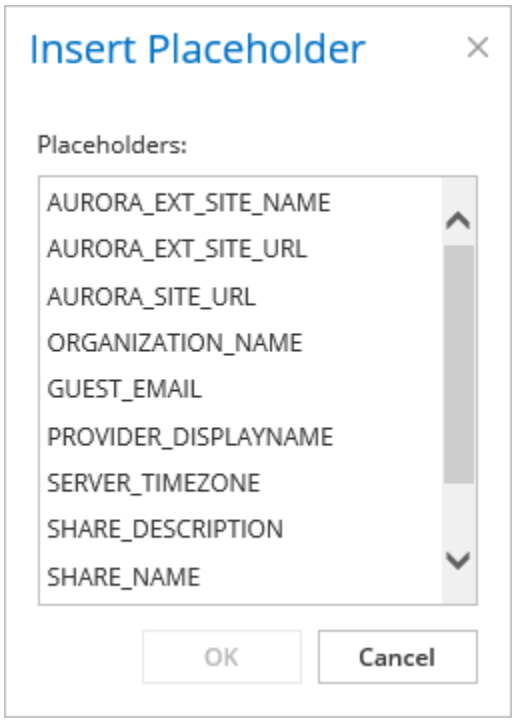
Mail templates exist for both *New Share* and *Updated Share*.

4.5.1 Placeholder Tokens

Both the *Subject Line* and the HTML template itself support *Placeholder Tokens* that are replaced with context-based data.

For the *Subject Line*, insert one of the following Placeholder Token text entries from the table below, being sure to add the required leading and trailing curly brace, each separated by a single white space.

For the HTML template in the *Design* view, click on the placeholder icon in the toolbar and select an entry:



Optionally, click the *HTML* tab and edit the HTML content directly, inserting one of the placeholder tags below

.

Placeholder Tokens must be surrounded by a leading brace **{** and trailing brace **}**, each separated by a single white space.

For example, to use the token **SHARE_NAME** it should be written as **{ SHARE_NAME }**. Selecting a token from the *Design* view with the token selector will automatically add the necessary braces and spacing, but manually typing the token into the Subject Line or via the *HTML* text view requires careful attention to the exact spacing.

Table 1 - Mail Placeholder Tokens

Tag	Replacement Text
AURORA_EXT_SITE_NAME	Name of the Aurora .Ext site as configured in *Branding -> Aurora .Ext Site Name*
AURORA_EXT_SITE_URL	Name of the Aurora site as configured in *Branding -> Aurora Site Name*
AURORA_SITE_URL	The Aurora site URL as configured in *Sharing -> Aurora Site URL*
ORGANIZATION_NAME	The organization name as configured in *Branding -> Organization Name*
GUEST_EMAIL	The Guest User's email address
PROVIDER_DISPLAYNAME	The *displayName* attribute of an Aurora Internal User as found in Active Directory. This is typically the user's name in First Last format.
SERVER_TIMEZONE	The name of the Aurora server's local time zone, such as **Eastern Daylight Time**
SHARE_DESCRIPTION	The *Description* text found in a configured Guest Share
SHARE_NAME	The share name found in a configured Guest Share
SHARE_START_TIME	The start-of-share time for a configured Guest Share, displayed in the Aurora server's local time zone and locality, such as **5/14/2016 7:25:00 AM**
SHARE_STOP_TIME	The expiration time for a configured Guest Share, displayed in the Aurora server's local time zone and locality, such as **5/24/2016 10:00:00 PM**

4.5.2 Saving a Template

To save changes made to a mail template, click on *Save Template*.

Selecting a different template from the *Select Template* drop-down list will load that template and discard any current changes. Please be sure to save your work first, before selecting a different template, or navigating to a different page.

4.5.3 Testing a Template

To test changes to a mail template:

1. Save any changes first by clicking *Save Template.*
2. Enter a valid email address that will receive the test mail.
3. Click *Send Test Mail*

Note that the settings in the *Mail* configuration section must be correct for this test to complete successfully.

Check the email account where the test email was sent and verify that the contents appear OK.



