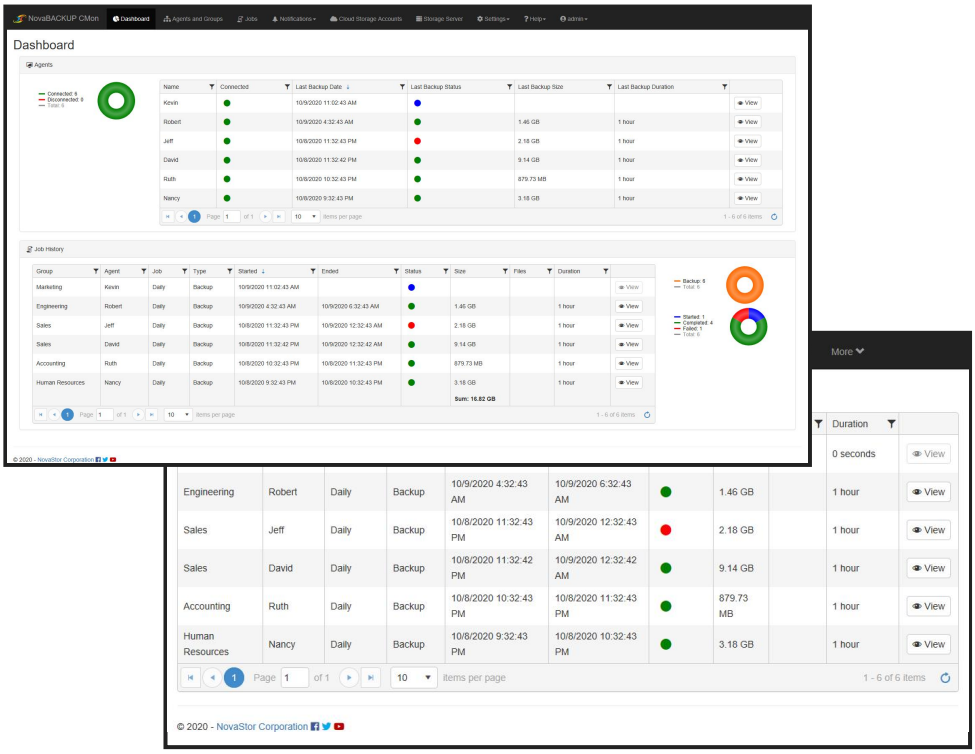
October 2020

NovaBACKUP®

CMon v19.6

User Manual



Features and specifications are subject to change without notice.
The information provided herein is provided for informational and planning purposes only.

© 2020 NovaStor. All Rights Reserved

Table of Contents

- Introduction
- System Requirements
- Installation
- Setting up the backup client
- Logging In
- The Dashboard
- Agents & Groups
  - Agents
    - Details
    - Devices
    - Create Device
    - View Network Device Details
    - Edit Network Device
- Log Viewer
- Notification Triggers
- Account Management
  - Set Password
  - Password
  - Time Zone
  - Language
- Cloud Storage Accounts
  - Create an account
  - Connect to an account
  - View details of an account
  - View computers
  - Edit cloud storage account
  - Change the password

- Change the license key
- Delete an account
- Delete a computer
- Storage Server
- Settings
  - Agent Settings
  - Security Settings
  - Notification Settings
  - Users
    - User registration
    - User registration and creating a cloud storage account in one step
    - Create a user
    - View a user
    - Edit a user
    - Delete a user
  - User Registration
  - Roles
  - Storage Servers
    - Add a storage server
  - Web Hook
  - Update
  - Application
- Server Administration Desktop Application
- Scheduled Task
- Web Configuration File
- IP Filter Configuration File
- Help
  - Documentation
  - About
  - Known Issues
  - Troubleshooting Tips
  - Windows Service Logging

Standalone Web Server Logging
Web Site Logging
Scheduled Task Logging

Introduction

Thank you for choosing NovaBACKUP® CMon by NovaStor

CMon (Central Monitoring Console) is an application that works along side your NovaBACKUP PC, Server, and Business Essentials backup software. The CMon can be utilized to monitor the associated backup jobs in your entire backup environment, all from a single pane of glass style website interface. CMon is accessible via web browser and can be viewed via Internet Explorer 9+, Google Chrome, Mozilla Firefox as well as most smart phone web browsers.

NovaBACKUP® CMon is composed of 2 components.

1. The CMon (Central Monitoring Console) application enables the capability to monitor backup agents from any edition of NovaBACKUP® PC, Server, or Business Essentials, **version 18.0** and above. Typically CMon is installed on a Windows Server machine which does not have NovaBACKUP backup software installed on it. CMon can run on the same server that NovaBACKUP backup client is installed but it may perform better on a separate server. Read the System Requirements section for more information.
2. Your installations of NovaBACKUP® PC, Server and Business Essentials, version 18.0 or higher, which are installed on your systems to backup critical data, such as SQL and Exchange databases, as well as virtual environments. This quick start guide will describe how to setup the CMon, along with how to connect one installation of NovaBACKUP® (referred to as an agent) to the CMon. Subsequent installations of NovaBACKUP® PC, Server and Business Essentials will require configuration to connect to the CMon in the same manner.

System Requirements

Hardware

- Intel **Dual Core** CPU or better
- 4 GB of RAM minimum
- 3 GB free hard drive available space on OS drive

Operating System

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2008 SP2

Microsoft .NET Framework

Microsoft .NET Framework 4.6 or higher

SQL Server (Optional)

Microsoft SQL Server is recommended when using more than 5 backup agents.

- Microsoft SQL Server 2017
  ⊟ Download Microsoft SQL Server 2017 Express
- Microsoft SQL Server 2016
  ⊟ Download Microsoft SQL Server 2016 SP2 Express
- Microsoft SQL Server 2014
  ⊟ Download Microsoft SQL Server 2014 SP2 Express
- Microsoft SQL Server 2012

How to determine the version, edition, and update level of SQL Server and its components

Web Server (Optional)

IIS with IIS 6 compatibility

Networking

- TCP/IP network

Web Browser

- Modern HTML5 supported **desktop** web browsers such as Internet Explorer 9 and above, Chrome, Firefox, Safari, Opera, Edge
- Modern HTML5 supported **mobile** web browsers such as Android 5.0, iOS 9.0, Windows 10, BlackBerry 10, Opera Mobile, Amazon Silk

Note: To test HTML5 compatibility with your current browser please test it here: https://html5test.com/. A points score closer to 500 is optimal.

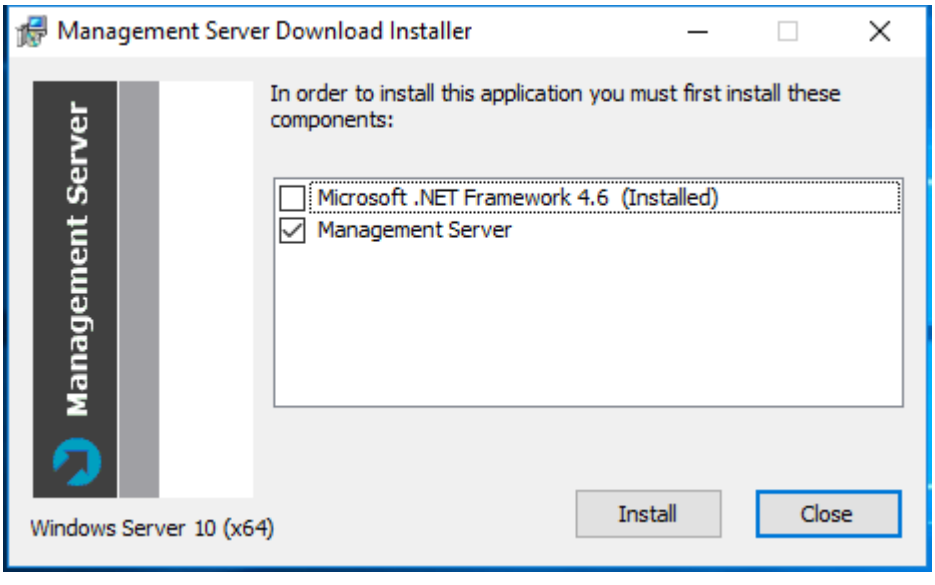
Installation

Please make sure the machine meets the System Requirements before continuing.

Run the setup executable to begin the installation wizard.

Download Installer

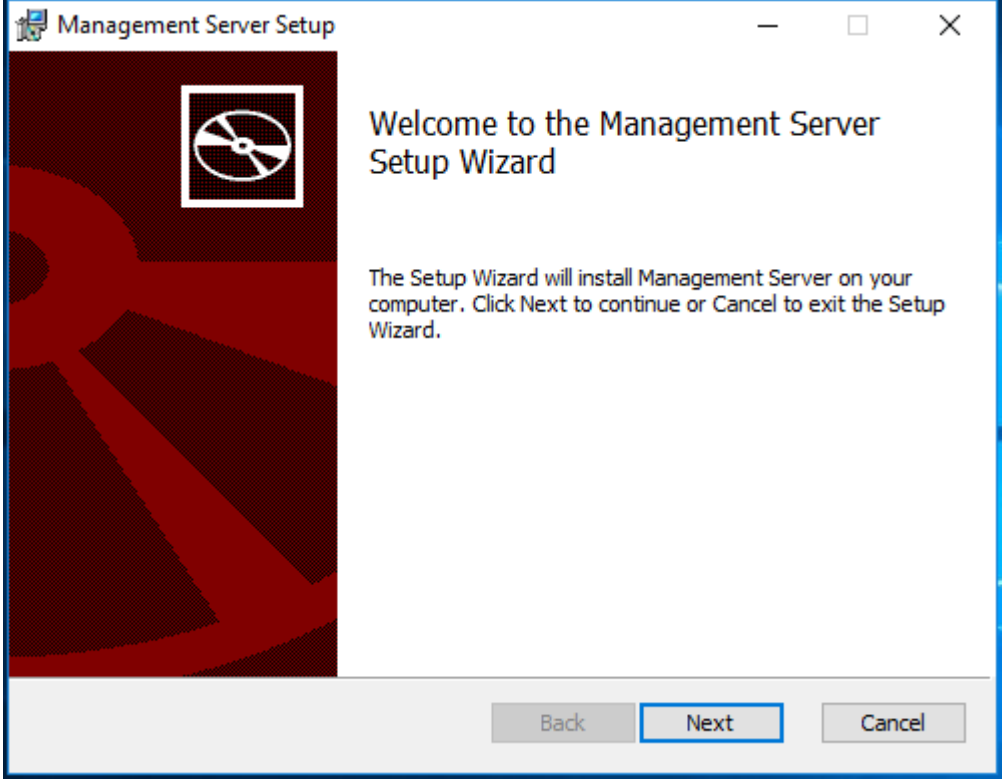
The `Download Installer` dialog indicates the missing required prerequisites and automatically downloads and installs them.



Click the `Install` button to continue.

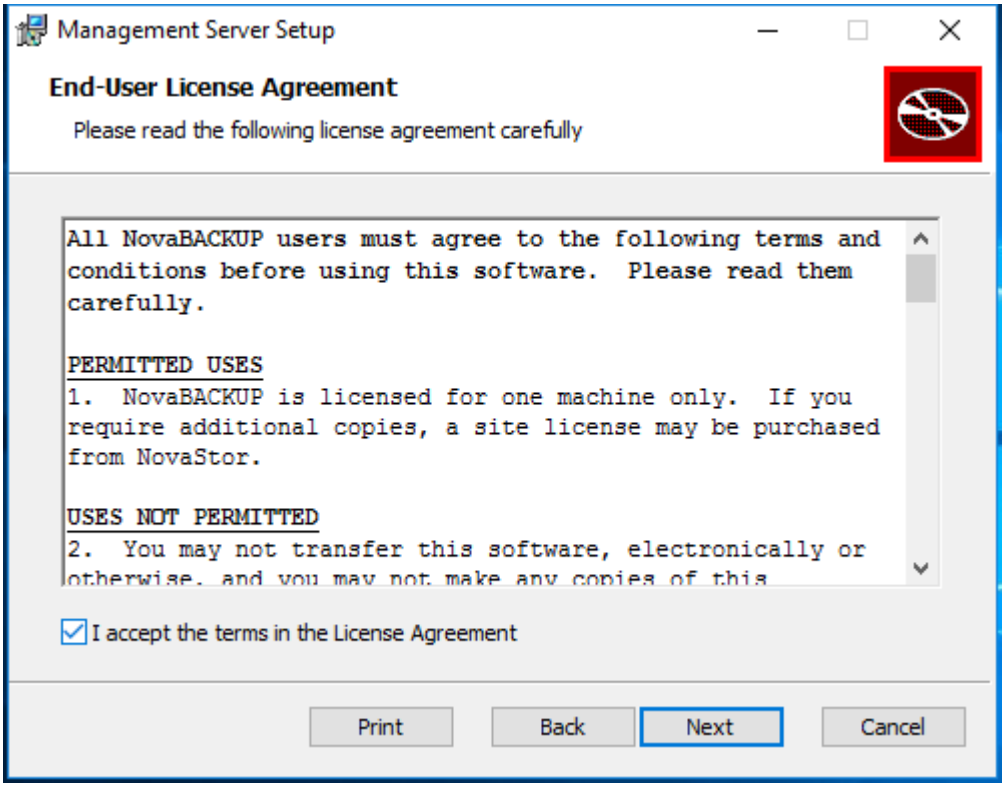
Welcome

After the prerequisites are installed, the CMon installation wizard's `Welcome` dialog is displayed.



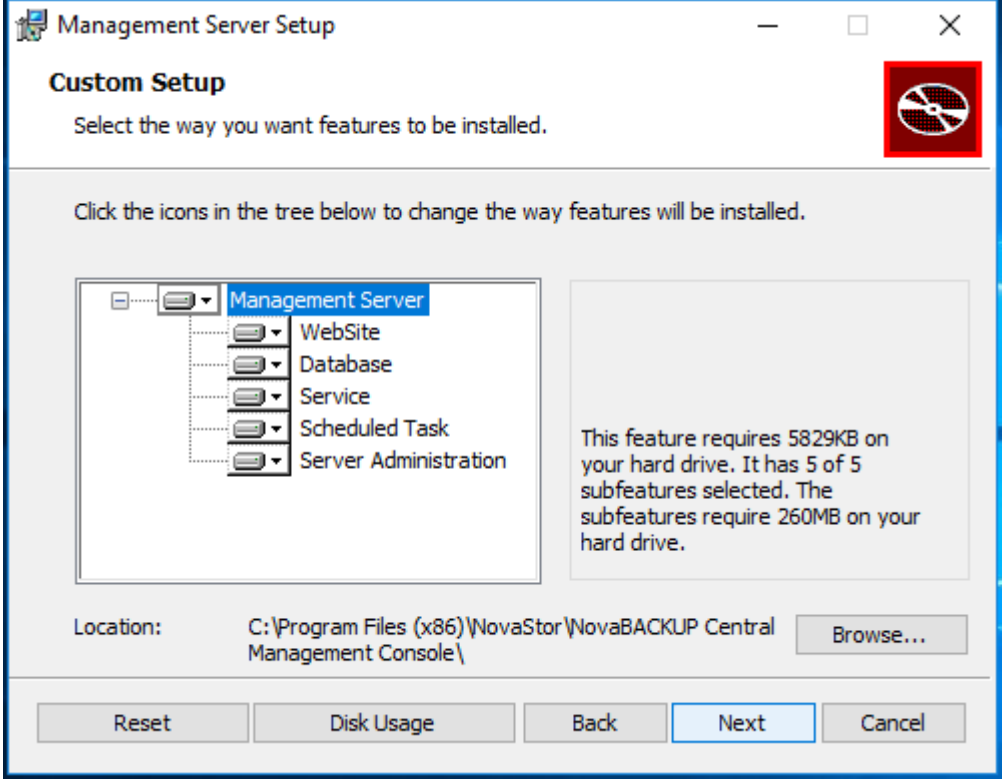
Click the `Next` button to continue.

End-User License Agreement



Check-mark the `I accept the terms in the License Agreement` check-box and click the `Next` button to continue.

Custom Setup

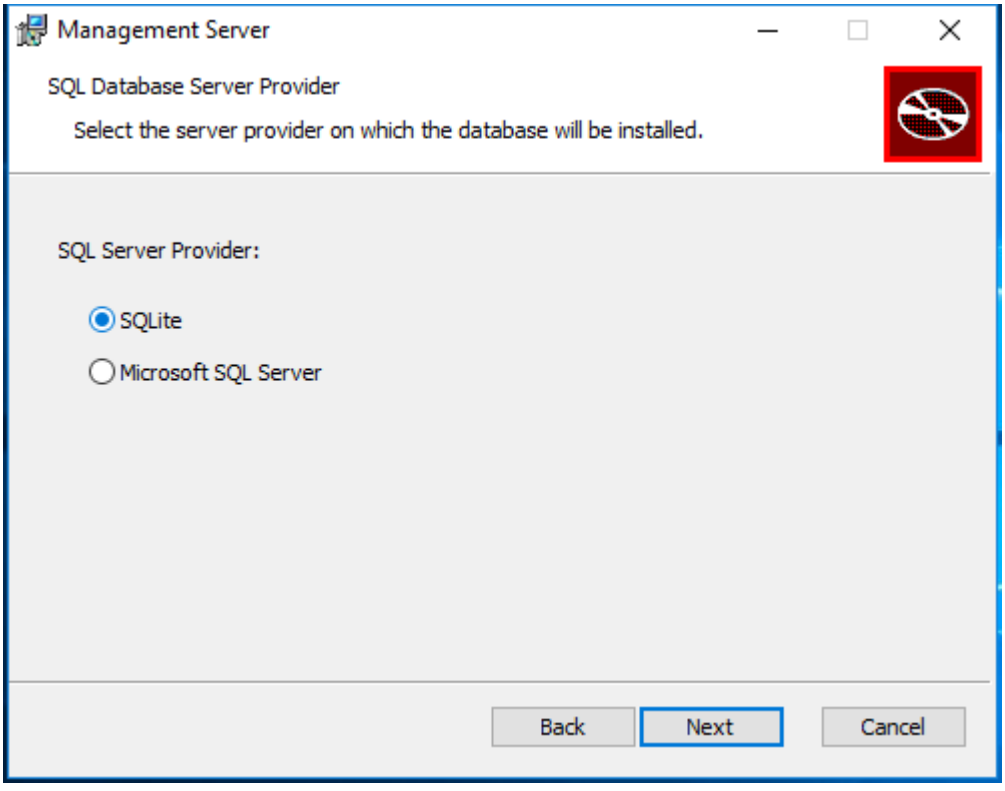


Click the `Next` button to continue.

SQL Database Server Provider

Select the sever provider on which the database will be installed.

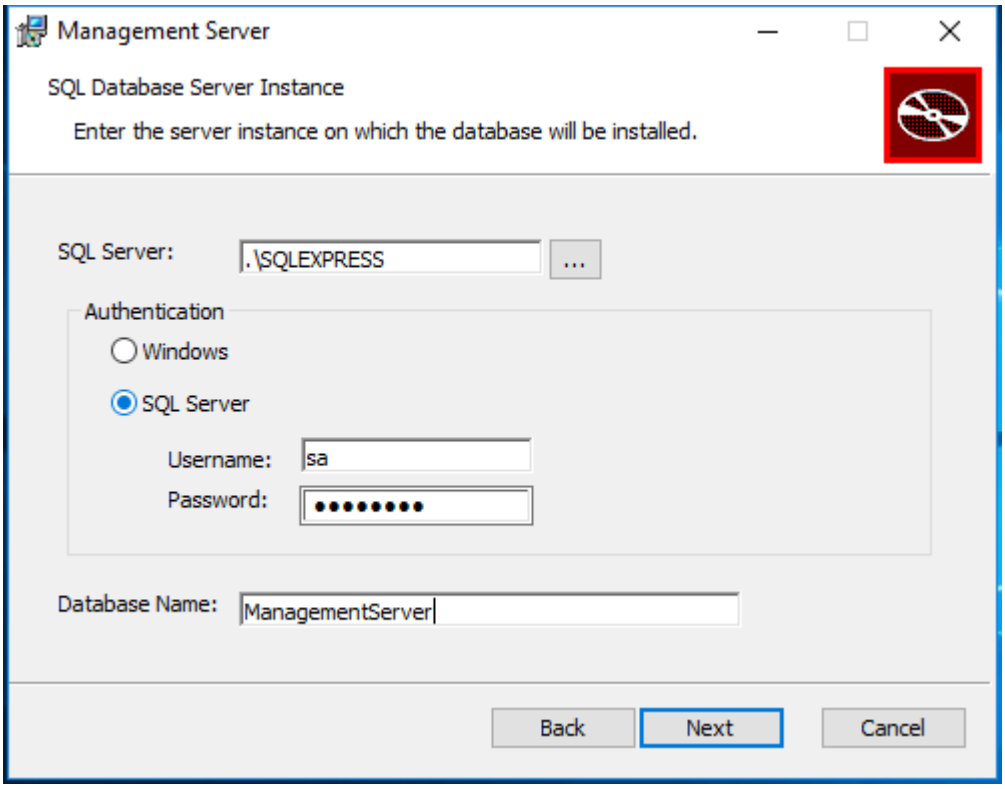
Microsoft SQL Server is recommended for better performance and an improved experience.



Click the `Next` button to continue.

SQL Database Server Instance

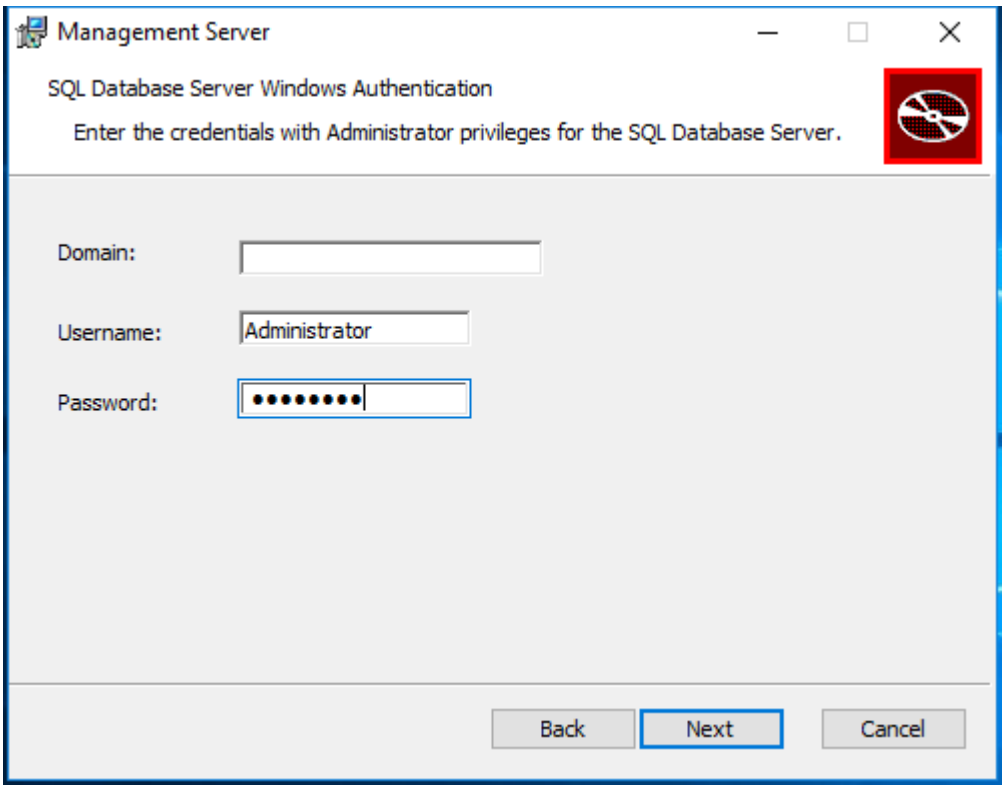
If `Microsoft SQL Server` was selected, the `SQL Database Server Instance` dialog is displayed.



Enter the required values and click the `Next` button to continue.