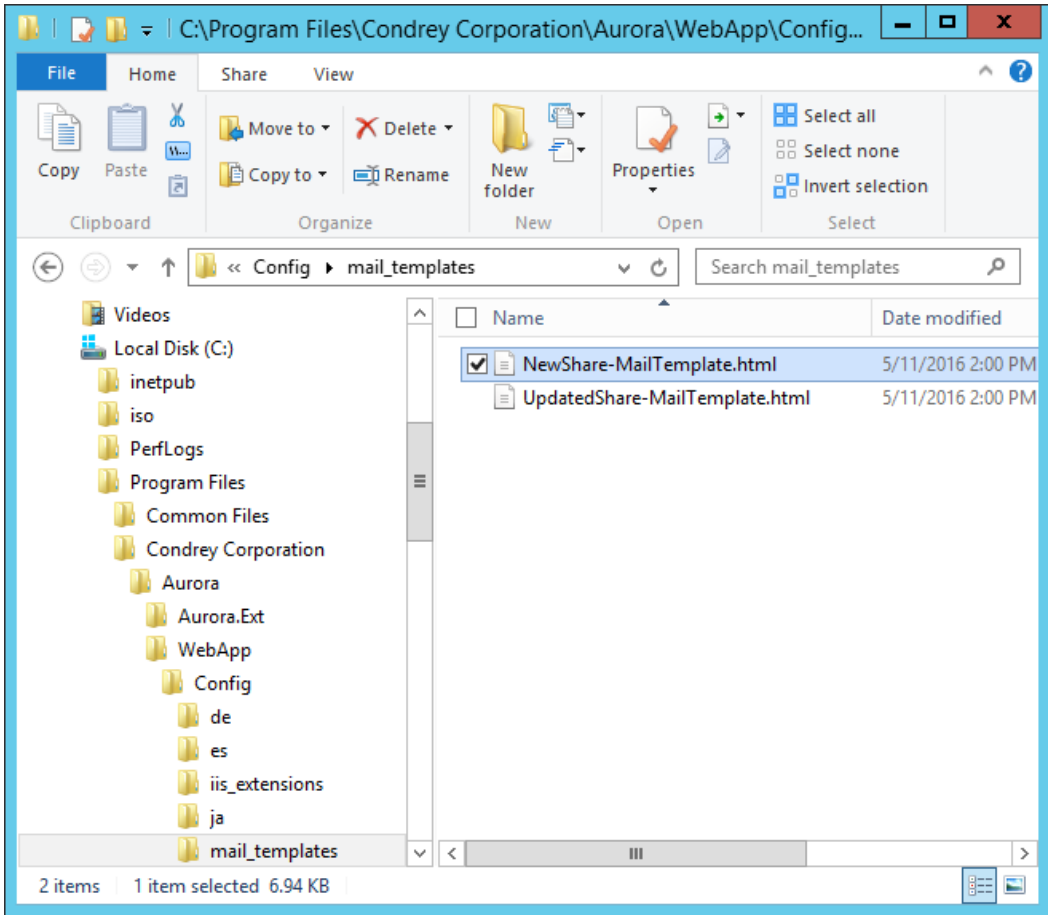
HTML email is notoriously difficult to get right. Many email clients and web services strip CSS classes and tags, and images are often refactored inconsistently across various mail clients. Some basic tips include:

- Only use inline styles, as CSS stylesheets are often removed
- Keep styles simple as newer CSS standards may be ignored
- Use tables instead of tags or CSS stylings for layout
- Keep the width to about 600 – 650 pixels wide maximum
- Keep any graphics to a minimum and be prepared to perform adequate testing across multiple email clients and web services.
- Always test with as many target email systems and clients as possible

4.5.4 Recovering the Default Templates

To recover the default HTML content for the *New Share* or *Updated Share* mail template:

1. Navigate to the Aurora *Configure -> Mail Templates* page.
2. Select the desired template to restore.
3. Select the *HTML* view tab at the bottom of the *Template* section.
4. Click in the HTML editor, select all text (Ctrl-A) then delete it (Delete key).
5. Using Windows Explorer, navigate to the Aurora mail templates folder found at `%PROGRAMFILES%\Condrey Corporation\Aurora\WebApp\Config\mail_templates` typically found as `C:\ProgramFiles\Condrey Corporation\Aurora\WebApp\Config\mail_templates`