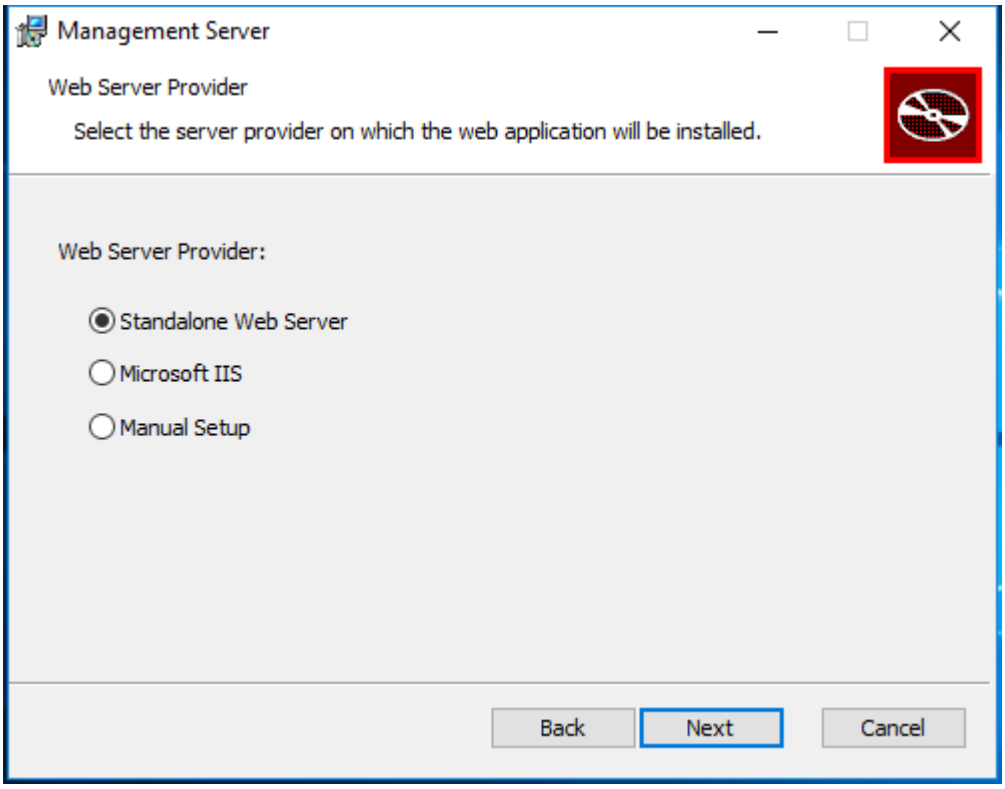
SQL Database Server Windows Authentication

If `Microsoft SQL Server` was selected, the `SQL Database Server Windows Authentication` dialog is displayed.



Enter the required values and click the `Next` button to continue.

Web Server Provider



Select the server provider on which the web application will be installed.

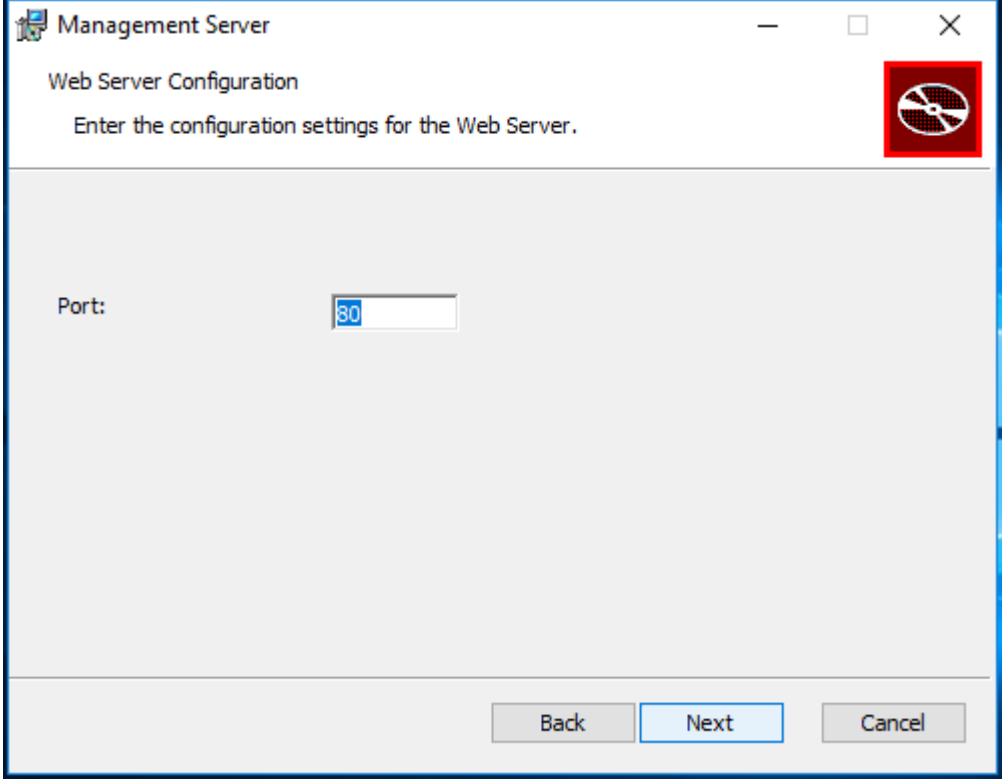
Microsoft IIS is recommended for better performance, an improved experience, and greater security.

Web Server Configuration

If `Standalone Web Server` is selected, the `Web Server Configuration` dialog is displayed.

The setup installer will automatically open this port on the Windows firewall.

Make sure network traffic on the selected port is allowed to enable accessing the CMon web application from a web browser.

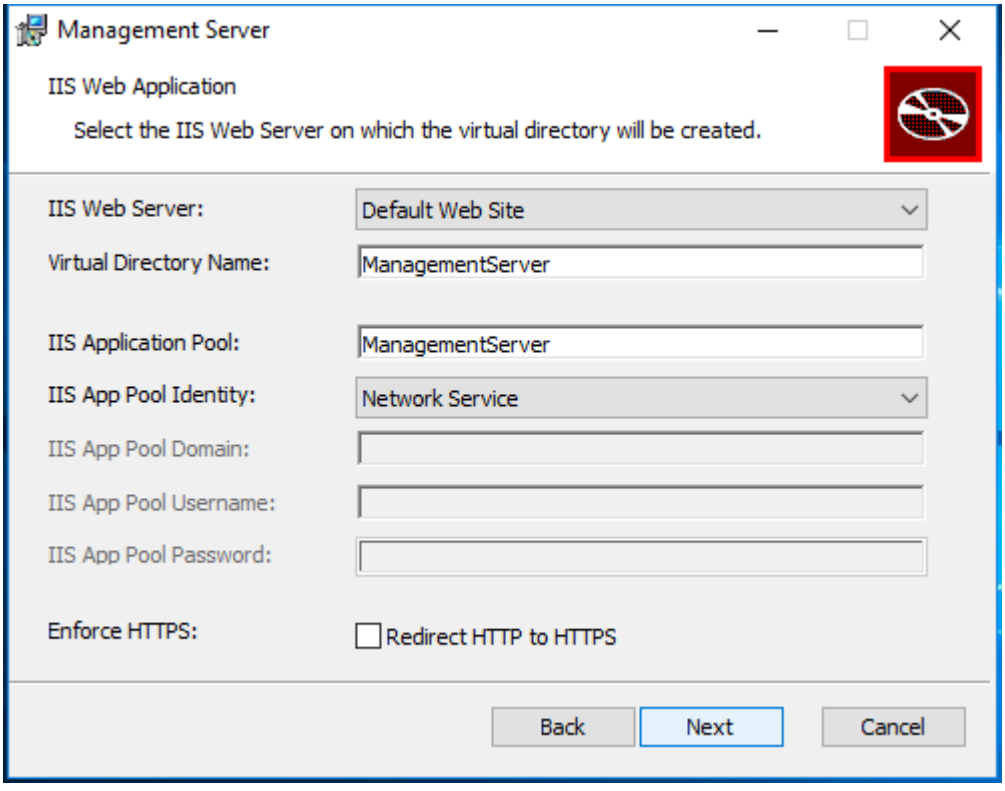


Click the `Next` button to continue.

IIS Web Application

If `Microsoft IIS` was selected, the `IIS Web Application` dialog is displayed.

Make sure network traffic on the web server ports are allowed to enable accessing the CMon web application from a web browser.



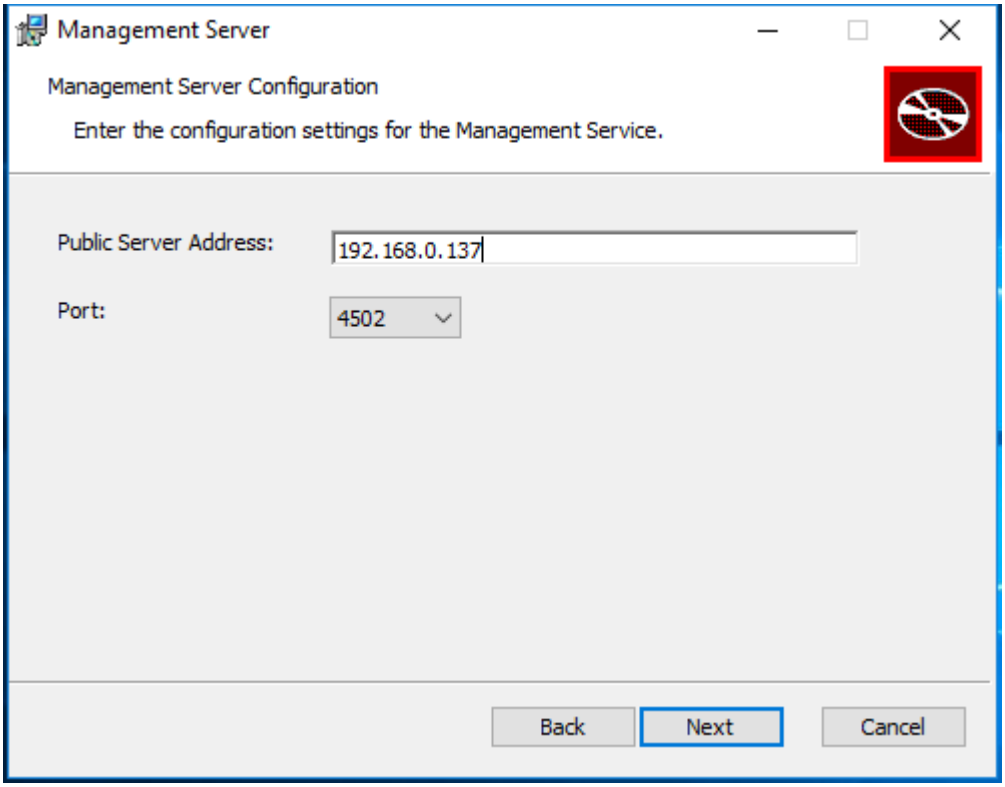
Check-mark the `Redirect HTTP to HTTPS` check-box to enforce requests to use HTTPS.

Using HTTPS is recommended for greater security.

The IIS Web Site in Microsoft IIS must be configured to support HTTPS.

Enter the required values and click the `Next` button to continue.

Management Server



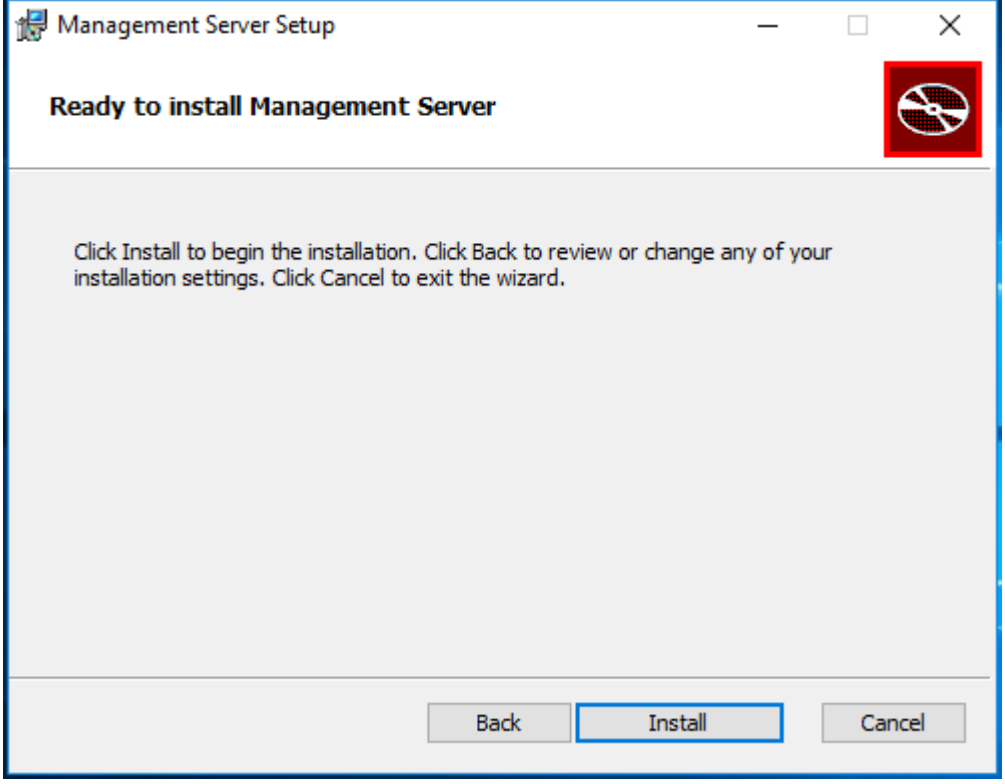
The `Public Server Address` (IP address, DNS, or computer name) and `Port` need to be configured in backup client agents in order to connect to CMon.

The setup installer will automatically open this port on the Windows firewall.

Make sure network traffic on the selected port is allowed to enable backup client agents from communicating with the CMon service.

Click the `Next` button to continue.

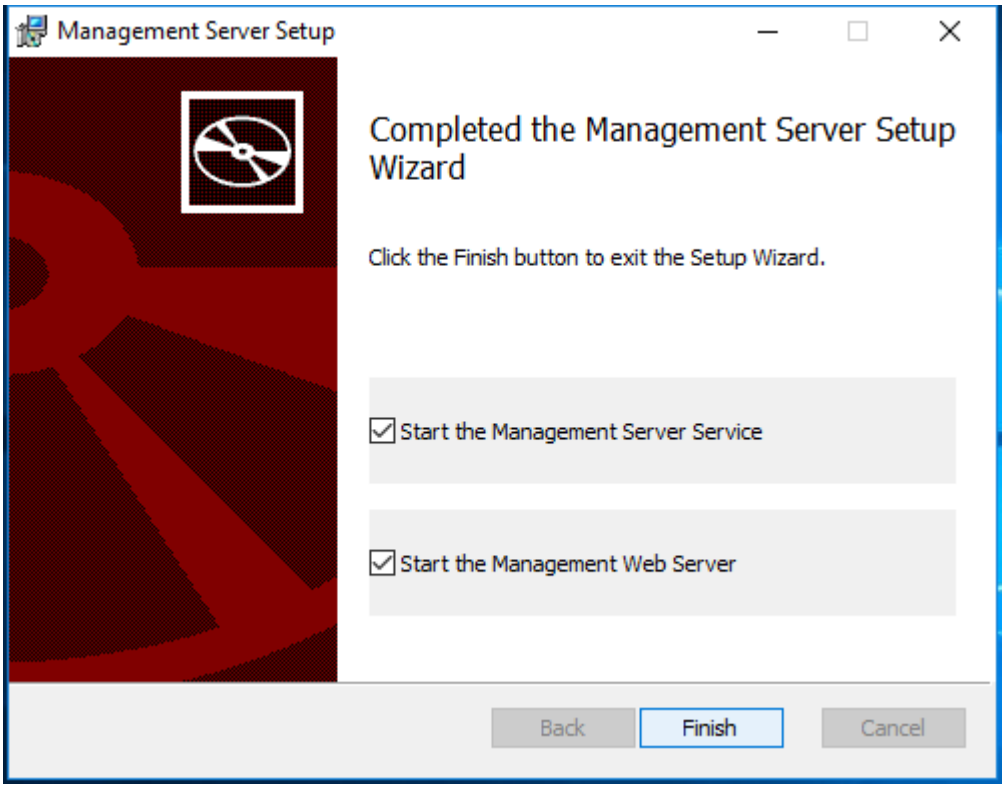
Ready to Install



Click the `Install` button to start the installation.

Finish

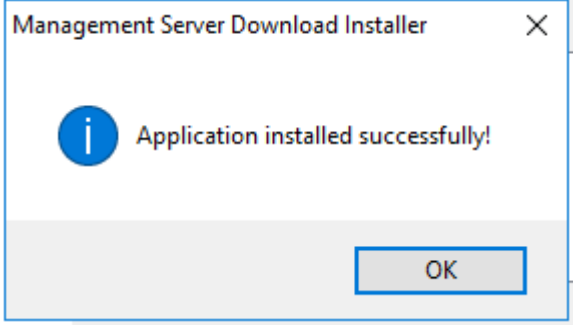
After a successful installation, the `Finish` dialog is displayed.



Check-mark the check-boxes to start the required services.

Click the `Finish` button to exit the installation.

Application Installed Successfully



Click the `OK` button to close the installer.

Next Steps

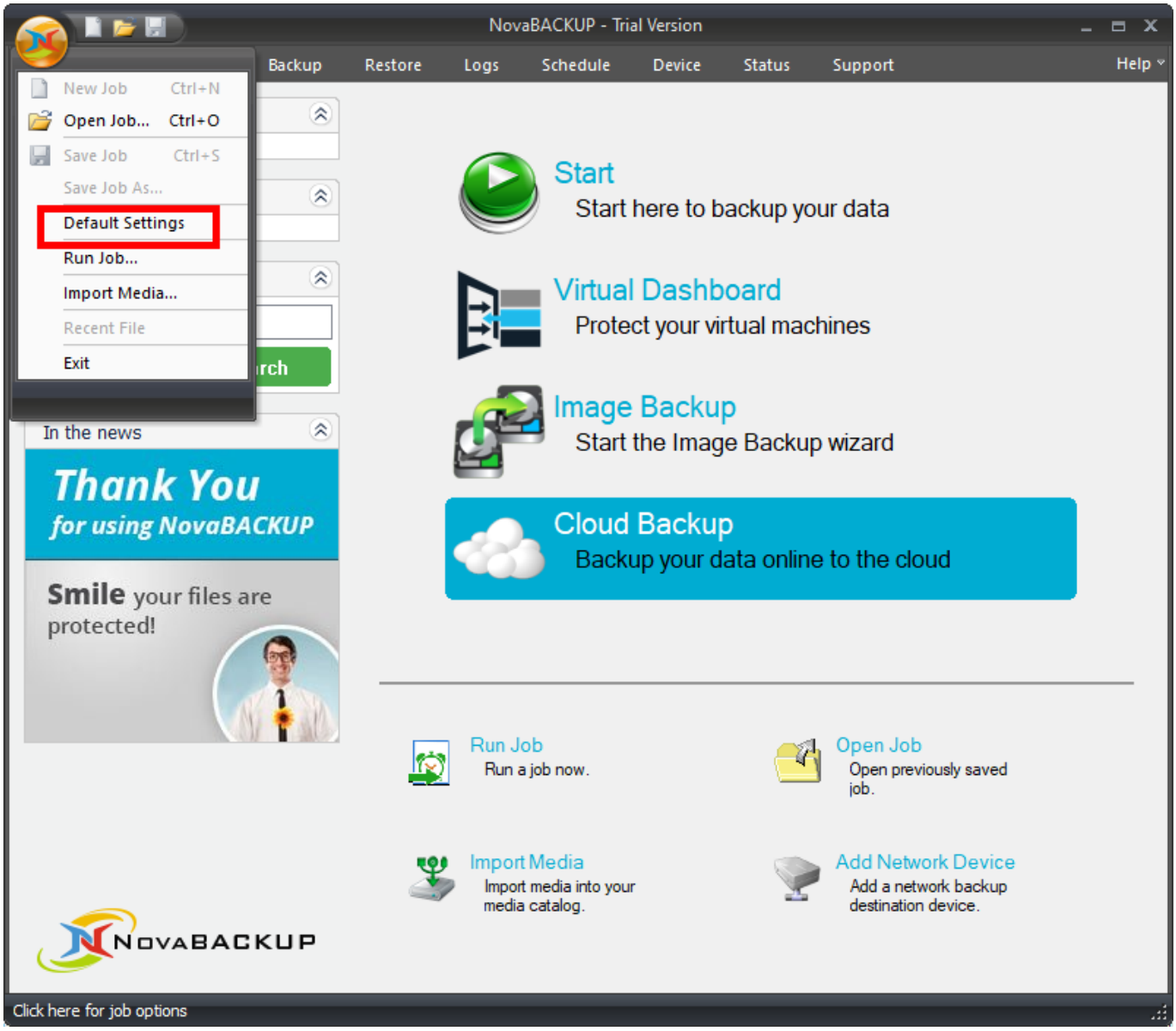
Logging in

Setting up the backup client

Setting up the backup client

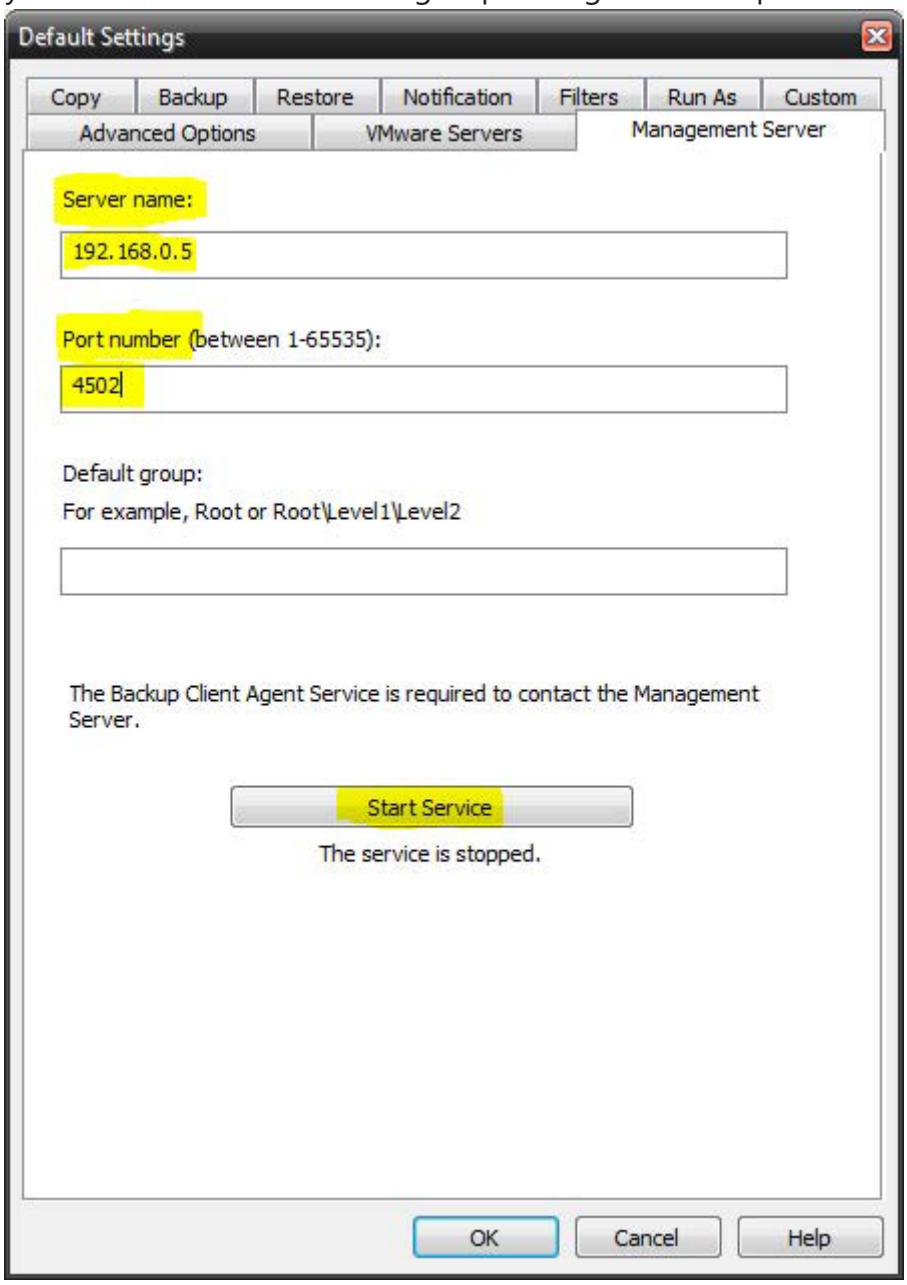
Now that you have the CMon successfully installed it's time to connect an agent to it. This section will cover how to setup the backup client software to connect to CMon.