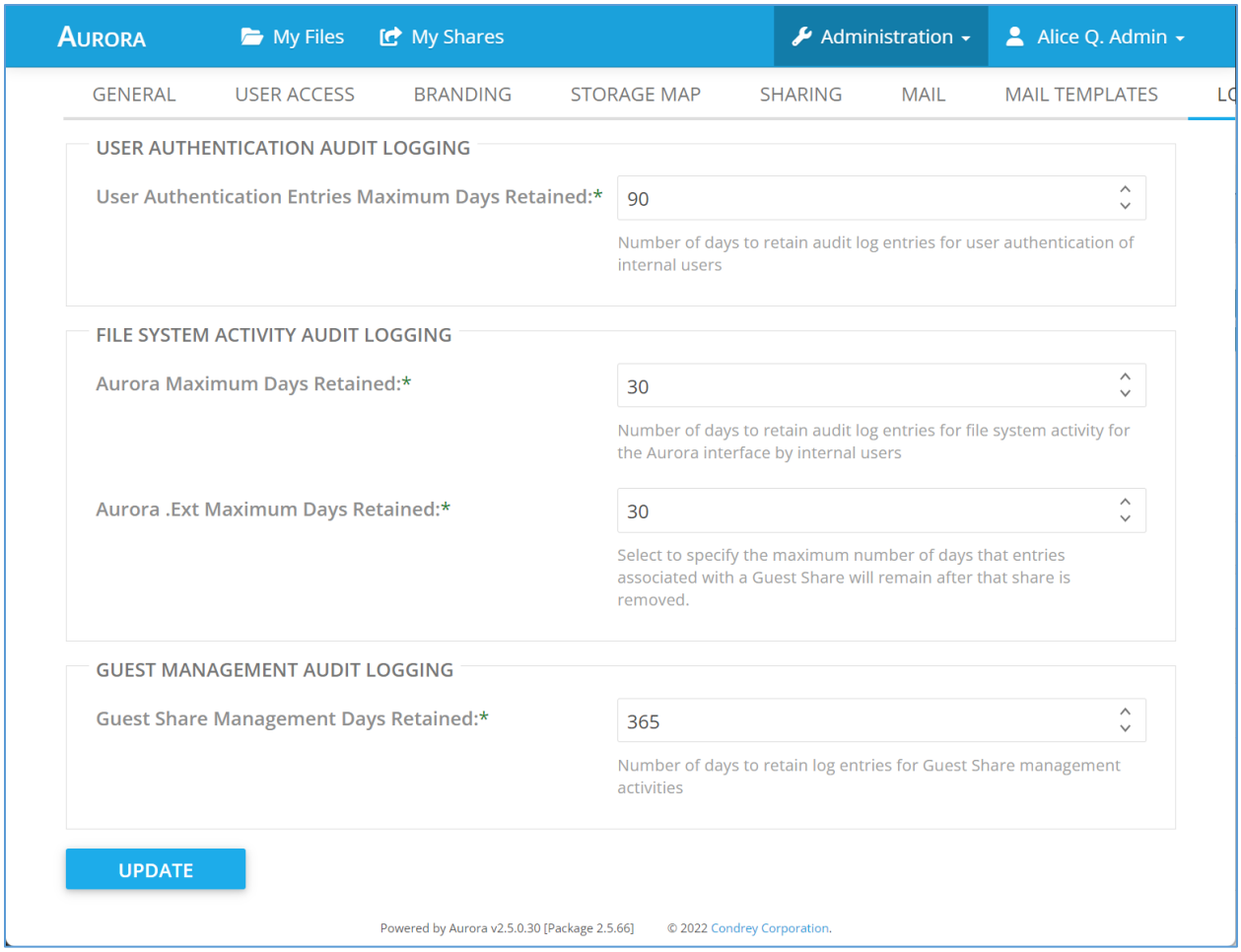


6. Open the HTML text for the desired template in a text editor, such as Notepad.exe.
7. Copy the contents of the HTML text from the text editor, then paste them into the *HTML* view of the current template on the Aurora *Mail Templates* page.
8. Click *Save Template* to save the updated contents.

4.6 Logging

To access the *Logging* configuration section of Aurora

1. Click the *Administration* menu, then select *Configure* from the drop-down list.
2. Select the *Logging* tab.



Audit Logging options include:

- *User Authentication Entries Maximum Days Retained* – number of days to keep entries in the user authentication audit log for Internal Users.
- *Aurora Maximum Days Retained* – number of days to keep entries for the File System activity audit log generated by Internal Users' access
- *Aurora .Ext Maximum Days Retained* – number of days to keep entries for the File System activity audit log generated by Guest Shares access after the share is deleted
- *Guest Share Management Days Retained* – number of days to keep log entries corresponding to changes in Guest Share management actions

Click *Update* to save any changes.

Note that the File System Audit Log typically consumes the most database space. For a capacity planning reference for this table, refer to *Deployment Planning* -> *SQL Server Database* -> *Capacity Planning* in the *Aurora 2.5 Installation and Deployment Guide*.

Note that File System audit log entries for Guest Share access are kept for at least the lifetime of the share.

5 UNDERSTANDING FILE ACCESS

5.1 File Access for Internal Users via Aurora

For Internal Users accessing Aurora, all file system access is performed using the user's credentials.

By making use of the user's credentials instead of a proxy account, all access to files and folders in through Aurora is limited to any share or NTFS file system permissions defined in the file system itself.

This access includes cases where Access Based Enumeration is defined, giving a similar experience for accessing the user's files whether from the desktop or the web interface provided by Aurora.

5.2 File Access for Guest Users via Aurora .Ext

File access for Guest Users is a combination of two separate security layers:

- Share permissions managed by Aurora at the web application level applied to the Guest account
- File system permissions managed at the operating system level applied to the proxy account

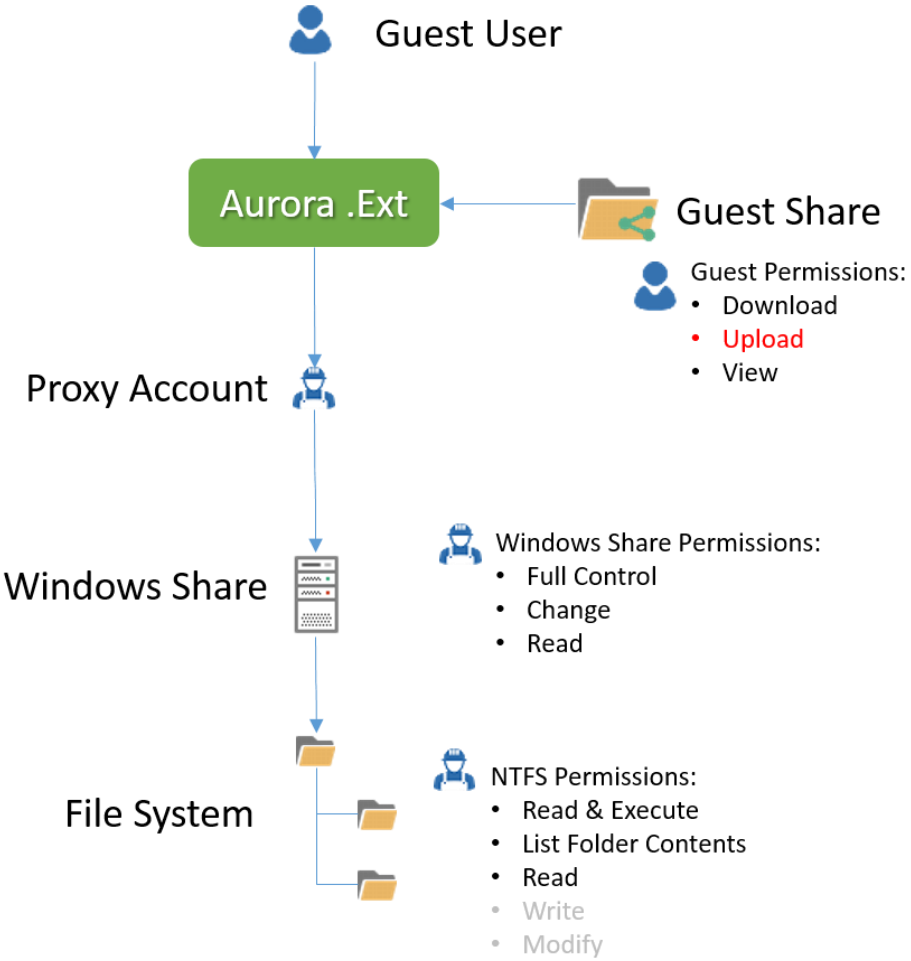
A consequence of having two layers of security is that permissions in both layers must allow an operation, such as Read or Write to take place, or the action is denied.