1. The first thing you need to do is install a backup client (NovaBACKUP® PC, Server, or Business Essentials) on the machine you'd like to back up. For instructions on how to do this please consult the NovaBACKUP® Quick Install Guide. By accepting all default options during installation, all necessary items will be installed. Once NovaBACKUP® PC, Server, or Business Essentials is installed we need to configure the connection to CMon. NovaBACKUP PC, Server, and Business Essentials clients require a setting to be configured in order for the backup client to become an Agent.
2. Start the NovaBACKUP client and click on the Home tab.
3. From the main menu click the large circle NovaStor logo button highlighted at the top left, and then click " **Default Settings** ". >



   This will open a screen with a series of additional tabs.
4. Once in " **Default Settings** " you will click on the " **Management Server** " tab. You will be required to configure the " **Server name** " and " **Port number** " variables on this screen. Enter the server address or IP address of the machine where CMon is installed in the "**Server name**" field. Enter the port number CMon is configured to use in the "**Port number**" field. These values

should be the same values entered during the CMon installation. The default port number is 4502. The "Default group" option on this screen will automatically place this agent into the group specified on the CMon. In general you do not need to enter anything in the Default Group option at this point. If you do not choose a Default group this agent will be placed in the "Pending" group in CMon. >

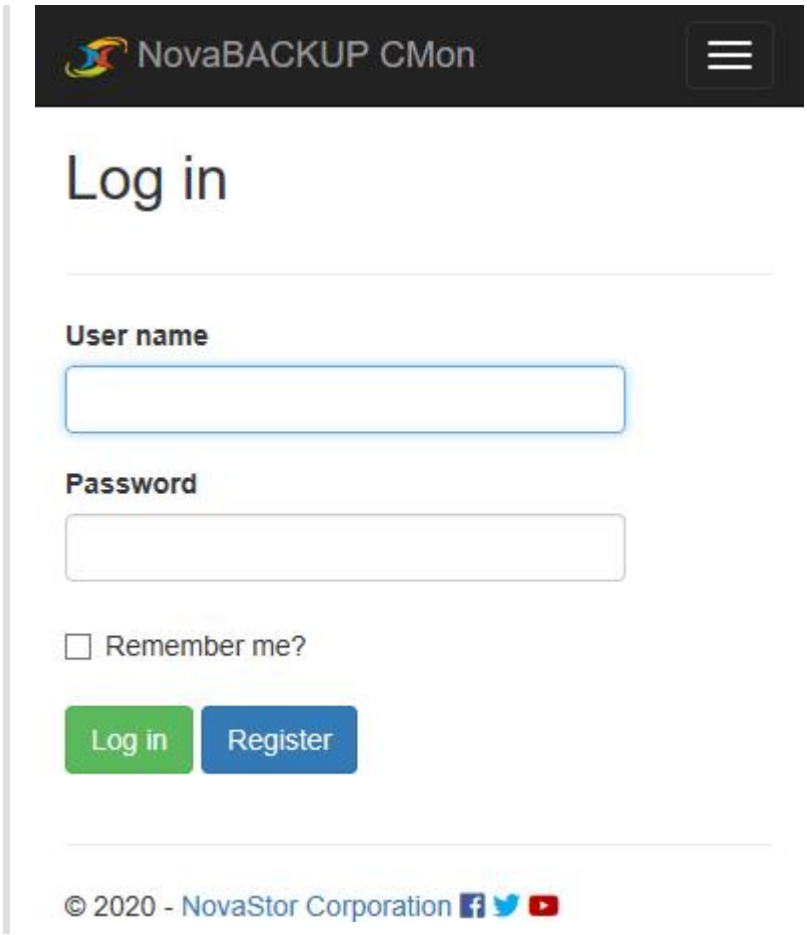


5. Click the "**Start Service**" button to start the service. "The service is started" is displayed when the service has started successfully which is required in order to connect to CMon. Click the "OK" button to save the changes. Now you have the CMon installed, the backup client installed, and the agent connected to CMon. You should now be able to login to the CMon and see the agent.
6. To verify the service is an automatically starting service, open up Windows Services. Once in the Services screen, find the service named "Backup Client Agent Service". This is the service that actually connects to the CMon so you can monitor your agent. By default this service is set to Manual, go to the properties of this service and set it to Automatic (Delayed Start), and [Apply]. You may now exit out of Windows Services.
7. Additional agents may be connected using these same steps.

Logging In

Logging in to the CMon is as simple as opening a web browser on your computer and browsing to the IP address, DNS name, or computer name along with the port number that you configured during the CMon installation; the default web port is 80. A shortcut to the website is installed on the computer where CMon was installed in the Start Menu in the "NovaStor" group for convenience.

The CMon website should work with any modern web browser including Internet Explorer 9 and above, Google Chrome, Mozilla Firefox as well as most smart phone web browsers.



The default login Username is **admin** with a Password of **admin**.

After logging in for the first time, it's recommended to change your password using the Account Management page.

If the number of times a user fails to log in because of an invalid password exceeds the maximum number configured in the Web Configuration File, the user will be locked out. Use the Users page to unlock an account. To unlock the admin account, use the Server Administration Desktop Application.

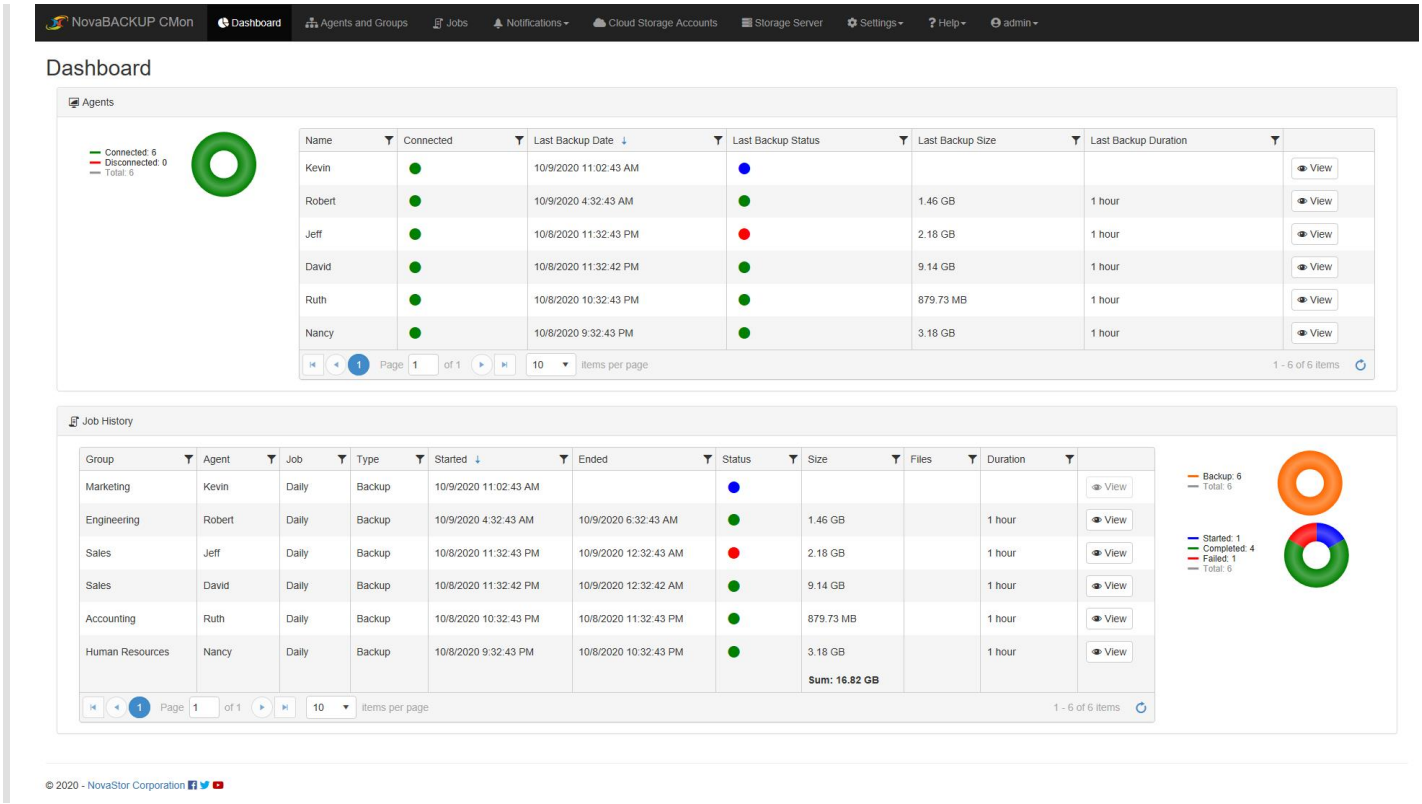
Users logging in or registering from the embedded web browser in the backup client will automatically be redirected to view or create a new cloud storage account if permitted.

If the "Remember me?" check box is checked, a cookie will be created which allows the user to remain logged in for up to 7 days of inactivity by default.

Dashboard

The CMon can be utilized to monitor all of the NovaBACKUP clients and the associated backup jobs in your environment, all from a single pane of glass interface. CMon is accessible via web browser and can be viewed via Internet Explorer 9 +, Google Chrome, Mozilla Firefox as well as most smart phone web browsers.

The **Dashboard** is displayed just after login. It is an overview of your NovaBACKUP environment.



The **"Menu"** that is displayed on the top of each page shows the various functions that can be quickly accessed. If the browser's width is too narrow, the menu will be collapsed and in order to expand the menu, click on the 3 horizontal lines near the top right corner of the page.

On the Dashboard screen you can perform various functions.

To view more details about a particular NovaBACKUP Agent in your environment, you can double-click on an "Agent" via the Dashboard screen. An Agent is simply a computer that is running NovaBACKUP backup client software that was configured to utilize the CMon application for monitoring.

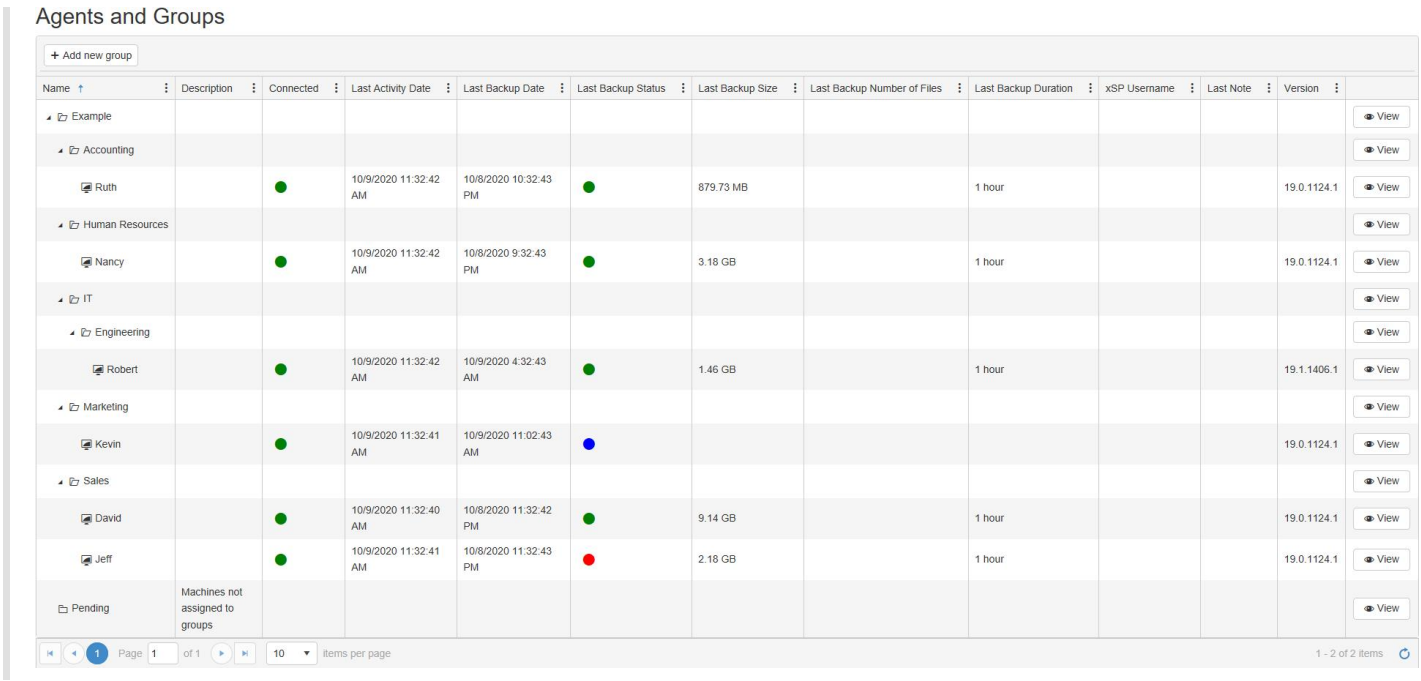
You can hover over the circular pie-chart graphic near the bottom right of the screen to see your job statuses. To display jobs with all of the various types of status including Failed, Successful, Warning, Stopped, and Started jobs.

PERMISSIONS REQUIRED

View Dashboard

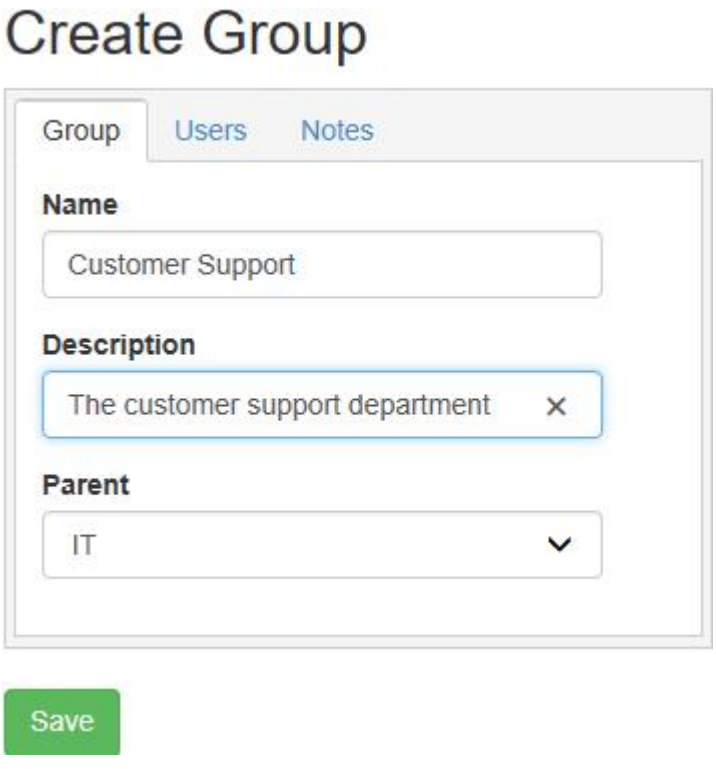
Agents and Groups

Agents and Groups is the area in CMon where you will view all of your client software that has been configured to connect to the CMon. You can create Groups here as well as print a Report of the contents of the Agents & Groups area.



Agents and Groups - Add new group function example:

Adding a Group is performed by clicking the " **Add new group** " button as seen in this example.

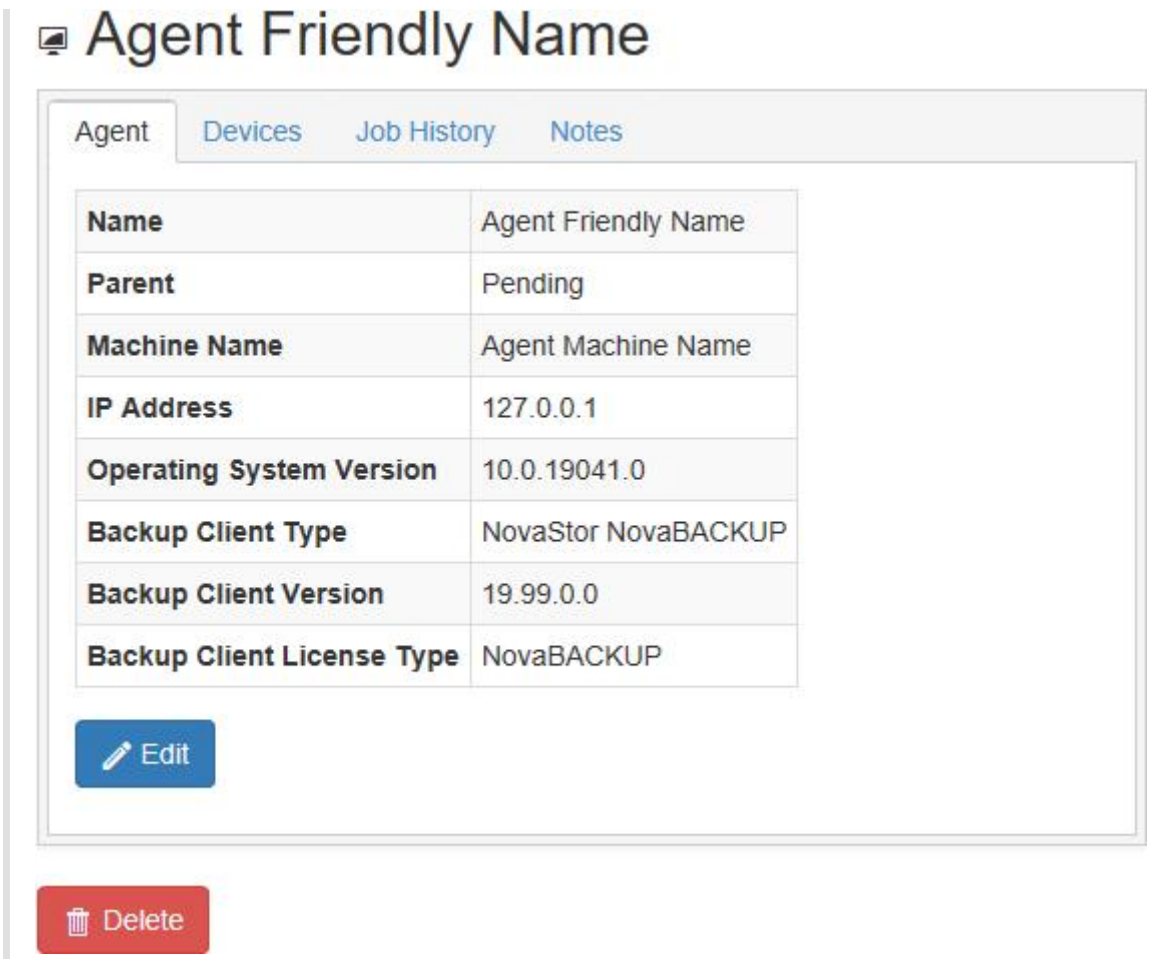


PERMISSIONS REQUIRED

View Agents and Groups

Edit Groups

Agent Details

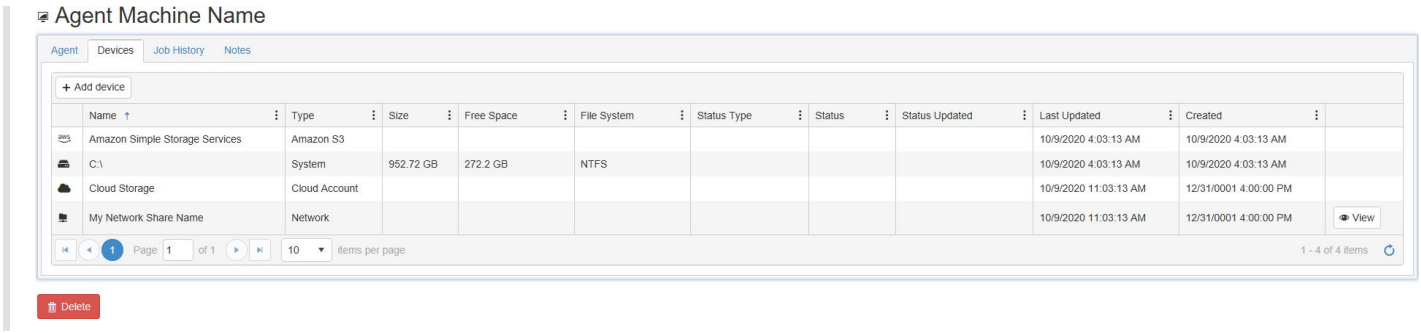


PERMISSIONS REQUIRED

View Agents and Groups

Agent Devices

The Devices tab of the Agent's details view lists the devices on the agent.



Users with permissions to edit the agent can add a new device.

Double-click on the row or click the `View` button to view the details of a device.

Related Topics

[Create Device]

[View Network Device Details]

PERMISSIONS

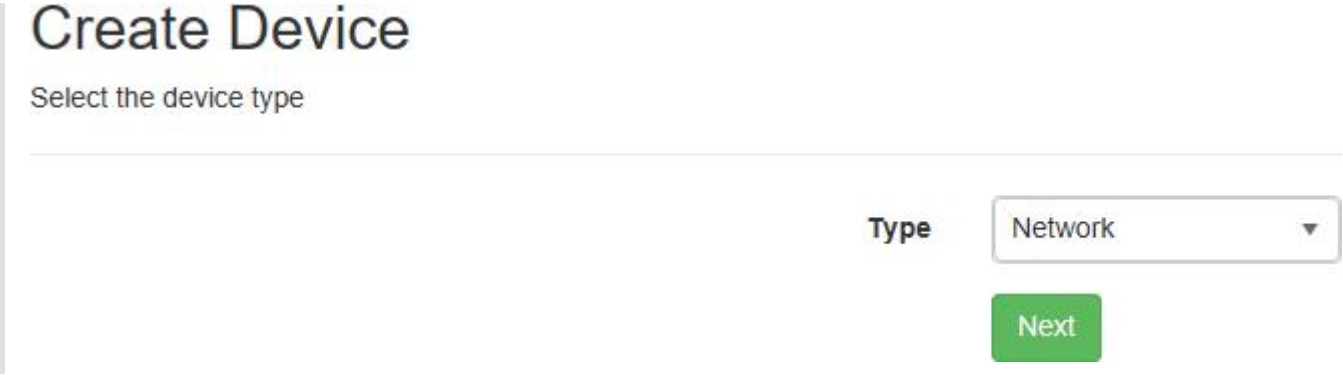
One of the following permissions are required:

View Agents and Groups

Edit Agents

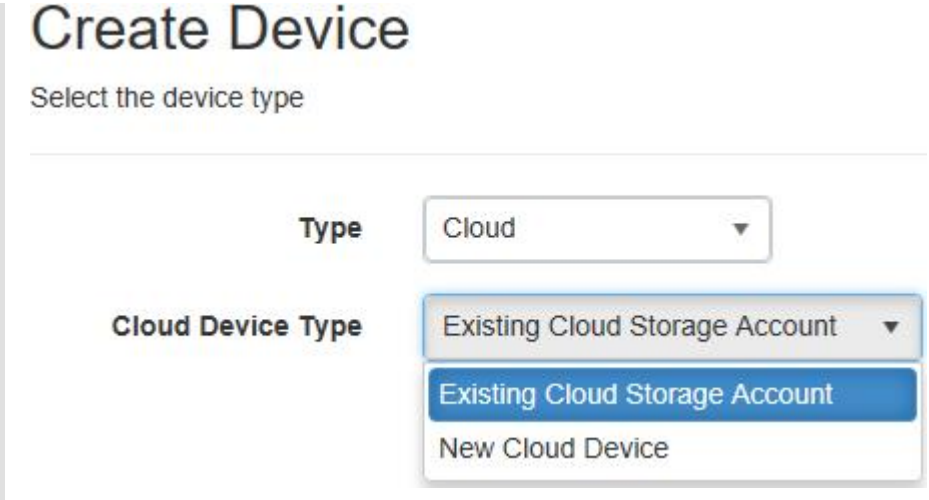
Create Agent Device

To add a new device, select the type of device in the Create Agent Device view.



A cloud device can only be added if the agent doesn't already have a cloud device because an agent is limited to one cloud device.

If a storage server is configured and the user has permissions to view cloud storage accounts, a cloud device can be added from an existing cloud storage account.



If the agent is disconnected, the device will be pending its addition until the agent reconnects.

If the agent is connected and the backup client service is running, the device will get created immediately.

Related Topics

Create Cloud Device From Existing Cloud Storage Account
Create Network Device

PERMISSIONS REQUIRED

Edit Agents

Create Agent Network Device

To add a new network device, enter the appropriate values in the required fields marked in **bold** and click the `Save` button.

Device name

- Required
- Must be unique
- Must not equal "Network"
- Maximum length is 99

Path

- Required
- Must begin with a double back slash
- Maximum length is 259

Domain

- Maximum length is 127

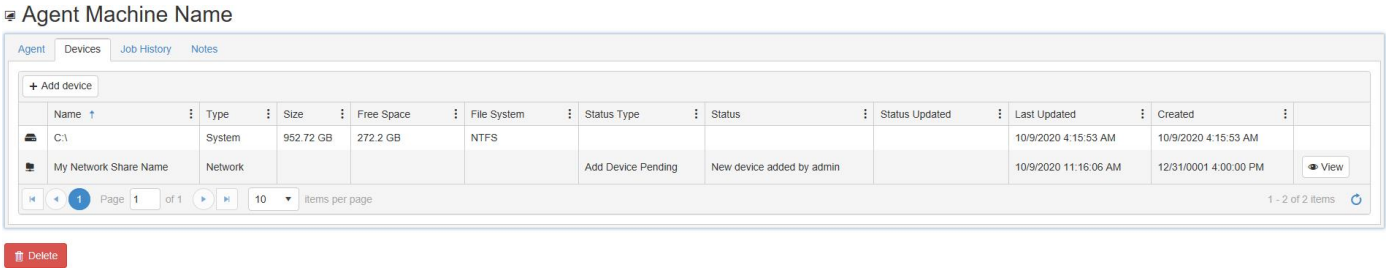
User name

- Maximum length is 127

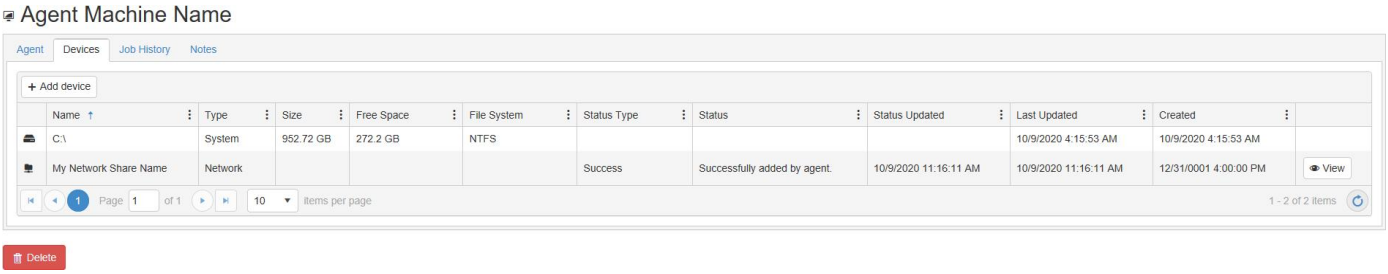
Password

- Maximum length is 127

If the agent is disconnected, the device will be pending its addition until the agent reconnects.



If the agent is connected and the backup client service is running, the device will get created immediately.

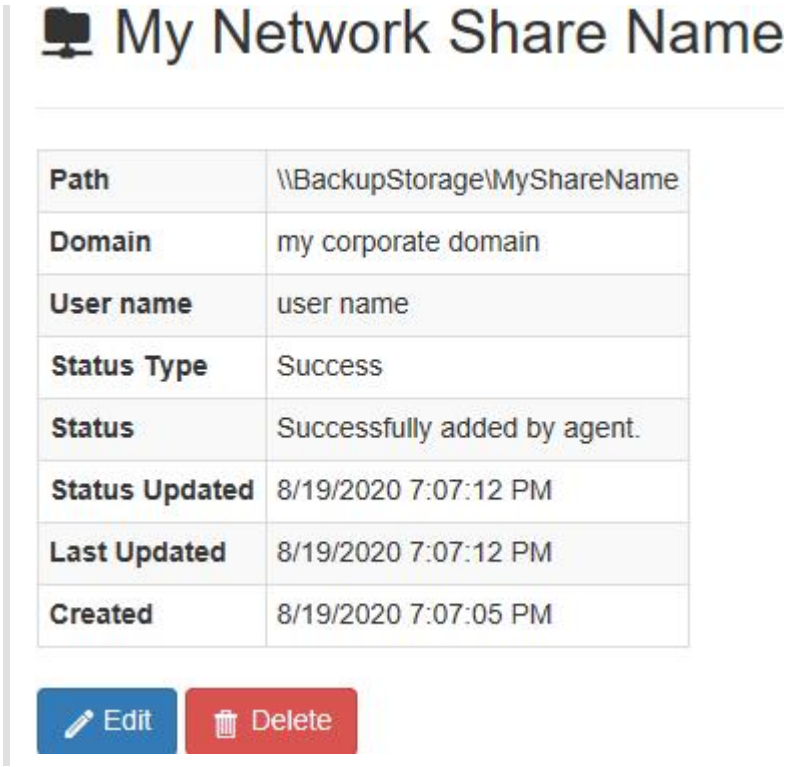


The network connection must be available at the time the device is added to the agent.

□ PERMISSIONS REQUIRED

Edit Agents

Network Device Details



Users with the `Edit Agents` role permission may edit and delete the network device.

Related Topics

Create Network Device

PERMISSIONS REQUIRED

View Agents and Groups

Edit Network Device

The device name can only be modified if the device hasn't already been added.

PERMISSIONS REQUIRED

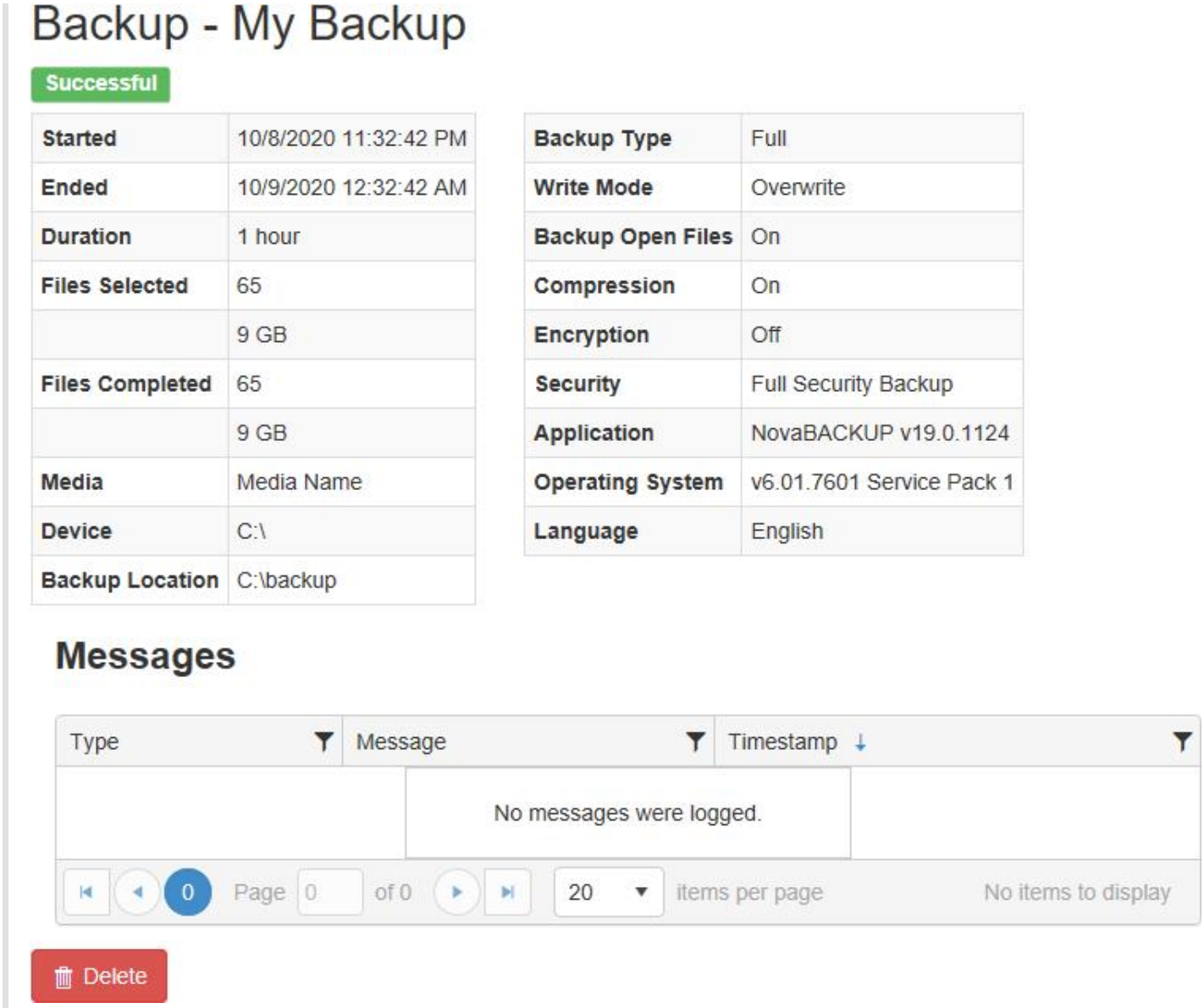
Edit Agents

Log Viewer

Log Viewer via the Dashboard example (1 of 2):

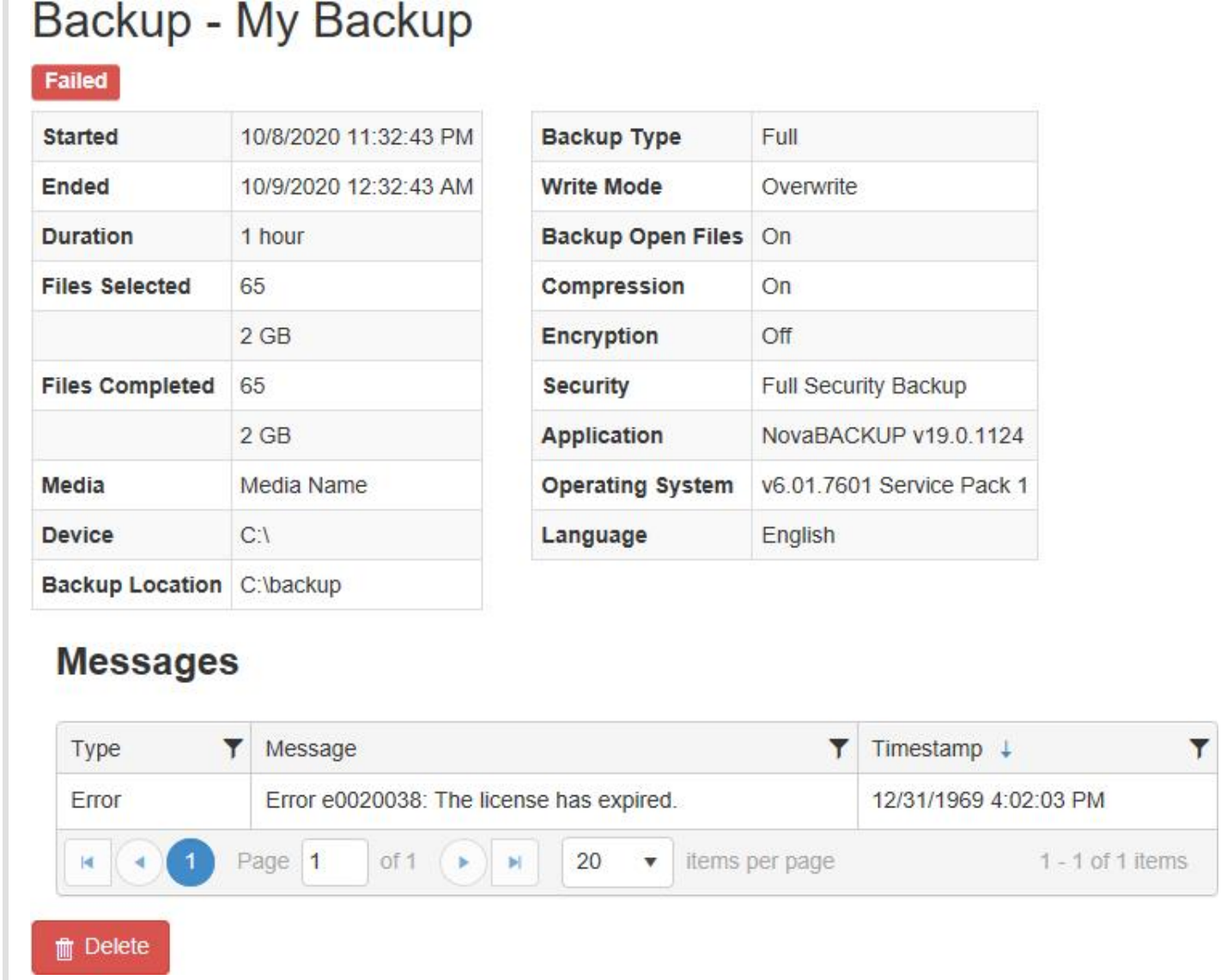
Via the Dashboard you can double-click on any agent name that you are interested in seeing the log for and it will display the backup log as seen in this example.

This first example is a job with Successful status.



Log Viewer via the Dashboard example (2 of 2):

This second example is a job with Failed status.



PERMISSIONS REQUIRED

View Job History

or

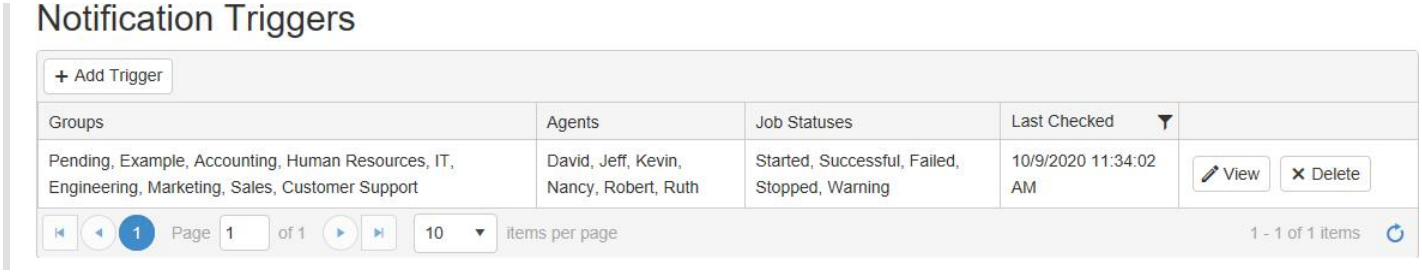
View Jobs and Job History

or

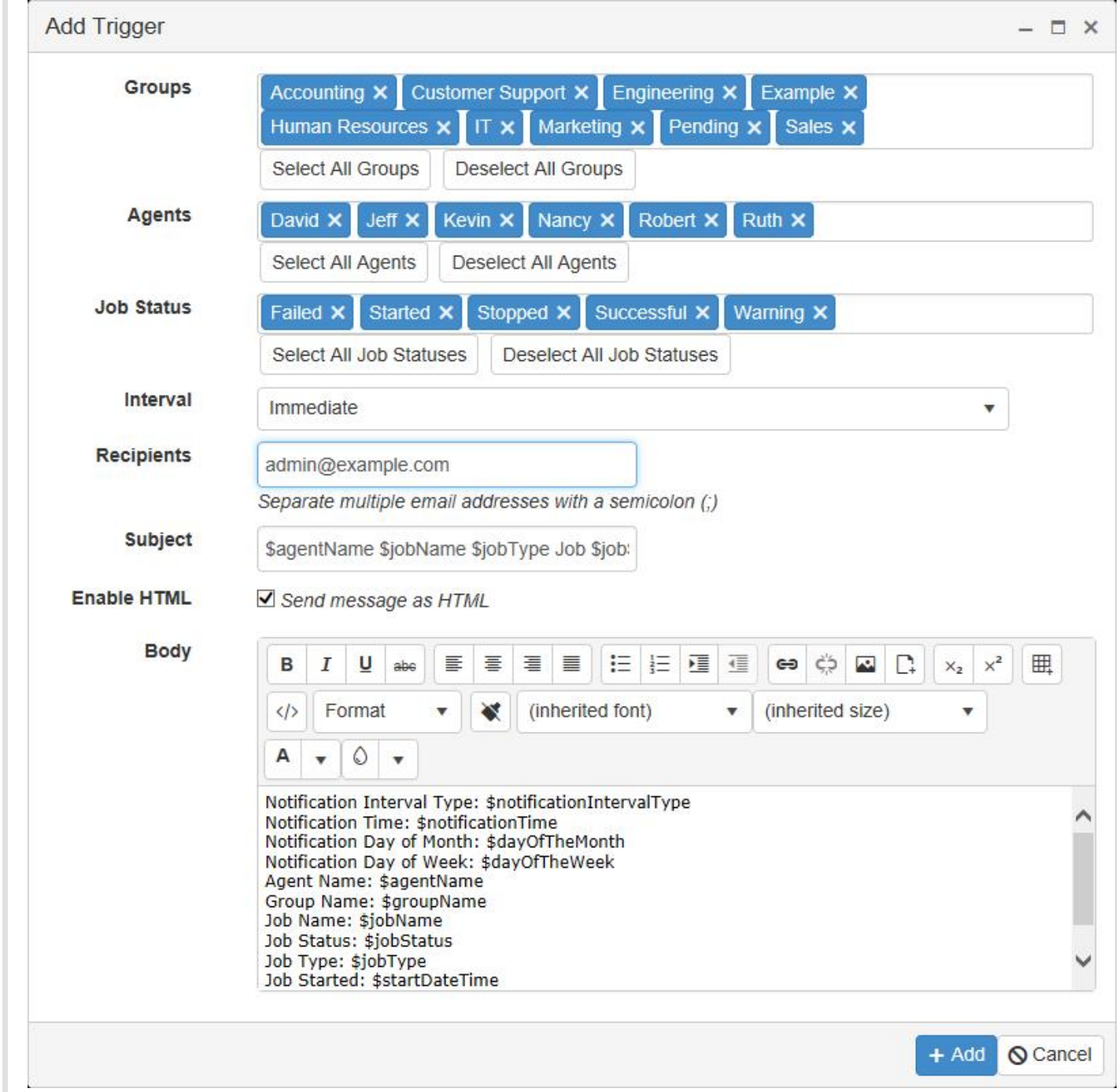
View Jobs Logs

Notification Triggers

A **Notification Trigger** is an e-mail notification for selected groups of agents on an interval basis. A single trigger can be created for an entire group of agents. The notification will be an e-mail sent to the e-mail addresses specified in the trigger configuration. The current triggers are shown in the "Notification > Triggers" page.



When creating a **New Trigger** , you are asked some questions including the agents and groups that will be included in the notification. The " **Notification Interval** " choices are Daily, Weekly, Monthly and Immediate. You can set a custom subject, message text, etc. When done configuring click the Add button.



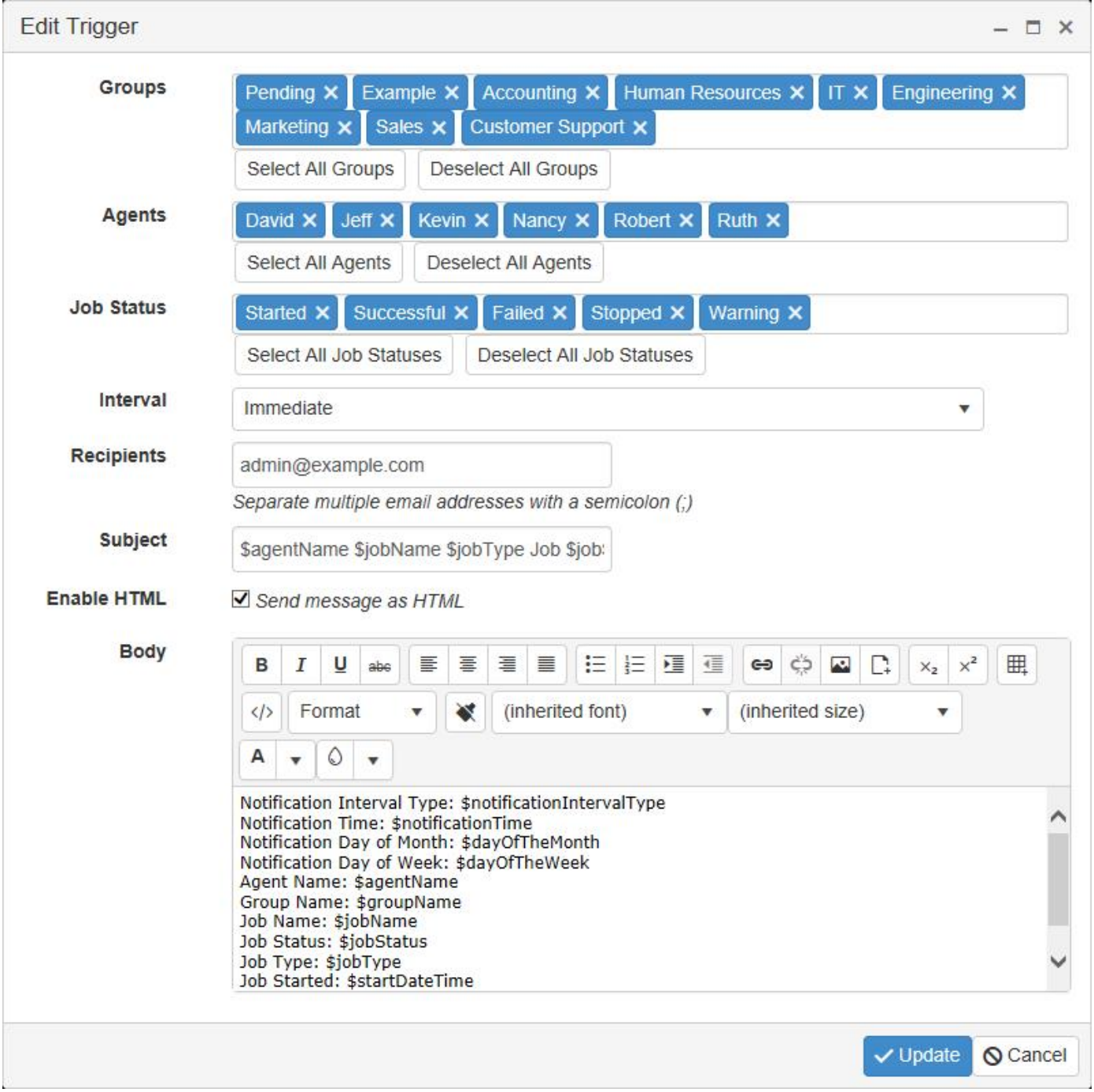
Once a **New Trigger** is added you can "**View**" or "**Delete**" the existing trigger by clicking on the buttons on the right-side of the screen in the Action column. To **Edit** you can click the **View** button.

The following custom email substitution variables can be used in the subject and body of the notification email.