One common cause for receiving an Access Denied error in the file management interface of Aurora .Ext is that the Share Permissions are granting access to an operation that the underlying proxy account may not have access to at the Windows share or NTFS file system level.

To address this error, either grant the necessary permissions to the proxy rights group in the file system or Windows share or restrict the Provider Rules so that the Internal User creating the Guest Share cannot allow that privilege in the first place.

Consider the following scenario where a Guest has been granted a share from Aurora giving him Download, Upload and View permissions at the Guest Share level:



Download and View are essentially Read permissions at the Windows share and file system level, so they will work as expected since the proxy account has that permission as well.

Upload, however, which is the same as Write or Modify at the NTFS level, will fail, since the proxy account does not have the corresponding rights in the file system.

5.2.1 Share Permissions and the Guest Account

When a Provider sets up a Guest Share for a particular Guest, he assigns a set of share permissions to that share for that Guest. These permissions are defined at the Aurora application level and are persisted in the Guest Share record in the database.

Regardless of other permissions that the underlying proxy account may have, the Share Permissions defined in the Guest Shares themselves are the final defense in the security layers for what the Guest may be allowed to do.

As an administrator, it is important to set proper limits in the Provider Rules so that Providers are not able to assign more permissions than necessary to Guest Users.

5.2.2 File System Permissions and the Proxy Account

Since Guest Users are defined only with Aurora, a proxy account is used to gain access at the file system level.

By default, a user named **auroraext_proxy** is created, along with a security group named **auroraext_proxyrights** by default, into which the proxy user is added as a member. As part of best practices, consider the following:

- Only assign permissions to the auroraext_proxyrights group, and not the proxy user itself.
- The auroraext_proxyrights group must be assigned share and file system permissions to every Windows share and file system where Aurora sharing will take place.
- Do not assign any more rights than necessary to a given Windows share or file system, that you as an administrator feel comfortable allowing an external entity to have.

Remember that simply giving rights to the proxy rights group does not mean that Guest Users will necessarily have that level of access – Internal Users acting as Providers must share a folder with those permissions, and that Internal User must also be allowed to grant those rights to the specified path in the first place.