Variable	Description	Examples
$notificationIntervalType	The notification interval type name.	Daily Weekly Monthly Immediate
$notificationTime	The notification time in the format *hh:mm:ss tt* as specified for a Daily interval.	07:34:55 PM

$dayOfTheMonth	The notification day of the month as specified for a Monthly interval.	15
$dayOfTheWeek	The notification day of the week as specified for a Weekly interval.	Sunday
$agentName	The agent friendly name for which the job was run on.	agent1
$groupName	The group name of the agent for which the job was run on.	group1
$jobName	The name of the job that ran.	job1
$jobStatus	The status of the job at the time of the notification.	Started Successful Failed Stopped Warning
$jobType	The type of the job.	Backup Restore Copy Import Image Backup Virtual Machine File Level Backup Virtual Machine Replication Backup Virtual Machine File Level Restore
$startDateTime	The time the job started.	6/15/2016 7:47:34 PM
$endDateTime	The time the job finished. If the job has not finished yet, the value will be empty.	6/15/2016 7:54:13 PM
$backupClientVersionNumber	The backup client version number.	18.0.1813.1

Example:



PERMISSIONS REQUIRED

View Alerts

Edit Alerts

Account Management

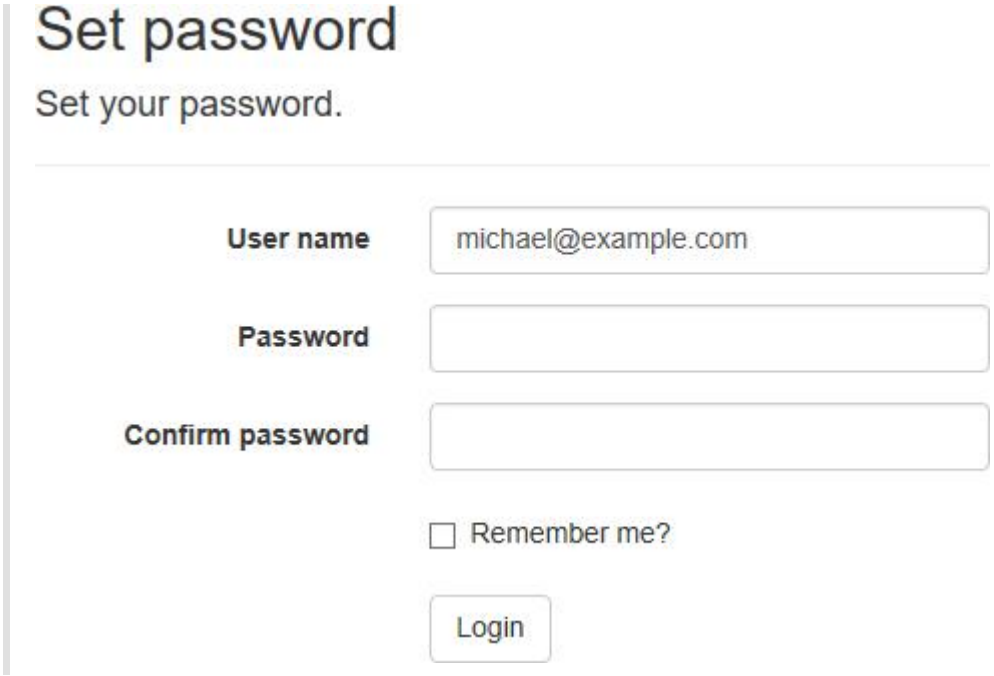
To manage the currently logged in user account, click on the username in the navigation menu.

The account management page provides the ability to change the following:

- Password
- Time zone
- Language

Set Password

New users created without a password must set their password from the "Set Password" page using the link provided in the user registration email.

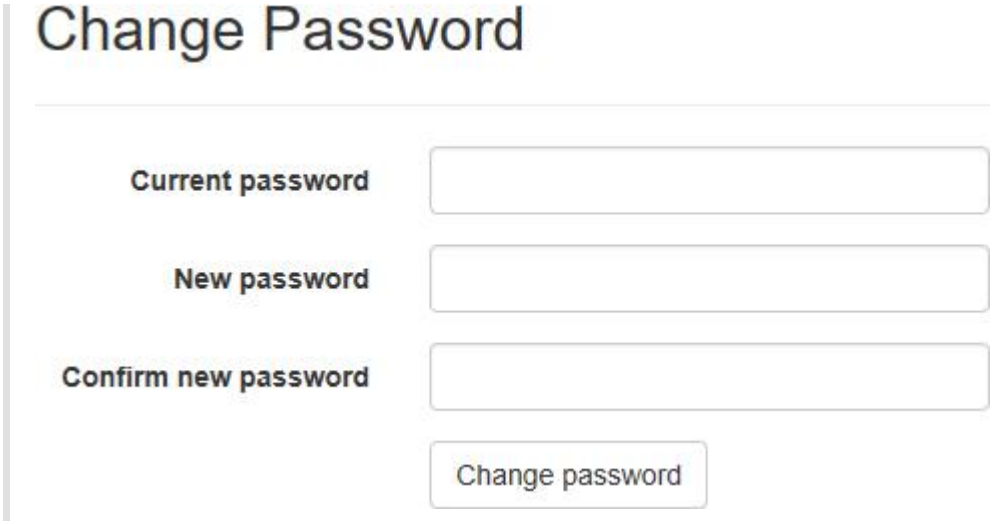


After setting their password, they'll be logged in.

If the "Remember me?" check box is checked, a cookie will be created which allows the user to remain logged in for up to 7 days of inactivity by default.

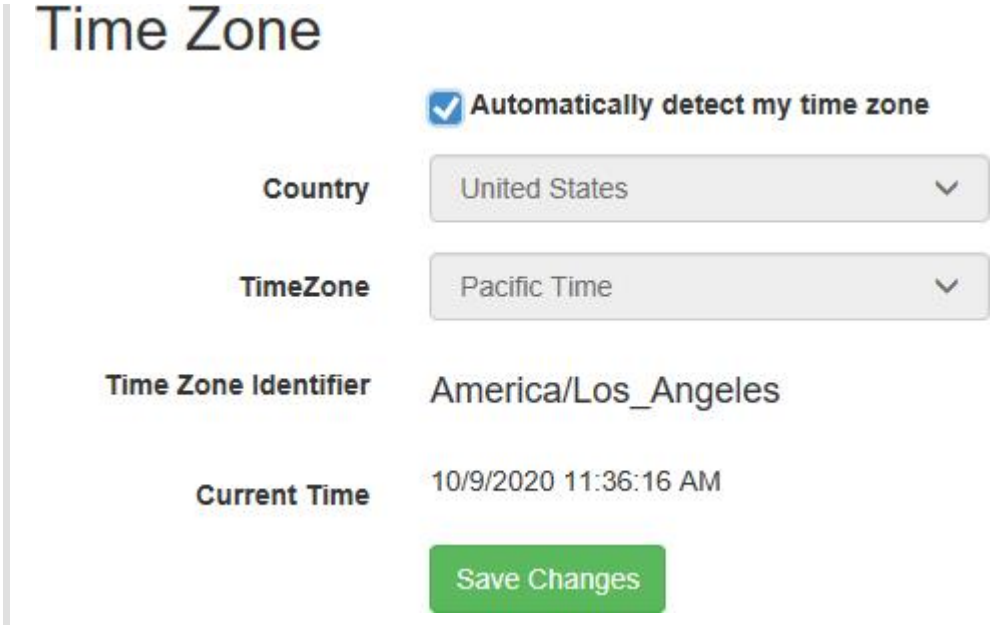
Password

The password for the currently logged in user can be changed from the "Change Password" page.



Time Zone

The date and time for the currently logged in user can be changed from the "Time Zone" page.



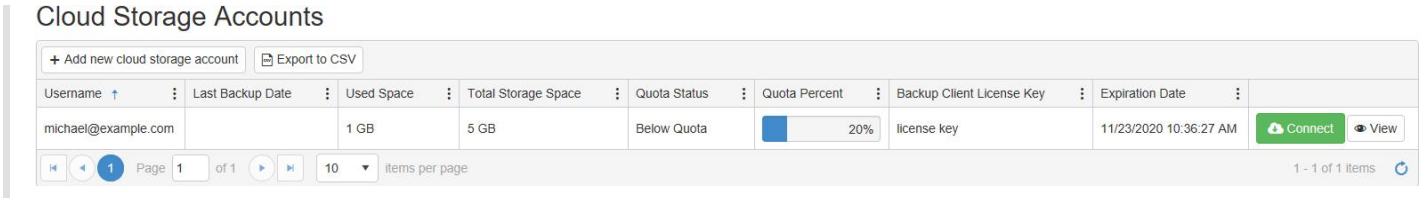
Language and Culture

The format dates, times, and numerals are displayed for the currently logged in user can be changed from the "Language and Culture" page.

Cloud Storage Accounts

The "Cloud Storage Accounts" view allows users to manage their cloud storage accounts.

The administrator must add a Storage Server in order for users to create cloud storage accounts.



Columns are dynamically displayed depending on the width of the browser window.

The column menus can be used to sort, show and hide columns, and filter the data.

The "Free Space" column is hidden by default.

The "Quota Percent" will turn from blue to orange when the account is near quota, and red when at or over quota. If there's no quota on the account, the percentage bar isn't displayed.

The "Expiration Date" field displays the closest expiration date for the license or its upgrade subscription, if a license key was used to create the account.

The "Days Until Expiration" will start as orange and fill up when there are 45 or less number of days until the license expires, and red when there are 14 or less. If the license doesn't expire, the countdown timer bar is not displayed.

Users can click on the "Export to CSV" button to create a comma-separated values (CSV) file containing the list of cloud storage accounts in all pages, sorted, and filtered as the current view.

The exported CSV file will contain the following columns:

COLUMN NAME	DESCRIPTION
GroupName	The name of the storage server group.
Username	The username in the storage server.
BackupClientLicenseKey	The backup client license key.
LastBackupDate	The date and time of the last backup in UTC.
UsedBytes	The amount of storage space used in bytes.
FreeBytes	The amount of storage space remaining in bytes.

COLUMN NAME	DESCRIPTION
QuotaBytes	The total amount of storage space available in bytes.
Enabled	Indicates whether or not the cloud storage account is enabled.
AccountStatus	The account status. ("Active", "Deleted", or "Pending")
NumberOfComputers	The number of computers.
QuotaStatus	The quota status. ("NONE", "BELOW", "NEAR", "AT", or "OVER")
QuotaPercent	The amount of used space as a percentage of the quota.
ExpirationDate	The backup client license's expiration date in UTC.
DaysUntilExpiration	The number of days until the backup client license's expiration date.
LicenseStatus	The status of the license in the storage server. ("Normal" or "Evaluation")

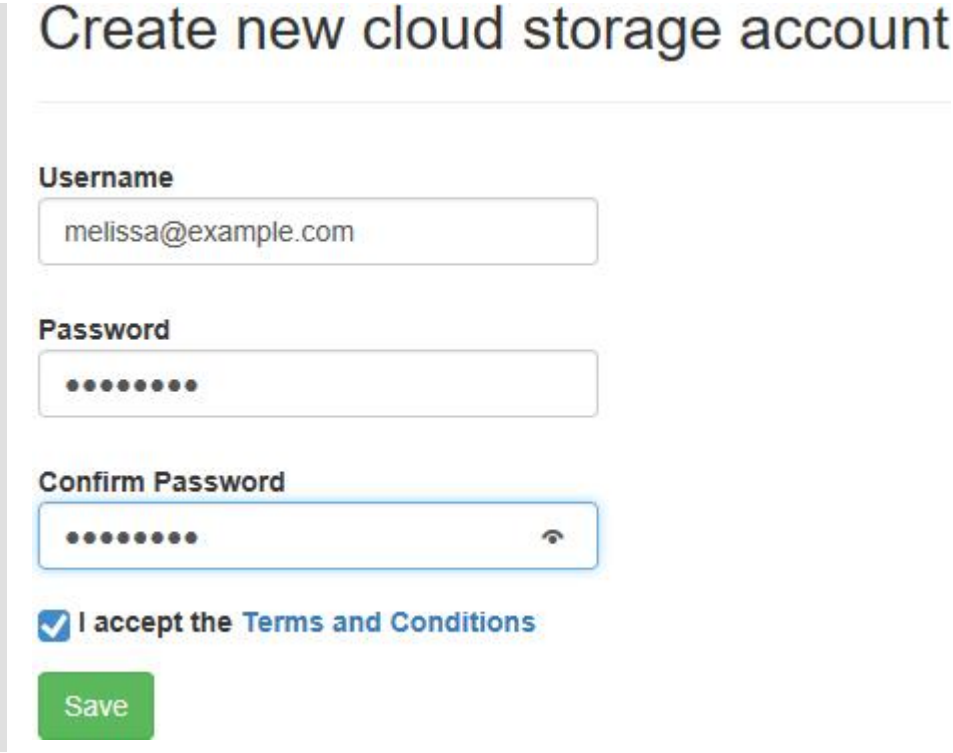
PERMISSIONS REQUIRED

View Cloud Storage Accounts

Create an account

From the "Cloud Storage Accounts" view, click on the "Add new cloud storage account" button to create a new cloud storage account.

Enter a username, password, and click the "Save" button to create a new cloud storage account.

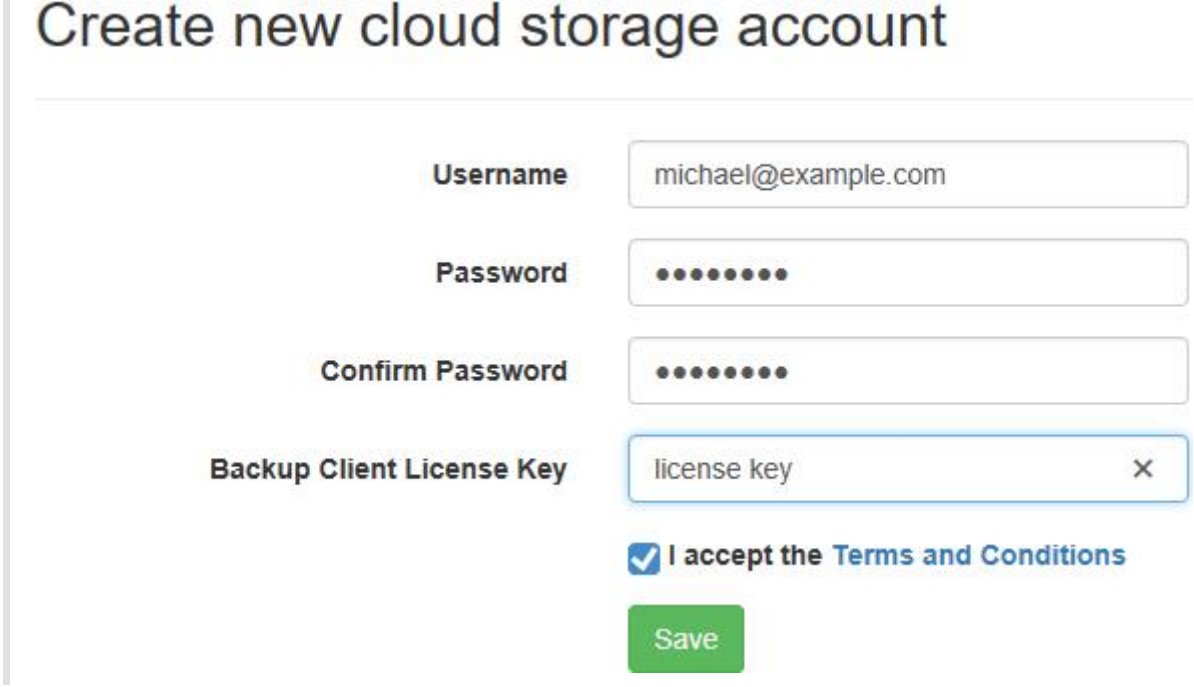


The username must be unique.

A new "Cloud Storage" device will automatically be added to the backup client when the user signs up inside the embedded web browser of the backup client, or re-connects to an existing cloud storage account.

When re-connecting to an existing cloud storage account, the user will be asked for their cloud storage account password if it's different then their user account password.

A backup client license key may be required to create a cloud storage account.



In this case, if the backup client license is disabled, expired, doesn't support cloud storage, or if it has an expired upgrade subscription, it can't be used to create a cloud storage account.

The backup client license key will be automatically populated if the user is signing up inside the embedded web browser of the backup client.

PERMISSIONS REQUIRED

Edit Cloud Storage Accounts

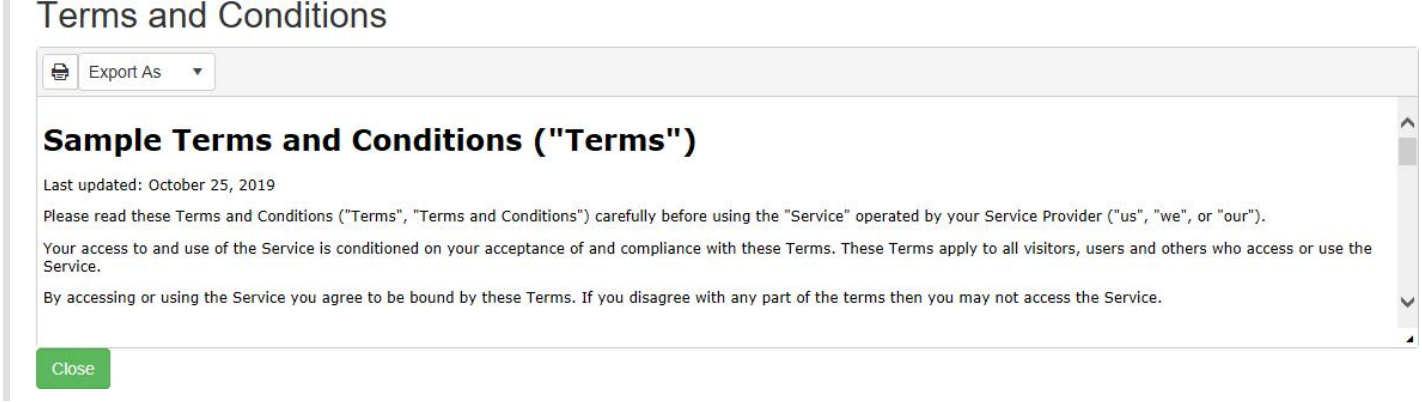
Terms and Conditions

Acceptance of the terms and conditions may be required.

The "Terms and Conditions" hyperlink will open a new window.

The new window displays the Terms and Conditions with options to print and save as a file in a different format.

The terms and conditions can be exported as a Microsoft Office Open XML Format word processing document (DOCX), Rich Text Format (RTF), Adobe Portable Document Format (PDF), HyperText Markup Language (HTML), and plain text (txt).



Related topics:

Add a storage server

User registration and creating a cloud storage account in one step

Connect to an account

The embedded web browser dialog from within the backup client must be used in order to successfully connect to a cloud storage account.

The embedded web browser dialog can be launched from either the "Home" or the "Device" tabs.

From the "Home" tab, click on the "Cloud Backup" button.

From the "Device" tab, click on the "Click HERE to add an online device" list item.

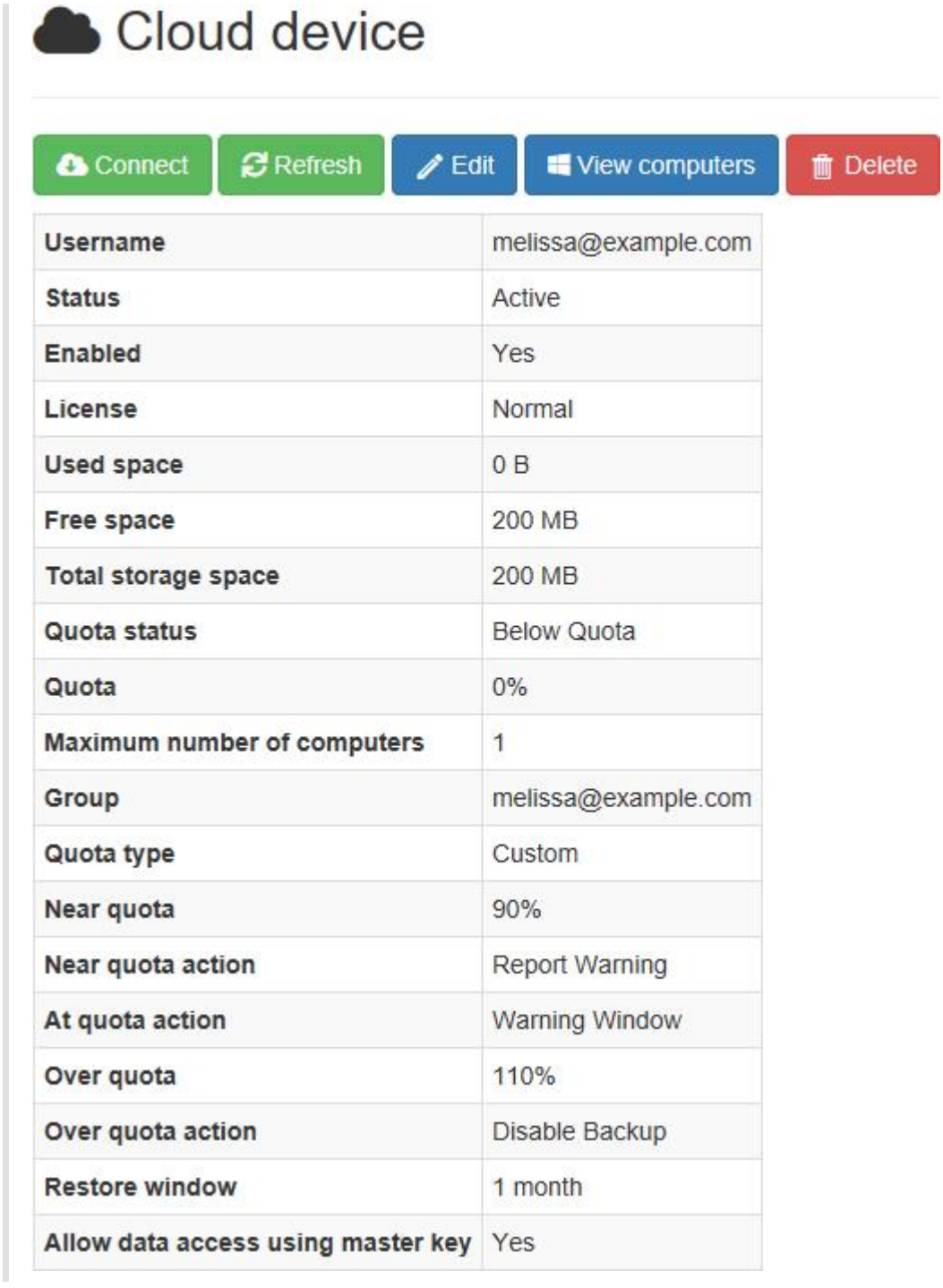
If a cloud storage account has already been added, the web browser dialog will not be displayed.

PERMISSIONS REQUIRED

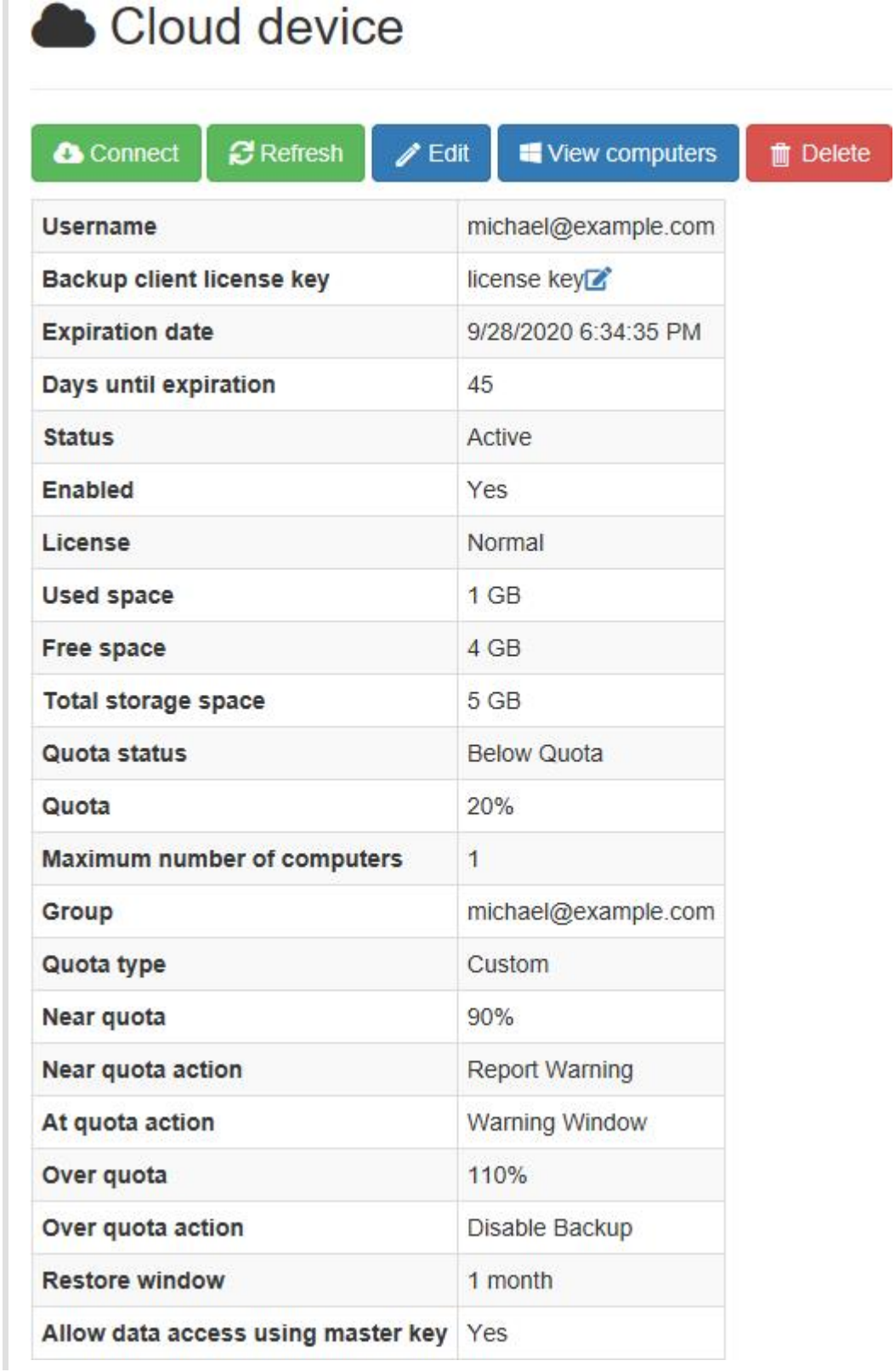
View Cloud Storage Accounts

View details of an account

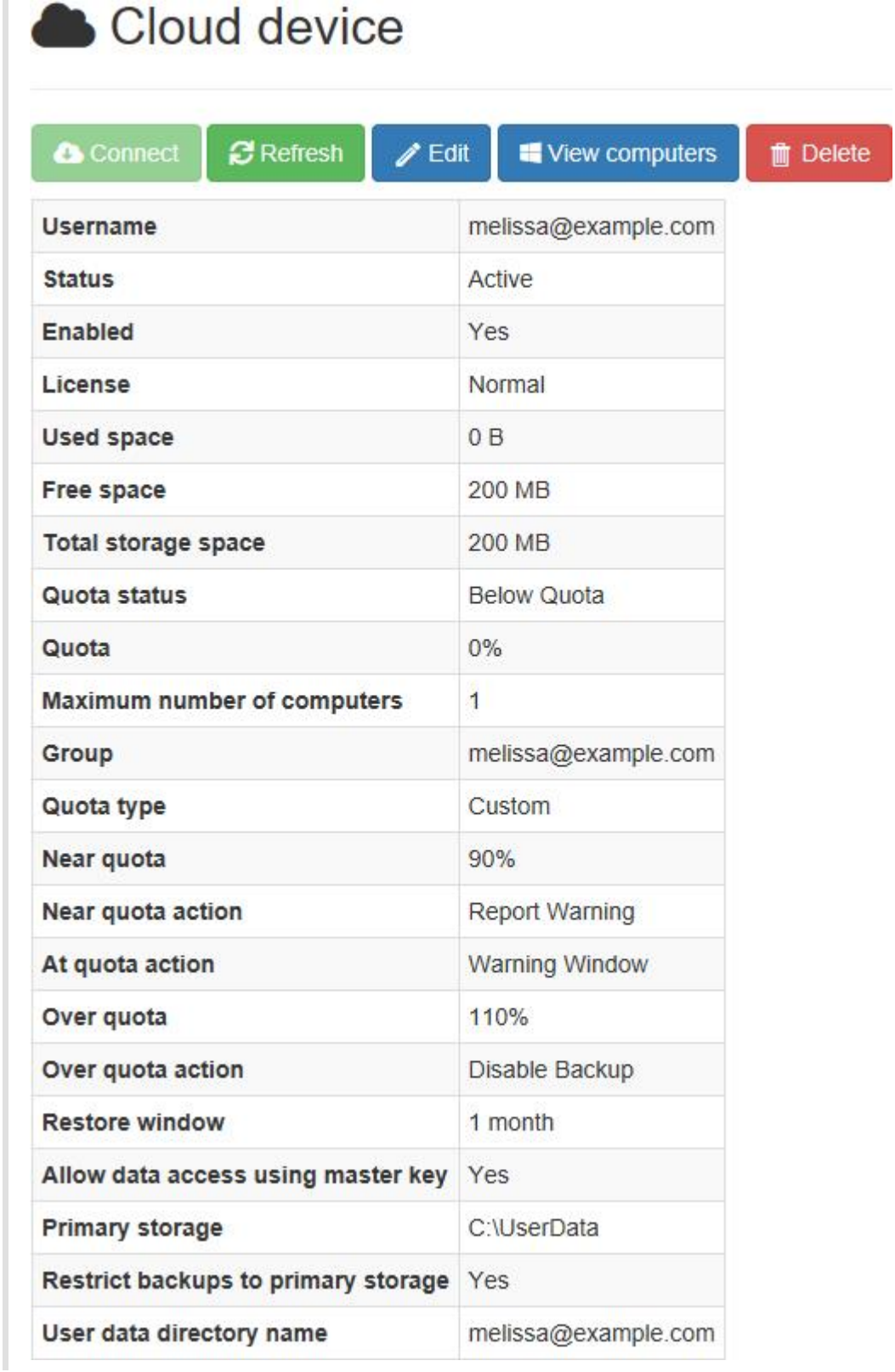
From the "Cloud Storage Accounts" view, click on the "View" button next to the cloud storage account to view its details.



If a cloud storage account has a license key, it's also displayed.



The administrator has the ability to view more details on the account.



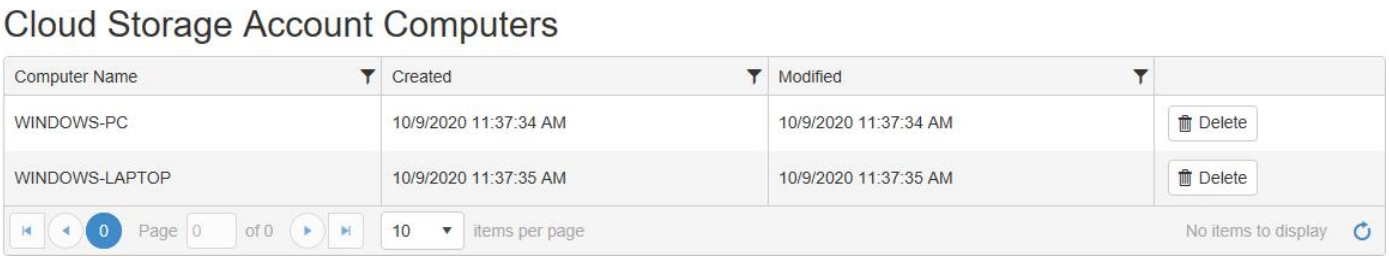
The administrator doesn't have the ability to connect to a cloud storage account of another user.

PERMISSIONS REQUIRED

View Cloud Storage Accounts

View computers

From the cloud storage account details view, click on the "View computers" button to view the computers attached to the cloud storage account.



PERMISSIONS REQUIRED

View Cloud Storage Accounts

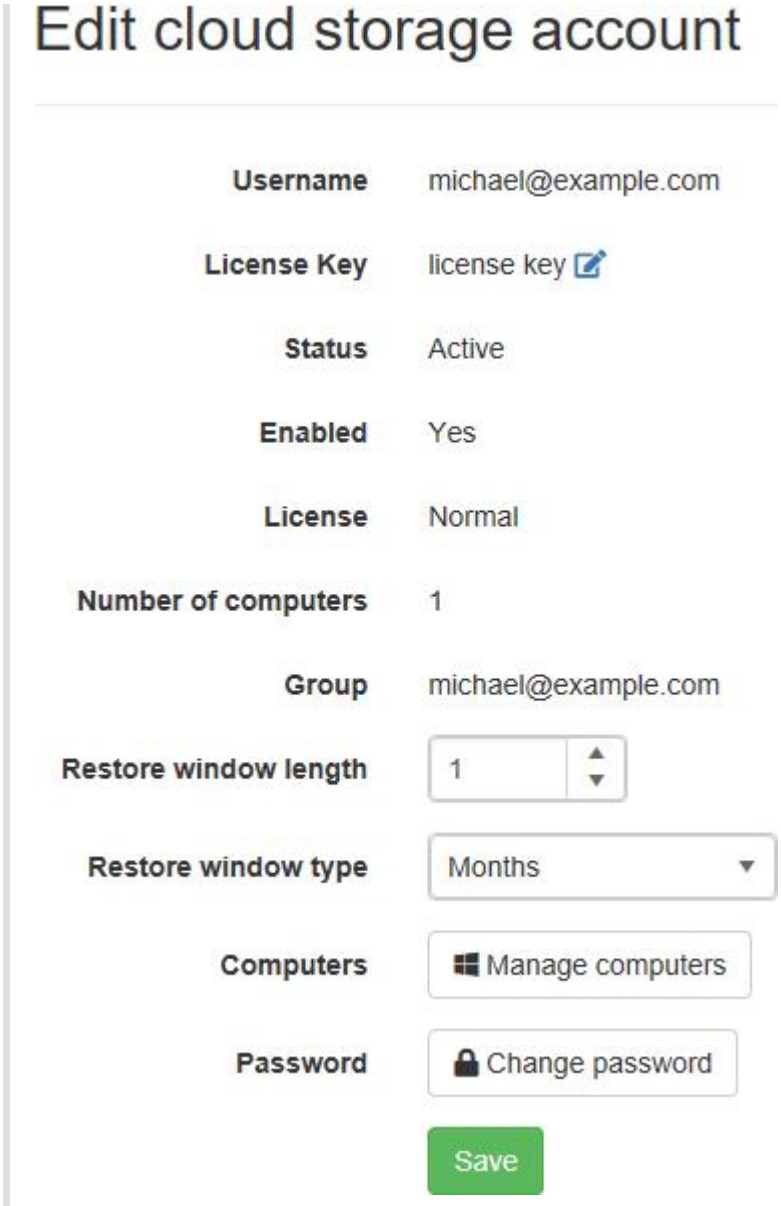
Edit cloud storage account

From the cloud storage account details view, click on the "Edit" button.

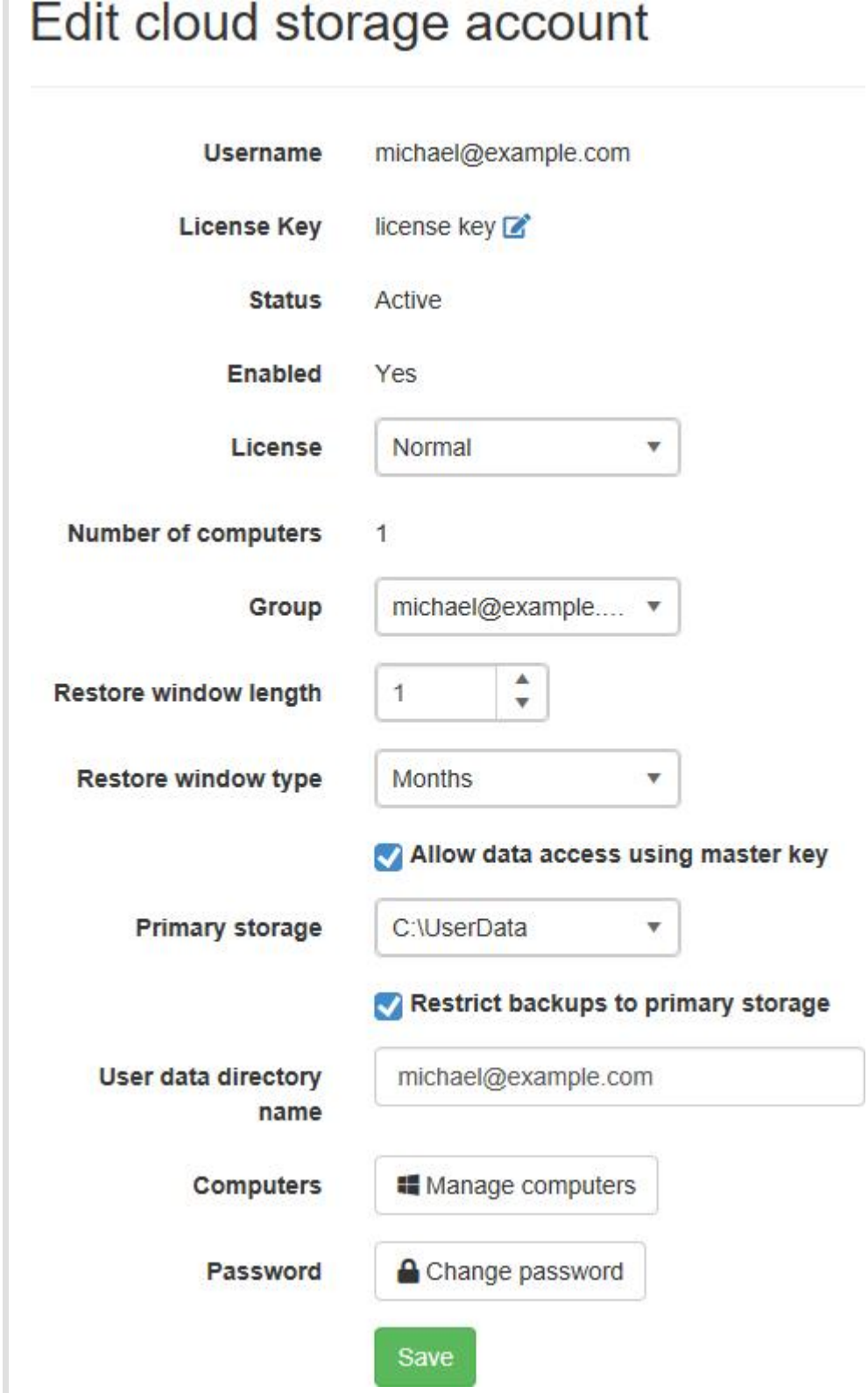
The editable fields depend on whether or not a license key is required and also the role of the logged in user.

License key is required

If a license key is required for the cloud storage account, only the license key and restore window can be modified. This is because the quota and the number of computers are retrieved from the license server.

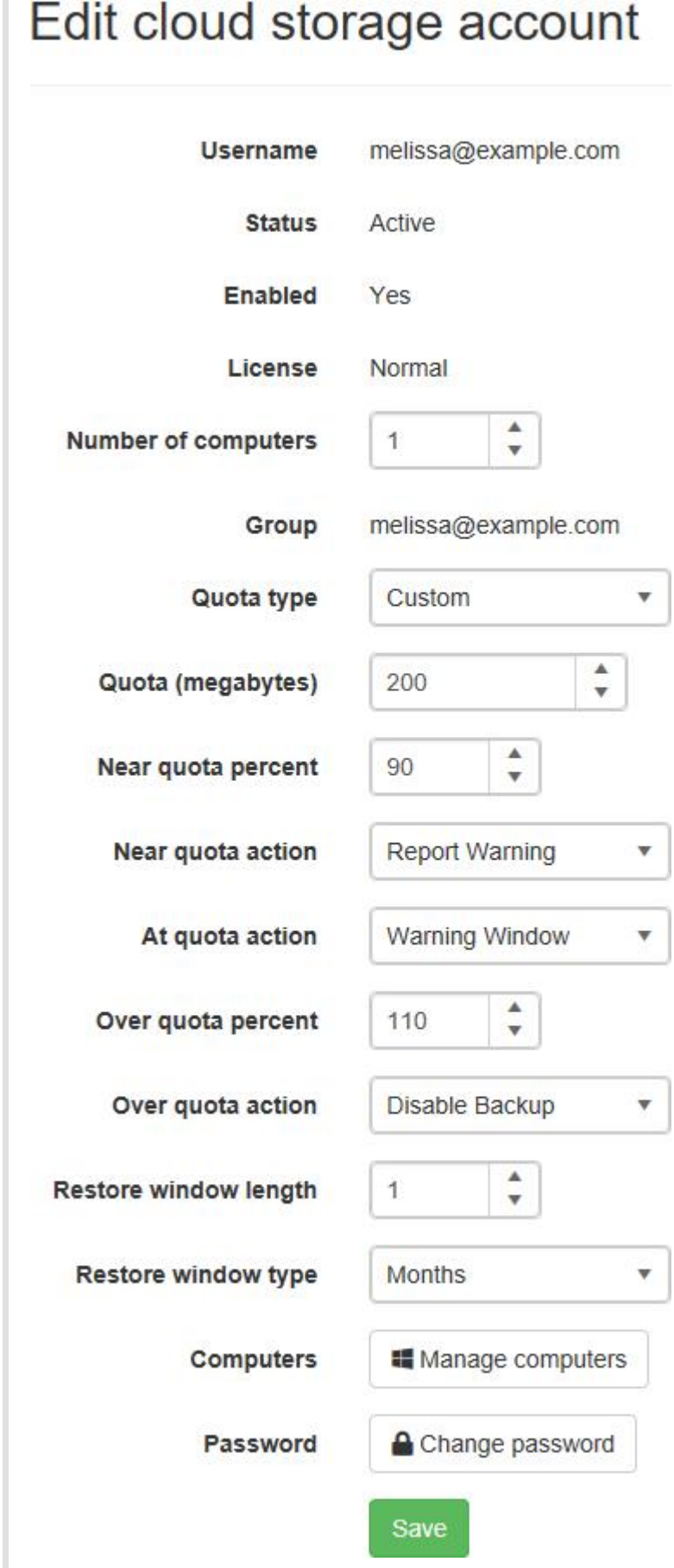


The administrator can also modify the "License status", storage server group, master key access, primary storage, and user data directory fields of the cloud storage account.



License key not required

If a license key is not required for the cloud storage account, the number of computers, quota, and restore window fields can be modified.



The administrator can also modify the "Account status", "Enabled", "License status", storage server group, master key access, primary storage, and user data directory fields of the cloud storage account.

Edit cloud storage account

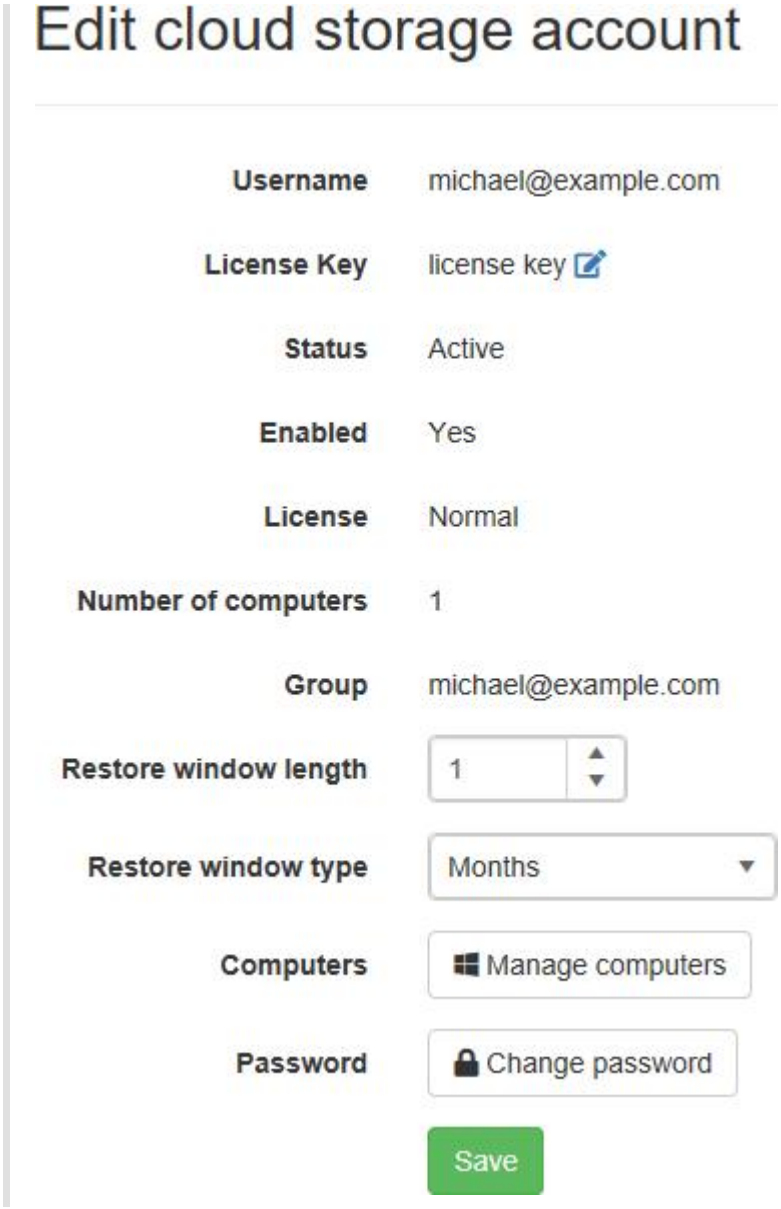
Username	melissa@example.com
Status	Active
	Enabled
License	Normal
Number of computers	1
Group	melissa@example....
Quota type	Custom
Quota (megabytes)	200
Near quota percent	90
Near quota action	Report Warning
At quota action	Warning Window
Over quota percent	110
Over quota action	Disable Backup
Restore window length	1
Restore window type	Months
	Allow data access using master key
Primary storage	C:\UserData
	Restrict backups to primary storage
User data directory name	melissa@example.com
Computers	Manage computers
Password	Change password
	Save

 PERMISSIONS REQUIRED

Edit Cloud Storage Accounts

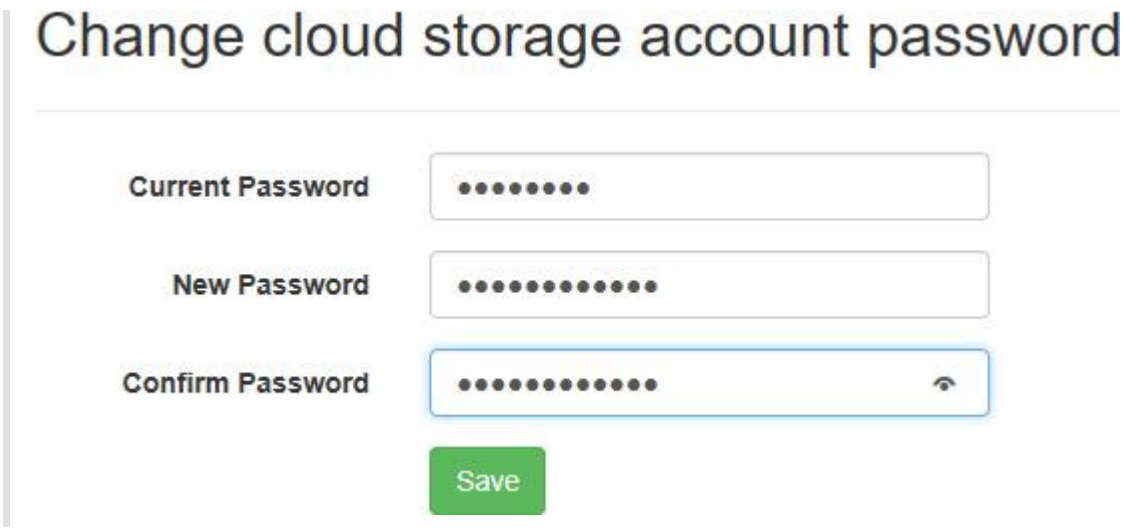
Change the password

From the cloud storage account details view, click on the "Edit" button.



Click on the "Change password" button.

Enter the current cloud storage account password, the new cloud storage account password, and click on "Save" to continue.