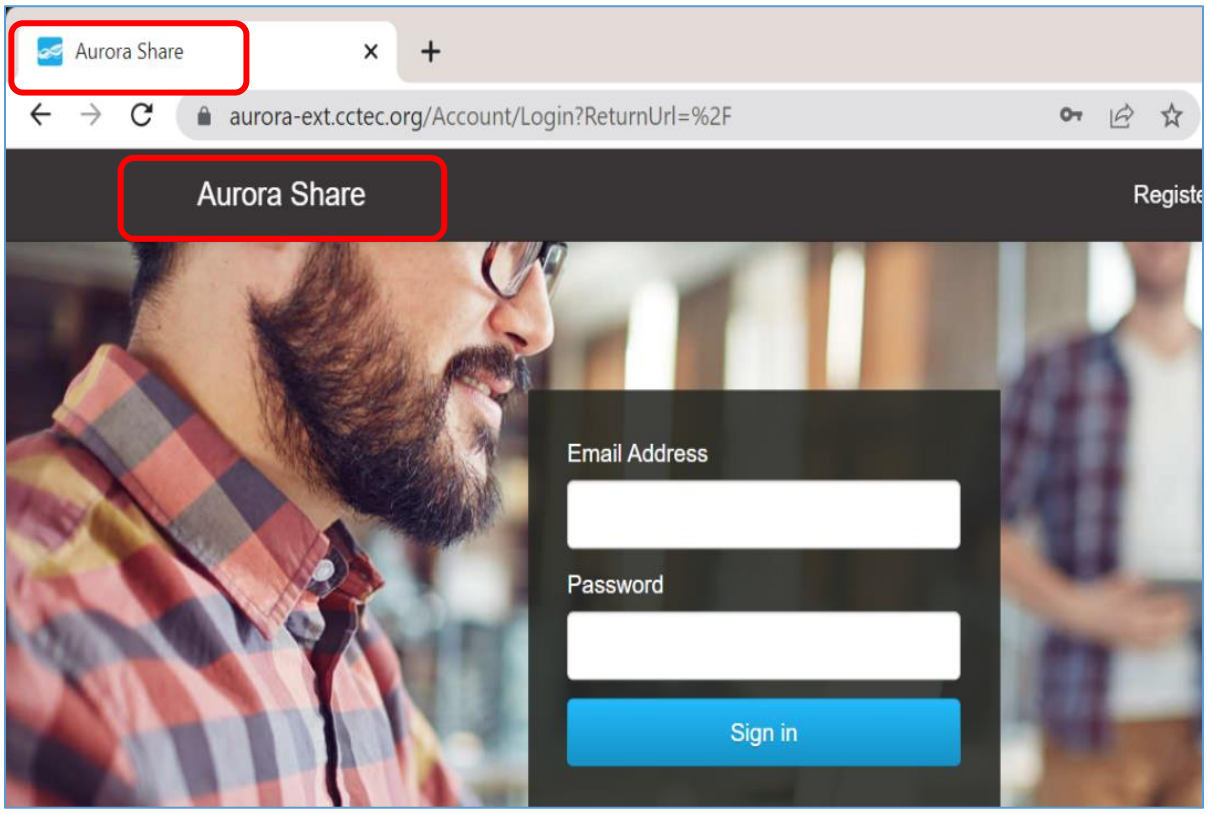
6 CUSTOMIZING AURORA

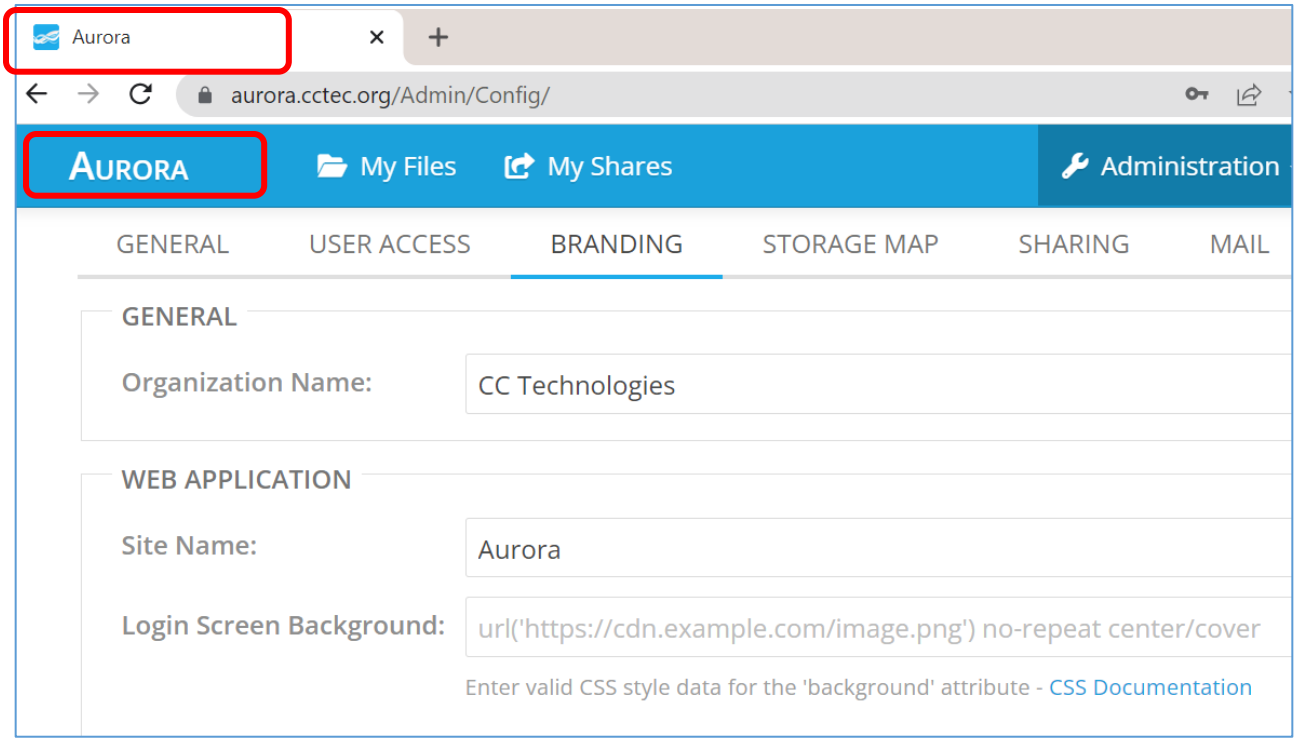
Aurora and Aurora .Ext may be optionally branded. Branding options include:

- Custom site title or name
- Custom email templates for Guest Share notification
- Customization of the sign-in page background
- Customization of other web elements

6.1 Site Names and Titles

The site name and title for both Aurora and Aurora .Ext can be changed via the *Configuration Settings* in the Aurora web application.





To change the site names and titles:

1. Sign in to the Aurora web application as an Aurora administrator.
2. Click the *Administration* menu, then select *Configure* from the drop-down list.
3. Select the *Branding* tab.
4. Update the corresponding Web Application *Site Name* and Guest Shares Web Application *Site Name* fields.