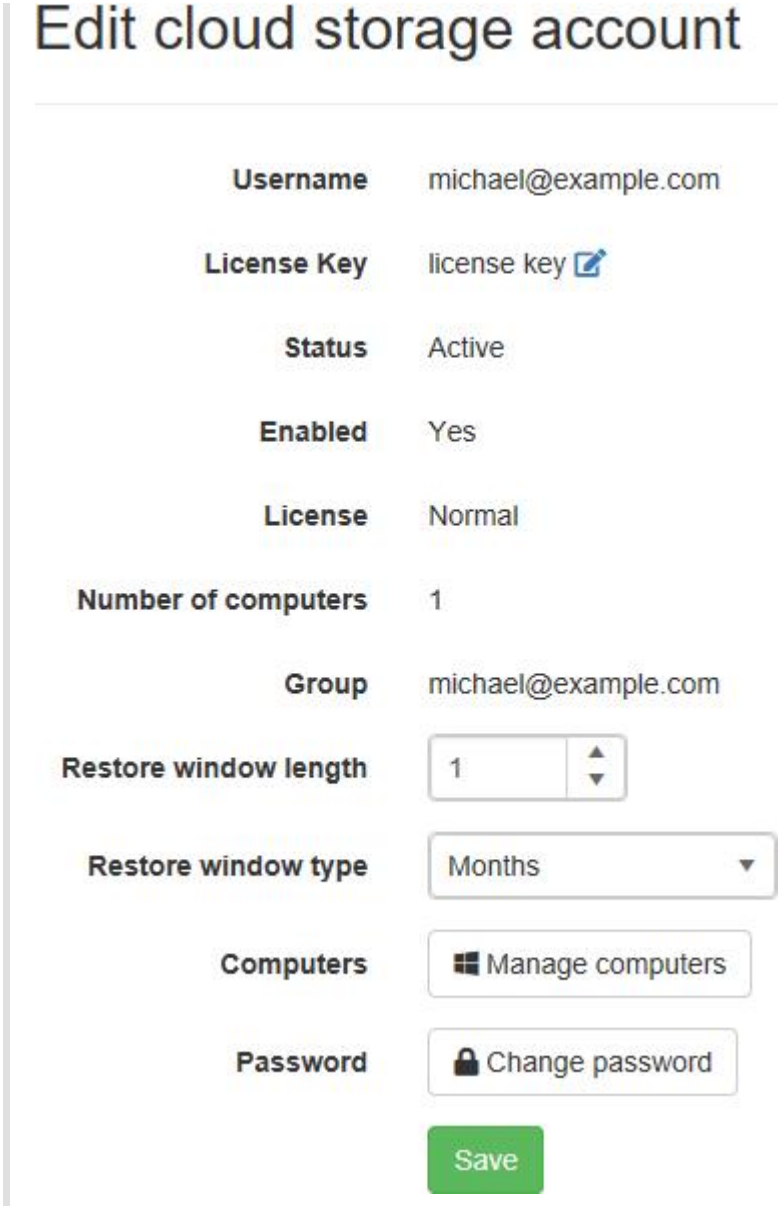
 PERMISSIONS REQUIRED

Edit Cloud Storage Accounts

Change the license key

The backup client license key can be changed only if one was used to create the cloud storage account.

From the cloud storage account details view, click on the "Edit" button.

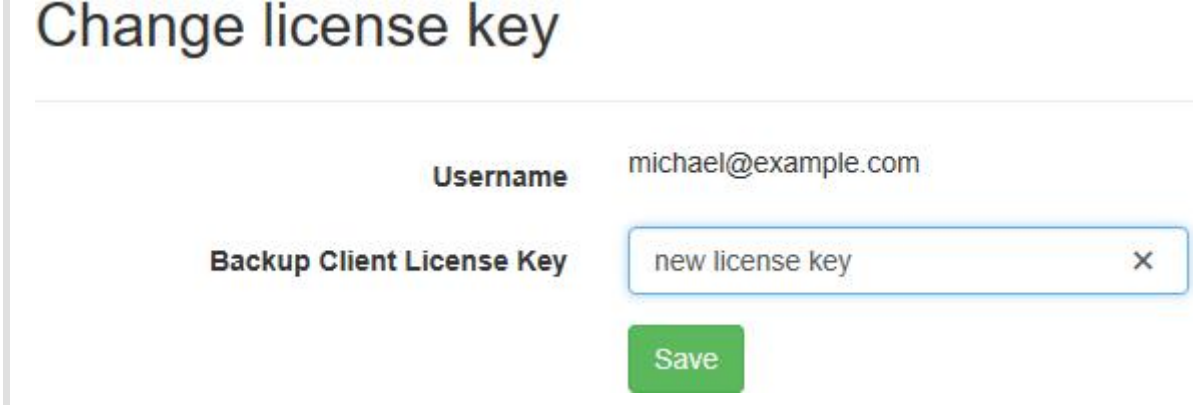


Click on the "Edit" icon next to the "License Key" field.

The "Edit" icon will not be displayed if a license key wasn't used to create the cloud storage account.

Enter the new backup client license key and click on "Save" to change the license key associated with the cloud storage account.

If the backup client license is disabled, expired, doesn't support cloud storage, or if it has an expired upgrade subscription, it can't be used as the new license key.



PERMISSIONS REQUIRED

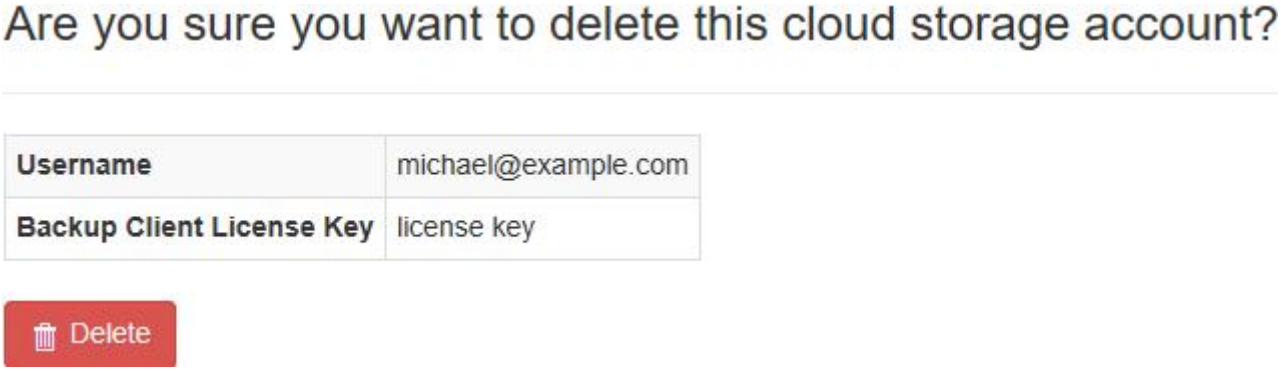
Edit Cloud Storage Accounts

Delete an account

To permanently delete your cloud storage account, and its associated data, from the cloud storage account details view, click on the "Delete" button.

The following page will allow you to confirm its deletion.

You will not be able to restore any data associated with the account after deleting it.



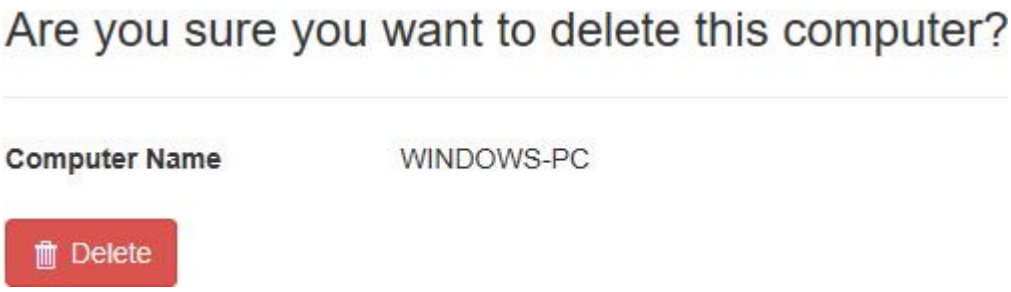
PERMISSIONS REQUIRED

Edit Cloud Storage Accounts

Delete a computer

To permanently delete a computer attached to the cloud storage account, and its associated data, from the "Cloud Storage Account Computers" view, click on the "Delete" button next to the computer. The following page will allow you to confirm its deletion.

You will not be able to restore any data associated with the computer after deleting it.



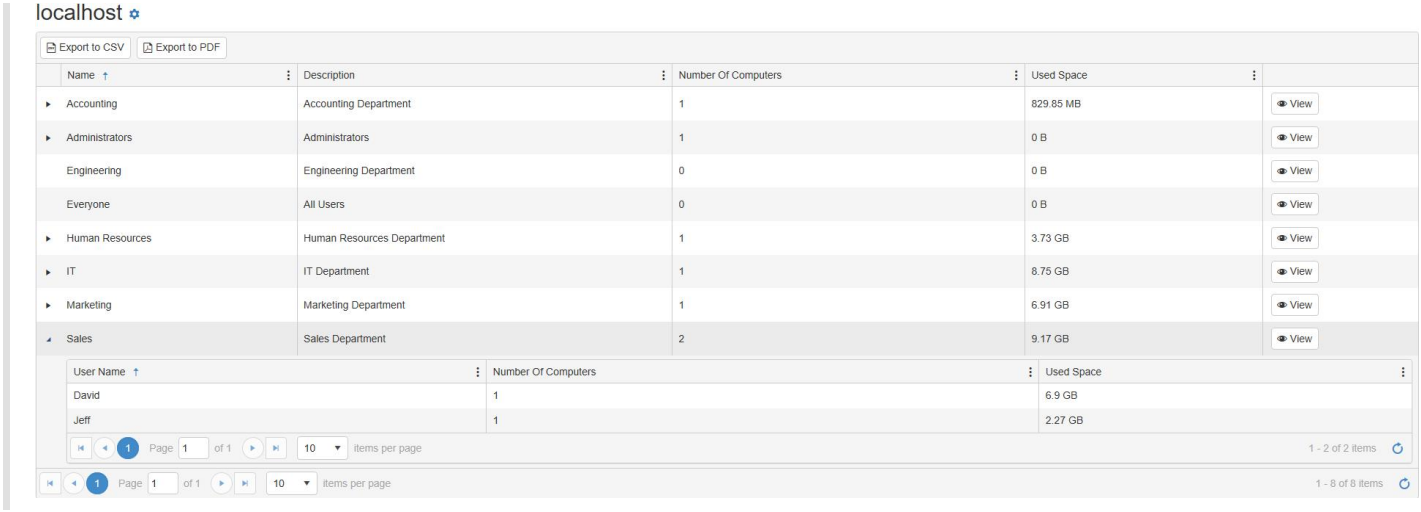
PERMISSIONS REQUIRED

Edit Cloud Storage Accounts

Storage Server

The "Storage Server" view allows an administrator to view NovaBACKUP Storage Server groups and users.

The administrator must first add a Storage Server.



The column menus can be used to sort, show and hide columns, and filter the data.

The "Status", "Quota Setting", "Quota", "Number Of Users", and "Used Gigabytes" columns are hidden by default.

Users can click on the "Export to CSV" button to create a comma-separated values (CSV) file containing the list of all storage server groups without users.

Users can click on the "Export to PDF" button to create a Portable Document Format (PDF) file containing the list of all storage server groups without users.

The exported file will contain the following columns:

COLUMN NAME	DESCRIPTION
Name	The name of the storage server group.
Description	The description of the storage server group.
NumberOfUsers	The number of users in the storage server group.
NumberOfComputers	The total number of computers in the storage server group.
UsedGigabytes	The amount of storage space used in gigabytes.

□ PERMISSIONS REQUIRED

One of the following permissions is required:

View Storage Server Groups

Edit Storage Server Groups

Settings

Security

Agent

Notification

Users

User Registration Settings

Roles

Storage Servers

Web Hook

Update

Application

Agent Settings

The Agent Settings page allows you to configure the timeout and ping interval for agent connections.

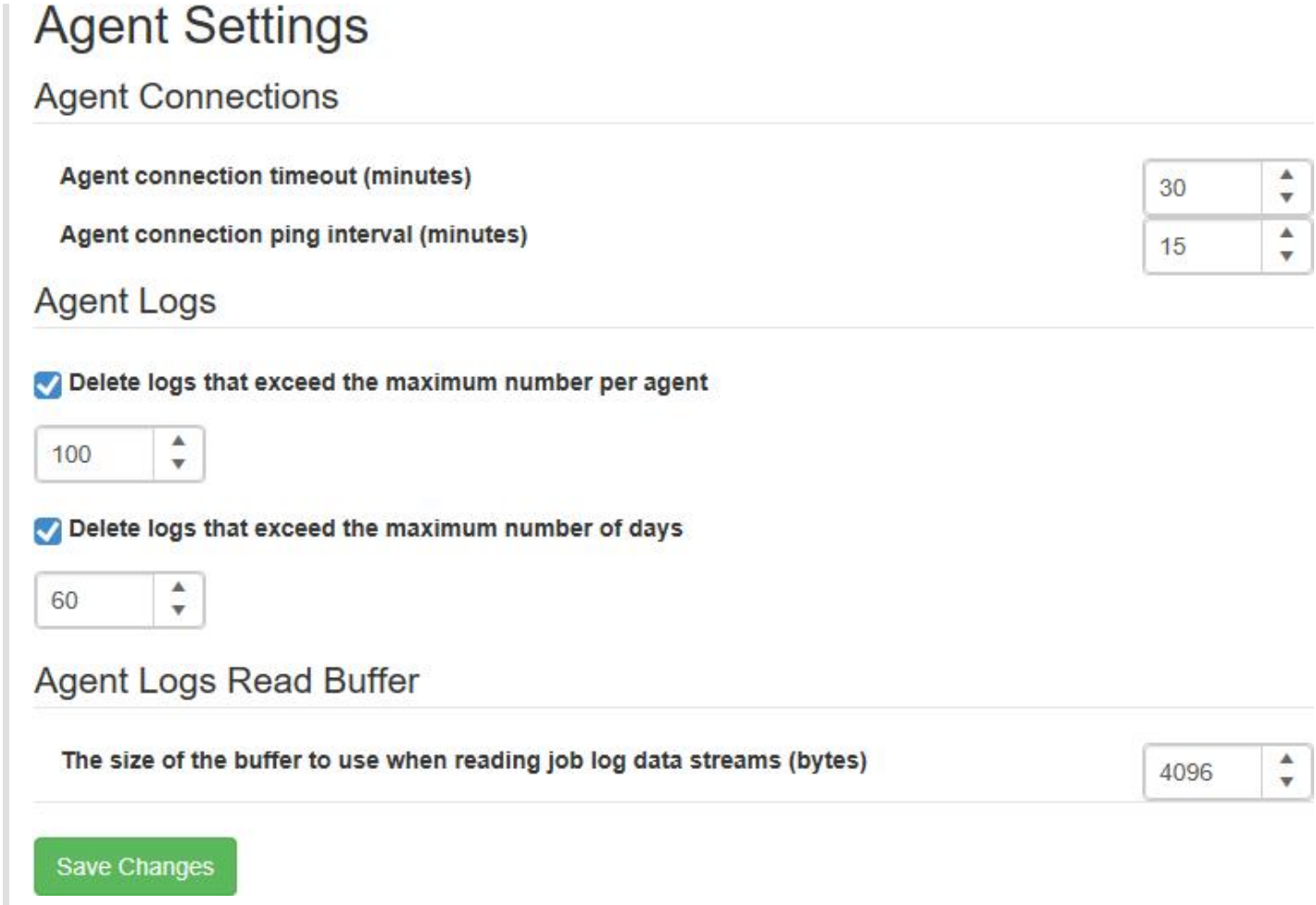
It also allows you to configure the maximum number of logs per agent and the time old logs are purged from the database.

When using the SQLite database provider:

- The buffer size on the server used when reading log files streamed from the client is configurable on this page.
- The maximum log file size that can be stored in the database is around 1GB.

When using the Microsoft SQL Server database provider:

- The maximum log file size that can be stored in the database is around 2GB.



PERMISSIONS REQUIRED

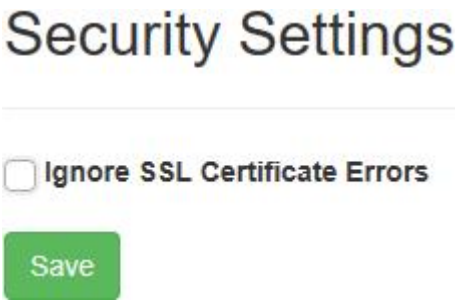
View Settings

Edit Settings

Security Settings

The "Security Settings" view allows an administrator to ignore SSL certificate errors.

Ignoring SSL certificate errors is not recommend.



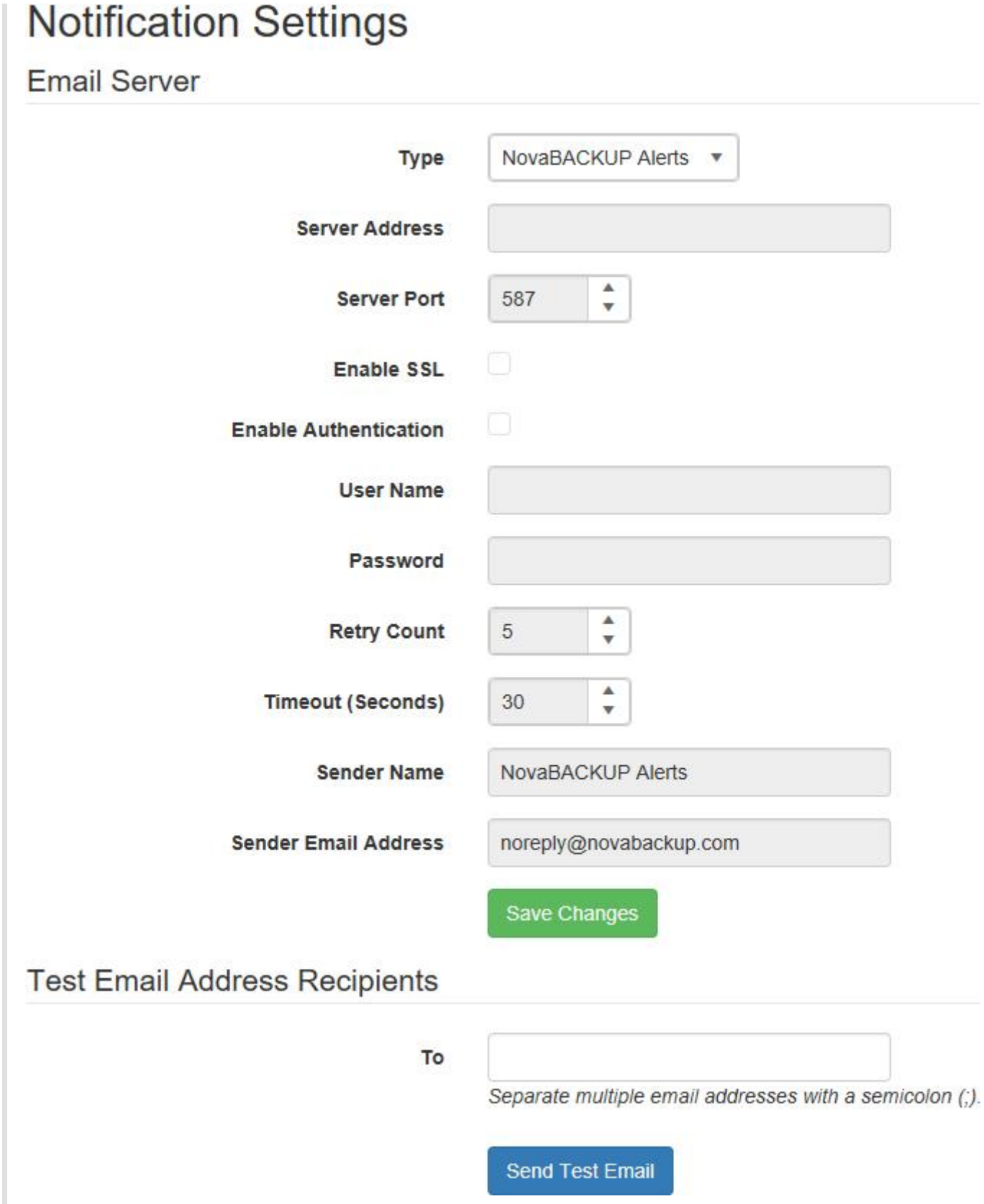
PERMISSIONS REQUIRED

View Settings

Edit Settings

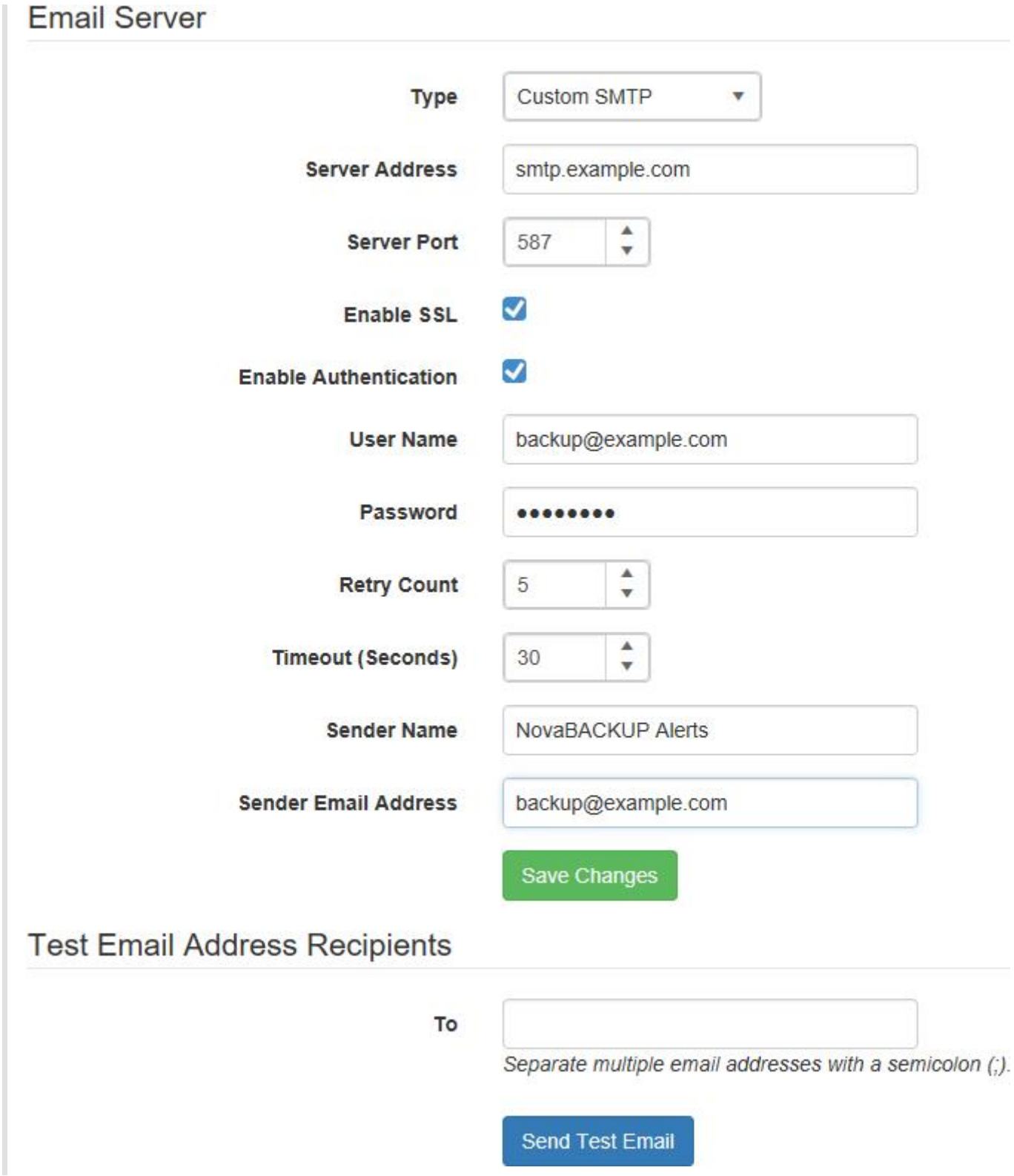
Notification Settings

To configure how the **Notification e-mails** are sent you, click on the "**Notification**" menu item under the "**Settings**" menu item. Notification e-mails are delivered **by default** via the built-in "NovaBACKUP Alerts" SMTP service.



You can also configure CMon to send Notifications using a "**Custom SMTP**" server. Make sure to fill in all of the details that are prompted for. Once the prompts are filled in click the " **Test Email Settings** "

button to verify all of the settings are correct prior to saving, otherwise your Notification e-mails will fail.



PERMISSIONS REQUIRED

View Settings

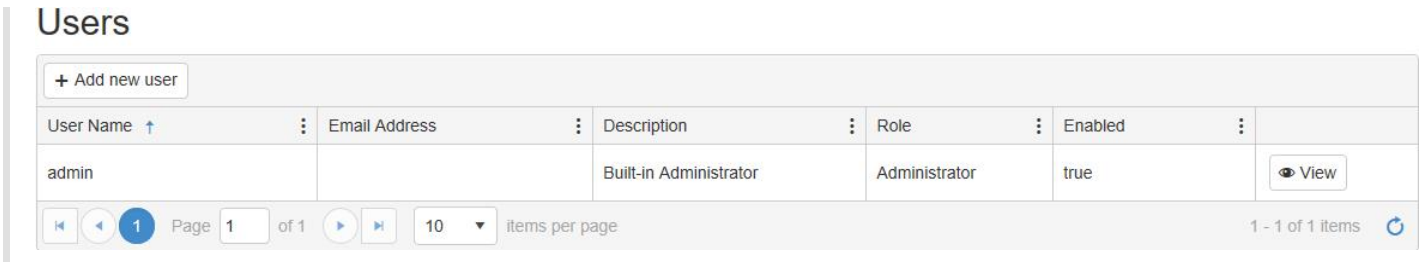
Edit Settings

Users

The "**Users**" page is where you can set up CMon to work with more than just the single built-in "admin" account. Once on the "**Users**" page you have the ability to add users by clicking on the "**Add new user**" button. Custom Roles can be created for users via the "**Roles**" page.