6.2 Customized Mail Templates

Aurora currently supports customized mail templates for outbound emails of new and updated Guest Shares.

For information on how to access and modify these templates, refer to section *4.5 Mail Templates*.

6.3 Sign-in Page Customization

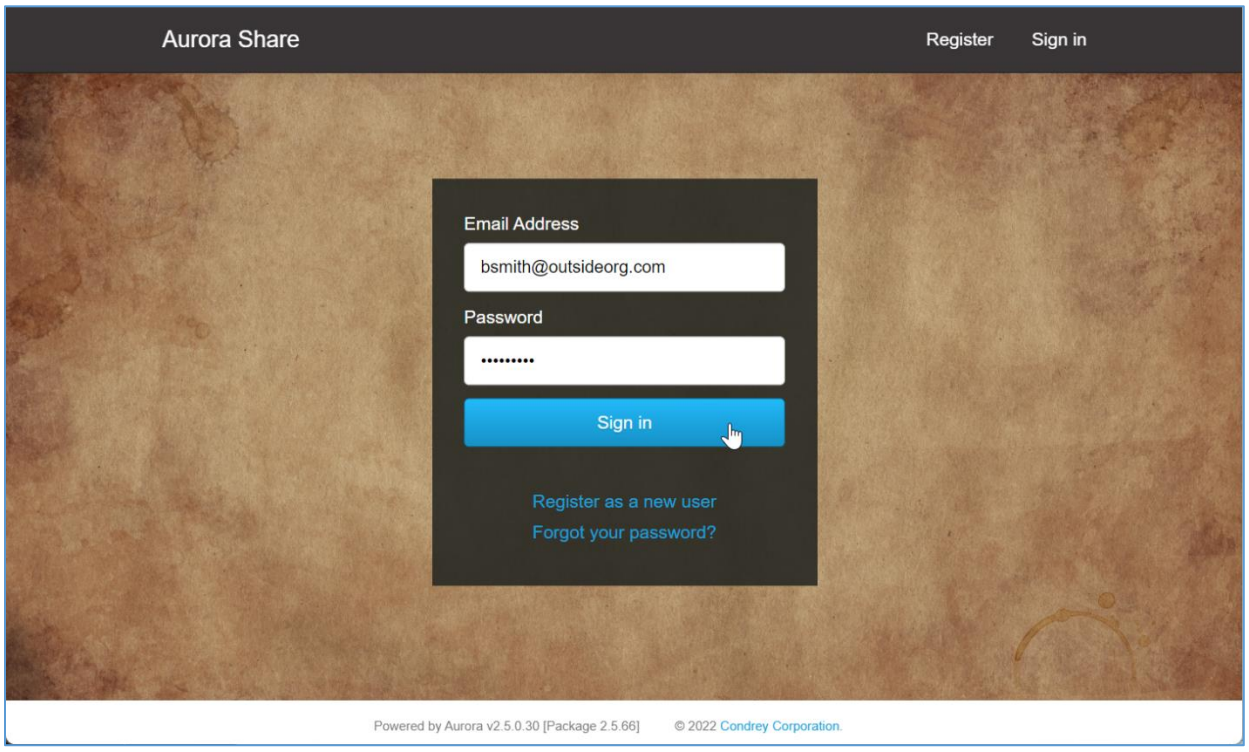
6.3.1 Customizing the Background

Update the *Login Screen Background* fields for a customized background for both the Web Application (Aurora) and Guest Shares Web Application (Aurora .Ext).

The sign-in page background may be customized using standard Cascading Style Sheet (CSS) values for the *background* CSS property.

For example, using an image copied into the Aurora .Ext application *Content\images* folder, you could use enter the following value into the Guest Shares Web Application *Login Screen Background* field:

```
url('/Content/images/login-background-2.jpg') no-repeat center/cover
```



Example of custom sign-in screen background graphic

The background property can be any valid value including

- Supported colors such as ‘red’ or #FF0000
- URL image references
- Gradients and other advanced patterns

For details on the *background* CSS property see:

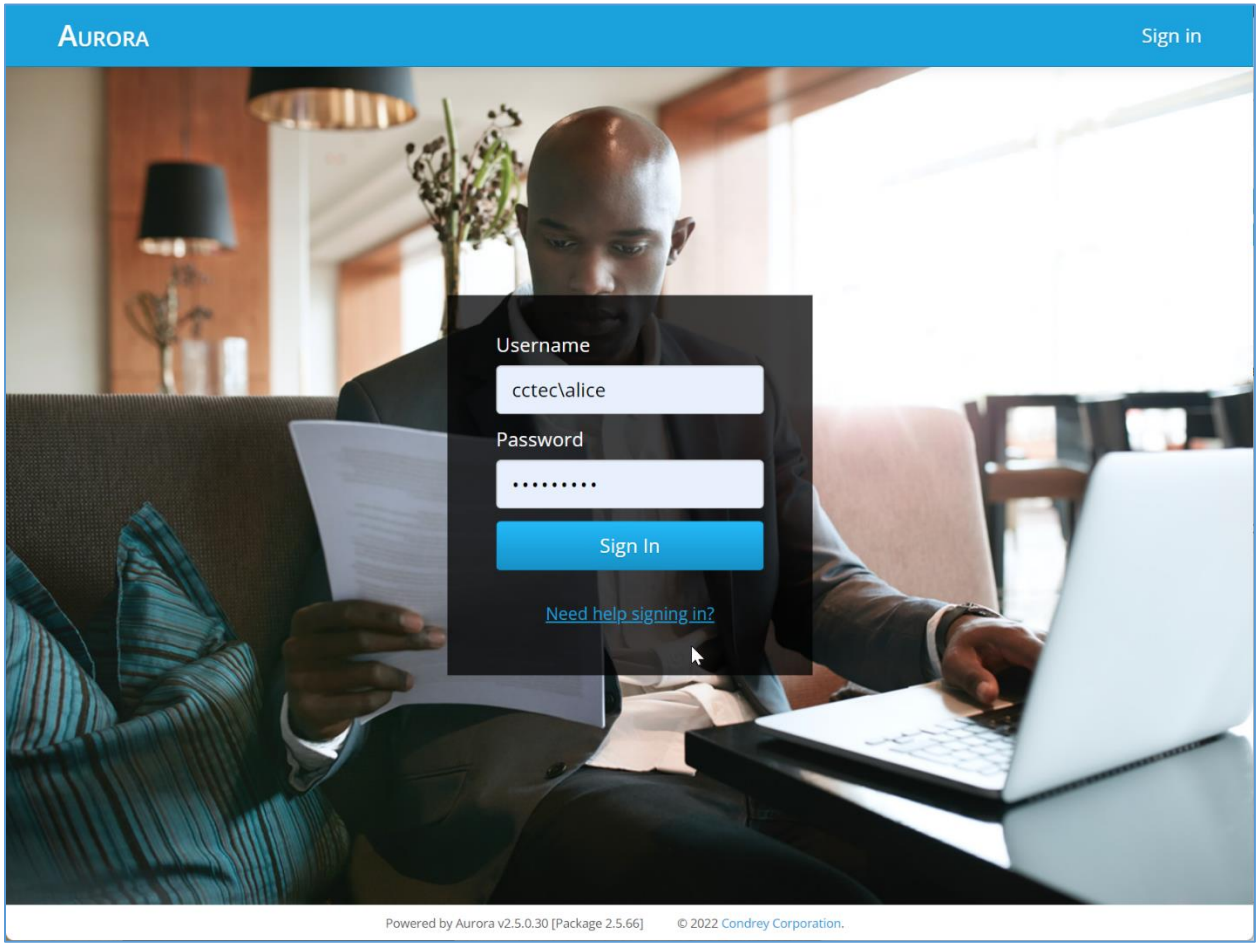
- https://developer.mozilla.org/en-US/docs/Web/CSS/background
- https://www.w3schools.com/css/css_background.asp

6.3.2 Adding Custom Help Link

For internal users, an optional Help link for authentication may be included on the Aurora login page.

To set the help website link enter a valid URL reference in the Web Application *Authentication Help* field.

The next time a user visits the Aurora login page, the *Need help signing in?* link is displayed at the bottom of the sign-in form.



6.4 Customizing other Web Elements

If you are proficient in web design with HTML and CSS, you may consider changing core elements of the appearance of Aurora or Aurora .Ext. Based on the default installation paths, the CSS stylesheets are found here:

- `c:\inetpub\aurora_root\Content` (Aurora)
- `c:\inetpub\auroraext_root\Content` (Aurora .Ext.)

Documentation on customization for HTML and CSS is beyond the scope of this document, but there are many resources available on the Internet for your consideration.



Please note that the only CSS and HTML changes directly supported by Condrey Corporation are those available within Aurora's web application itself for site branding and mail templates. While this section provides guidance on advanced customization of CSS and HTML content of Aurora, changes to CSS and HTML files along with consulting for CSS design is beyond the scope of Condrey Corporation technical support.



Upgrading Aurora or Aurora .Ext will replace any modifications to customized files in the website folder. Be sure to backup any modified files before upgrading since they will need to be replaced after the upgrade is complete.

APPENDIX A – KNOWN ISSUES

- If you see the error *"Attempted to access an unloaded appdomain"*, you may need to restart the Application Pool. This error message will only occur when accessing Aurora on the local server, while all other users will simply see the "Service Unavailable" message. This error message will also be found in the error log.

- The File Management interface may occasionally hide a modal dialog behind the grayed-out section of the screen. At this point, the only way to close dialog is via the 'Escape' key or a full-page refresh.

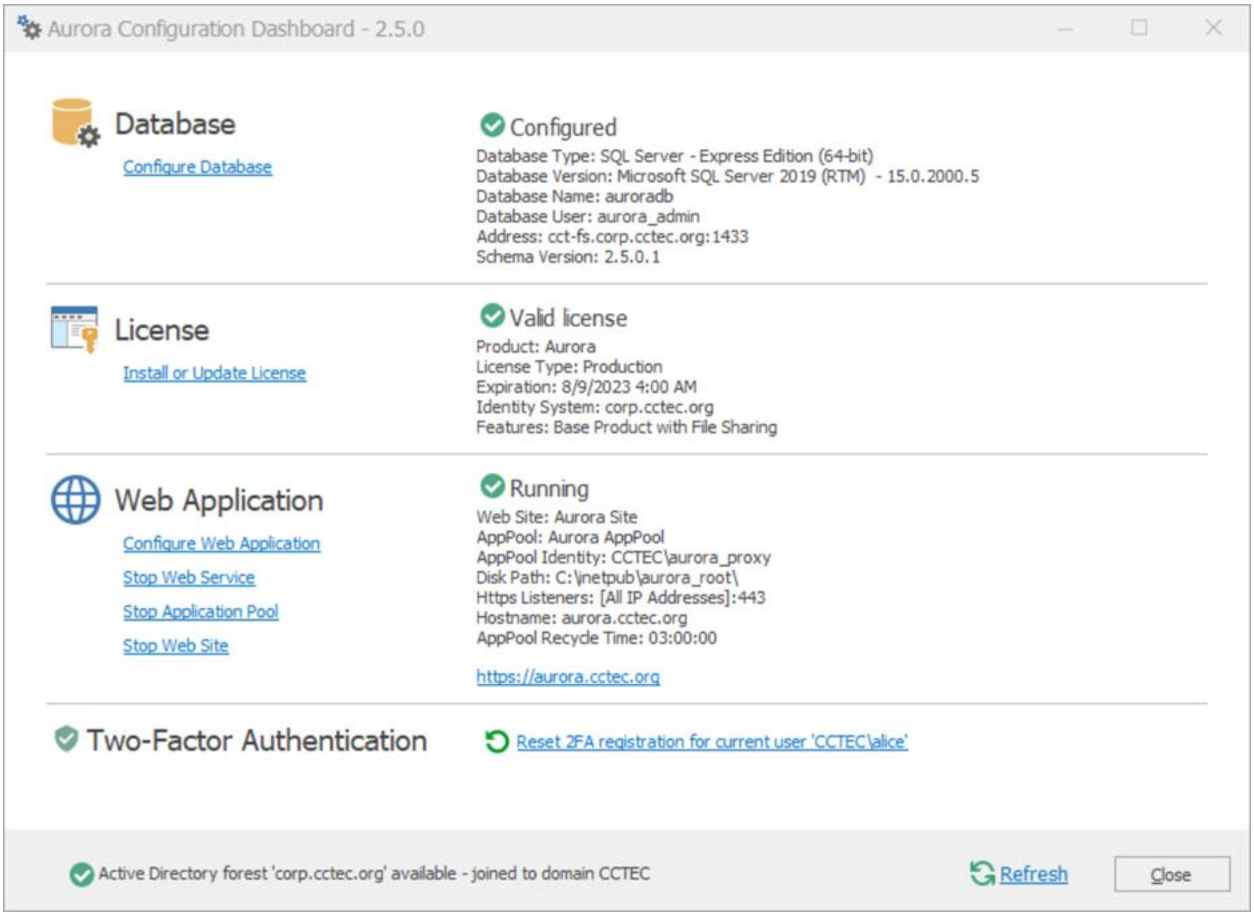
Appendix B – Troubleshooting Two-Factor Authentication

Resetting 2FA for Aurora Admins

If an Aurora administrator account is locked out of Aurora due to a missing device or invalid 2FA registration, any other Aurora administrator may reset that user's 2FA registration following the steps in section *2.4.3 Reset Two-Factor Authentication*.

In the case where no other Aurora administrator is available, an Aurora administrator can reset his own 2FA registration using the *Aurora Configuration Dashboard* utility on the server where Aurora is installed.

1. Login to the Windows Server where Aurora is installed using the Active Directory user account you wish to reset.
2. Launch the *Aurora Configuration Dashboard* utility from the Start Menu.



3. In the *Two-Factor Authentication* section at the bottom of the utility, click the link **Reset 2FA registration for current user *Domain\User***.

4. Click **Yes** to confirm the 2FA registration reset or click **No** to cancel.



Note that the Aurora admin user must also have login privileges on the Windows Server where Aurora is installed. The user who initially installs and configures Aurora requires this access during the install process anyway and is automatically added to the Aurora Admins group.

GLOSSARY

Aurora	A term referring to the entire Aurora suite of products providing web access for internal and external users of an organization. This term may also refer to just the primary web application accessed by Internal Users.
Aurora .Ext	The web application that provides Guests access to shared file system content.
Guest / Guest User	Any user that registers with and accesses storage via the Aurora .Ext application.
Guest Share	An access specification created by a Provider in Aurora for a specific file system folder that is “shared” with a Guest account.
Internal User	Any user that accesses Aurora using Active Directory credentials. It is assumed that this user is “internal” to the organization hosting Aurora.
Provider	Any Internal User that has been delegated rights to share a storage path with a Guest account.
Provider Rule	A Provider Rule is essentially a security construct that defines the delegation administrators give to trusted Providers so that they may share file access with Guest users. A single Provider Rule is the combination of a file system path, a Provider or Provider group, and the set of allowed share permissions.
Senergy	Senergy is a file system management product from Condrey Corporation that assists with the automation of file system data and hierarchies as it relates to identity management and associated lifecycles. See http://www.condreycorp.com/Senergy for more details.
Storage Map	The set of manually defined relations between specific file system paths and users or groups of users. A single Storage Map entry consists of a UNC path and a target user or group.

Storage Mapping / Storage Entry

A defined file system storage location, generally accompanied by a simple name or alias.

A Storage Mapping may come from automatic processing, or from an entry in the manually defined Storage Map.

Automatically defined entries include Home Folders and *Senergy* managed paths such as Collaborative storage and Auxiliary paths.