The column menus can be used to sort, show and hide columns, and filter the data.

The "Storage Server Group" column is hidden by default.



PERMISSIONS REQUIRED

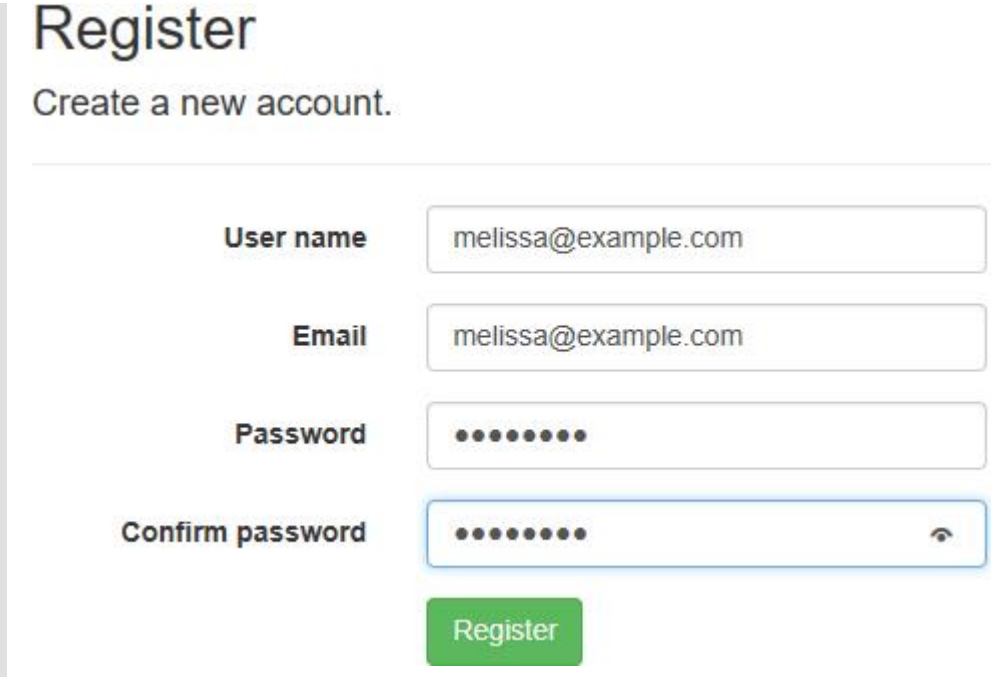
View Users

Edit Users

User registration

From the "Log in" view, click on the "Register" button to register for a new account.

Enter a username, password, email address, and click the "Register" button to continue.



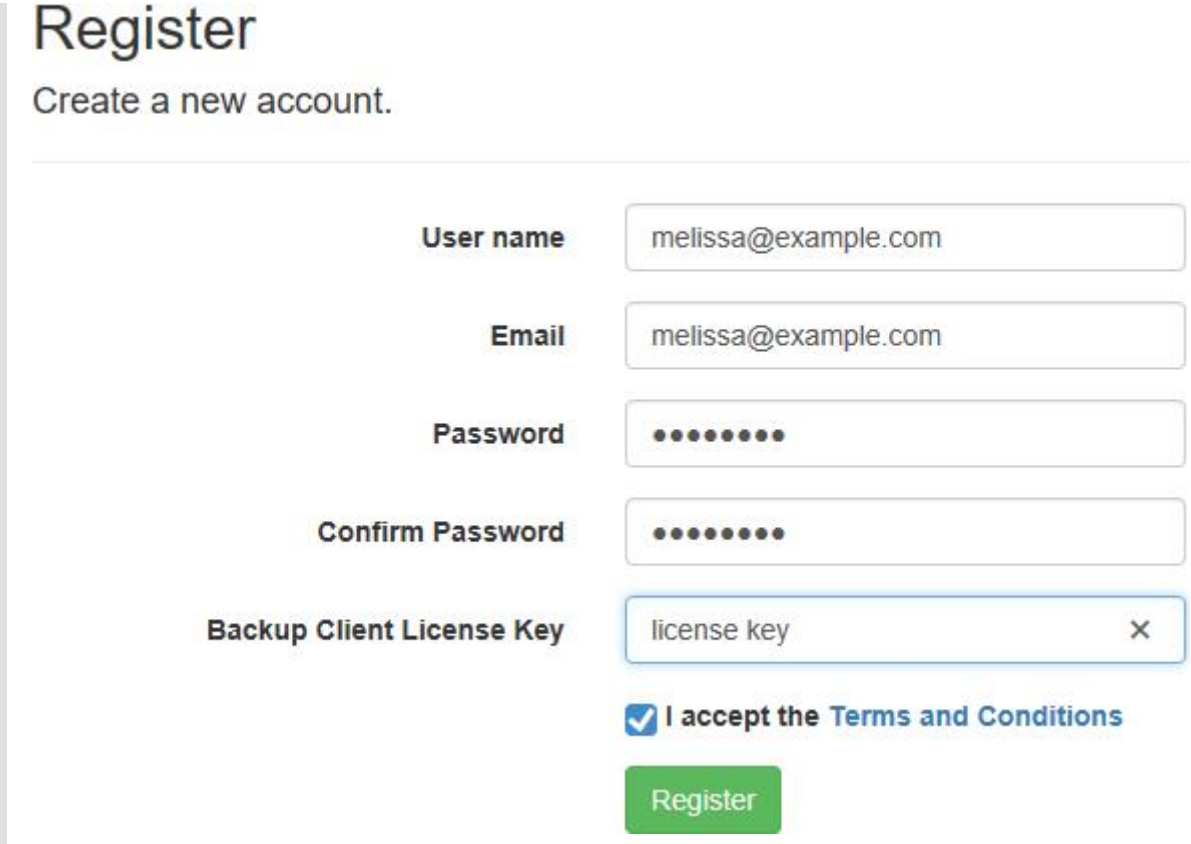
The username must be unique.

Related topics:

User registration settings
User registration and creating a cloud storage account in one step

User registration and creating a cloud storage account in one step

When using the embedded web browser dialog from within the backup client, clicking on the "Register" button from the "Log in" view displays a page allowing you to register for a new account and create a cloud storage account in one step.



Related topics:

User registration settings
User registration
Add a storage server
Create a cloud storage account

Create a user

From the "Users" view, click on the "Add new user" button to create a new user.

Enter a username, password, email address, select the user's role, and click the "Next" button to continue.

The username must be unique.

If a password is not specified, then the "User must set or change password at first login" and "Send registration email" check boxes must be checked.

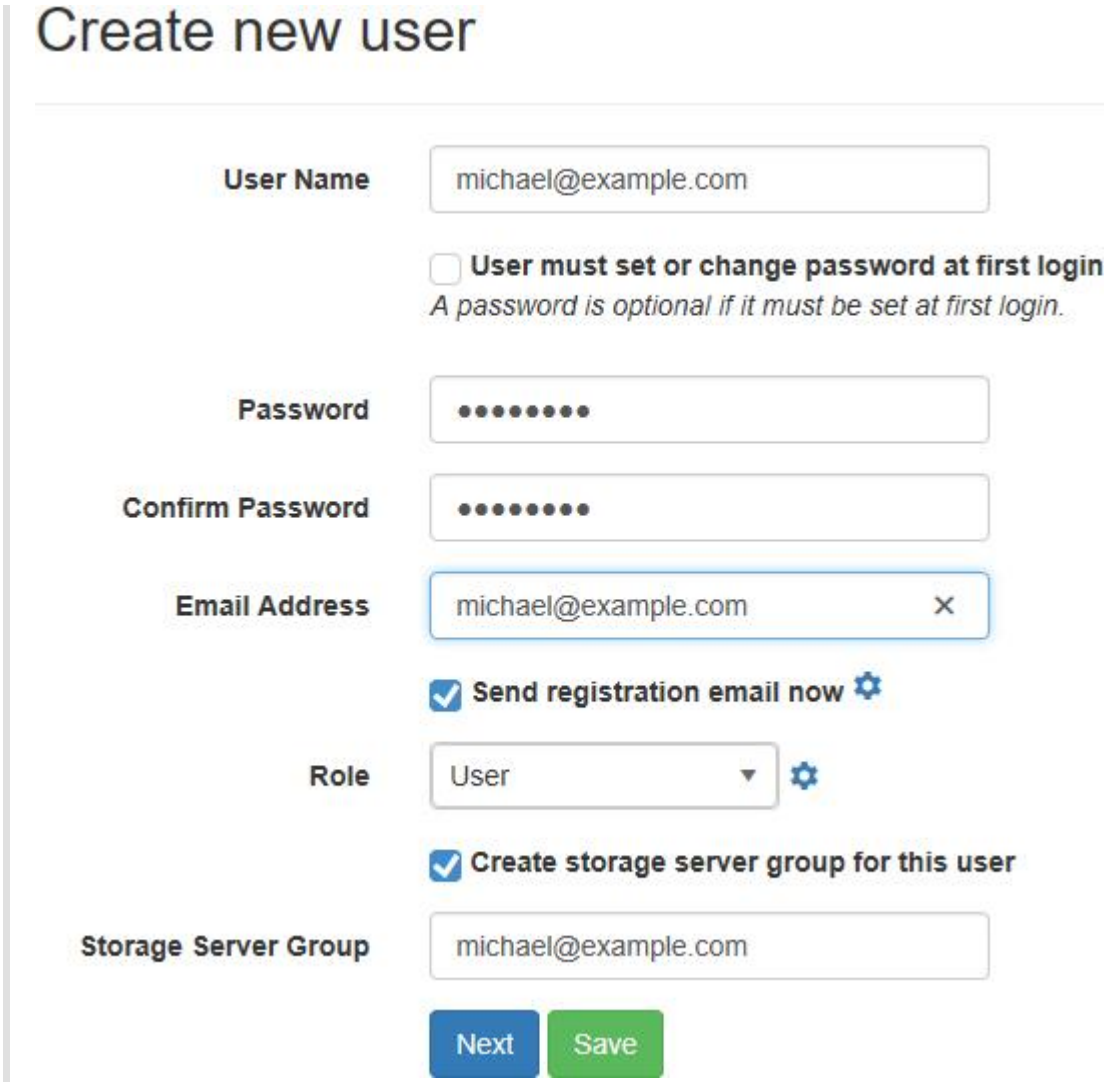
If a password is not specified, the user registration email will contain a link to the Set Password page, by default, to allow them to set their password.

The set password link contains a randomly generated token that expires after 30 days.

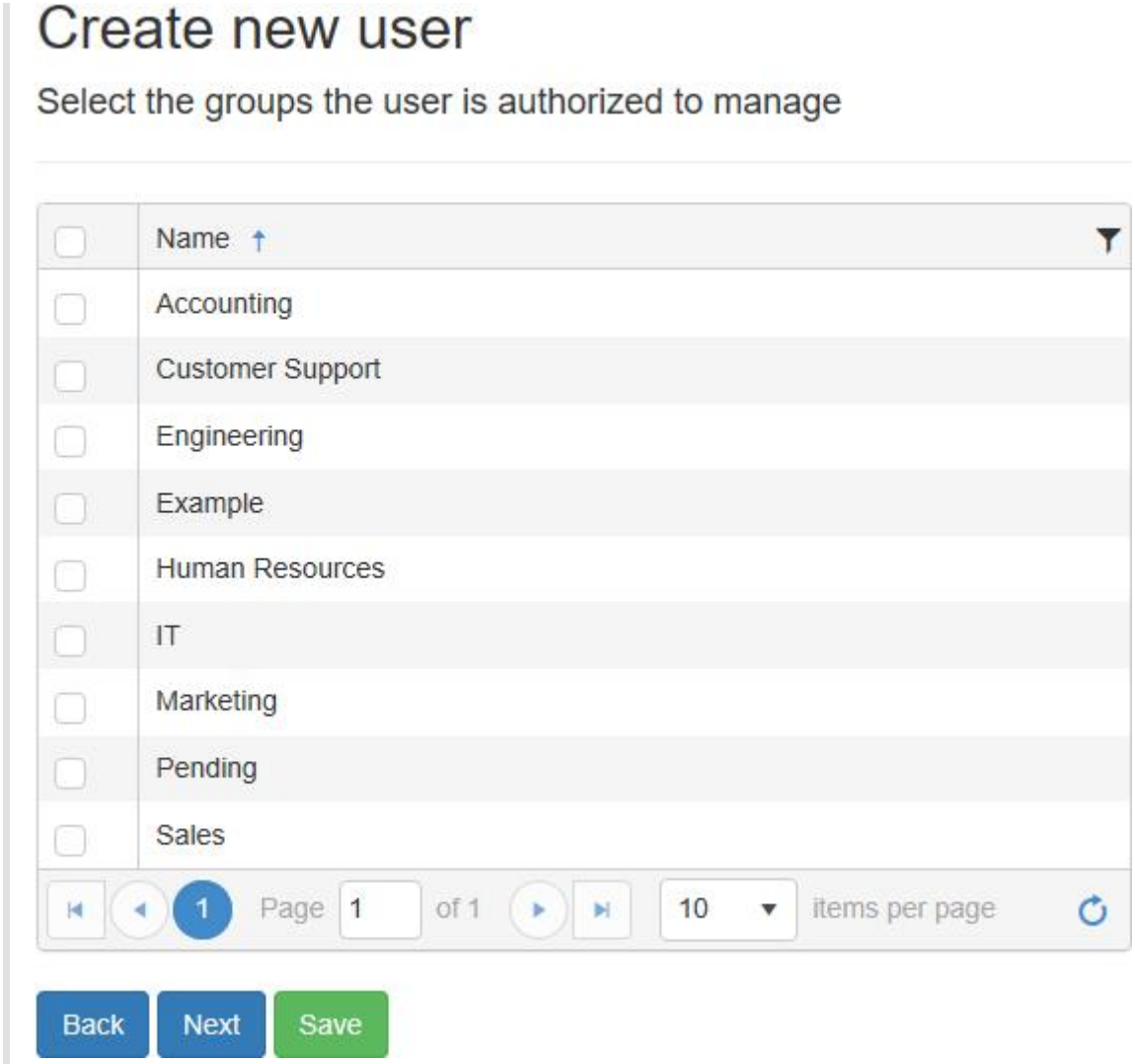
If a Storage Server was added by the administrator, the option to create a storage server group when creating a user will be displayed.

If the "Create Storage Server Group for this user" check box is checked in the storage server settings, a storage server group is created when this user is created.

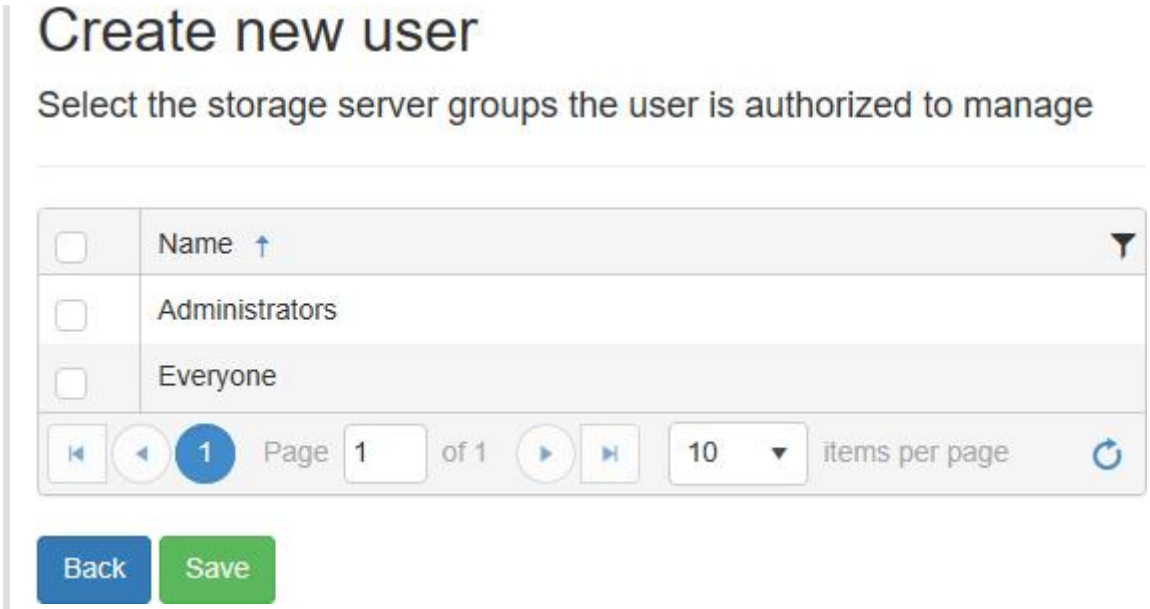
The storage server group name, derived from the username, must be unique.



Select the groups the user is authorized to manage.



If a storage server is configured, you can select the storage server groups the user is authorized to manage.



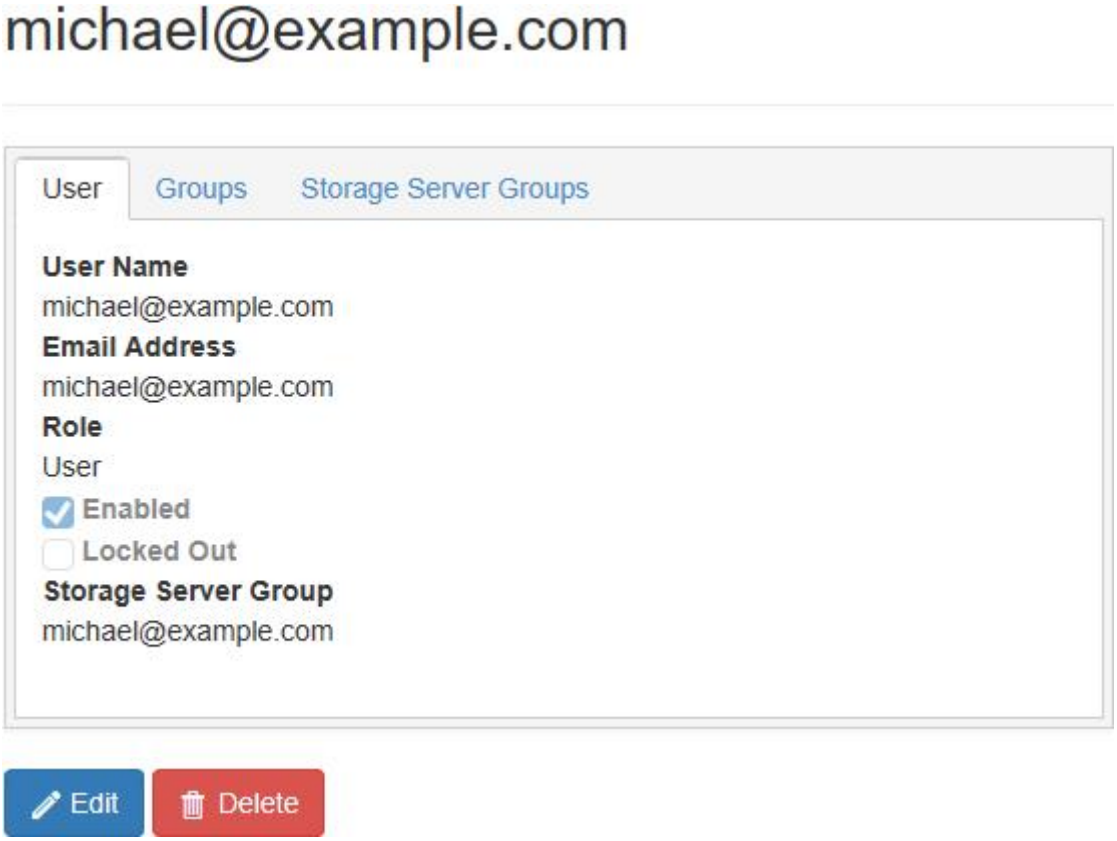
Click the "Save" button to create the user.

PERMISSIONS REQUIRED

Edit Users

View a user

From the "Users" view, click on the "View" button to view the details of a user.

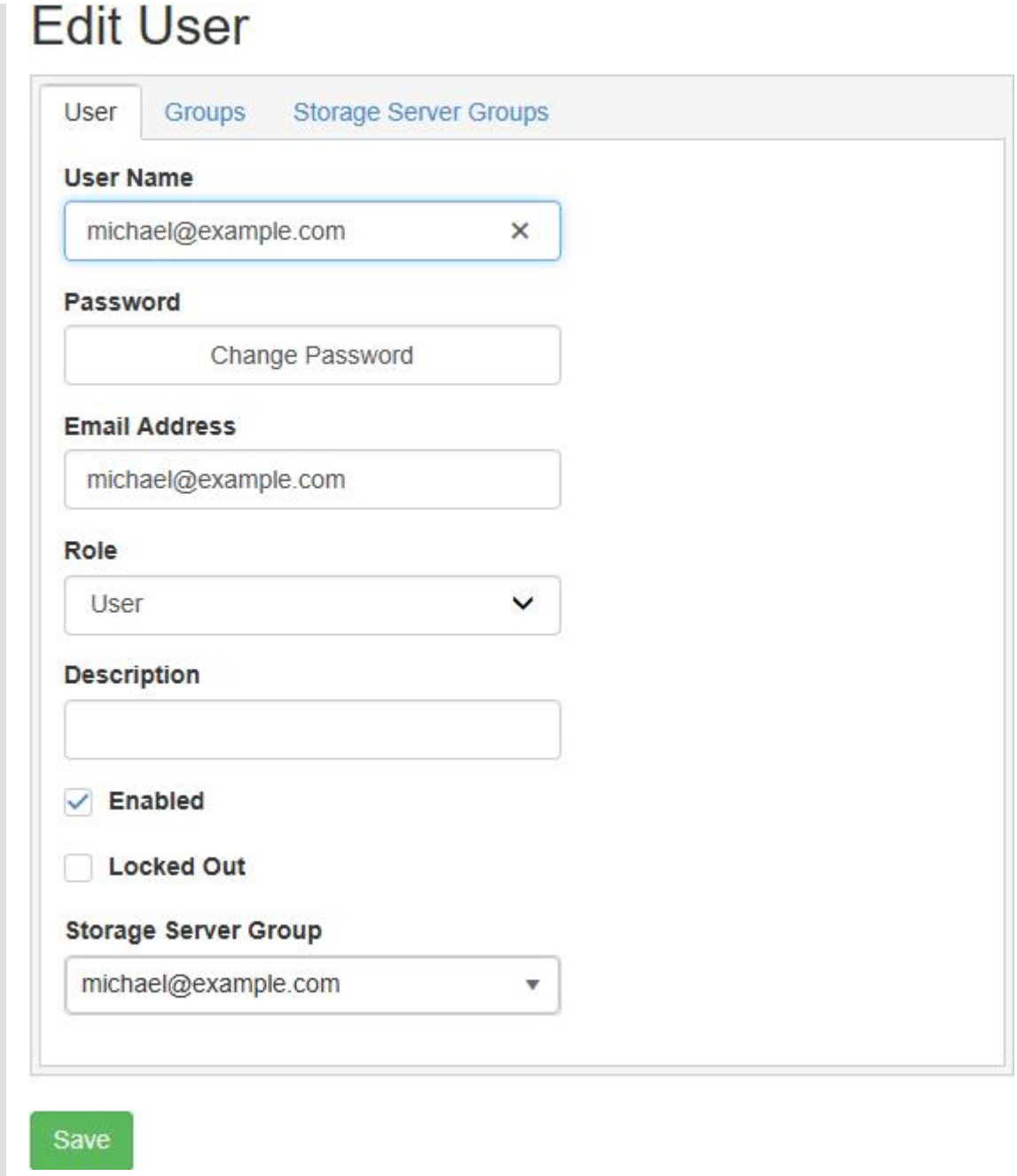


PERMISSIONS REQUIRED

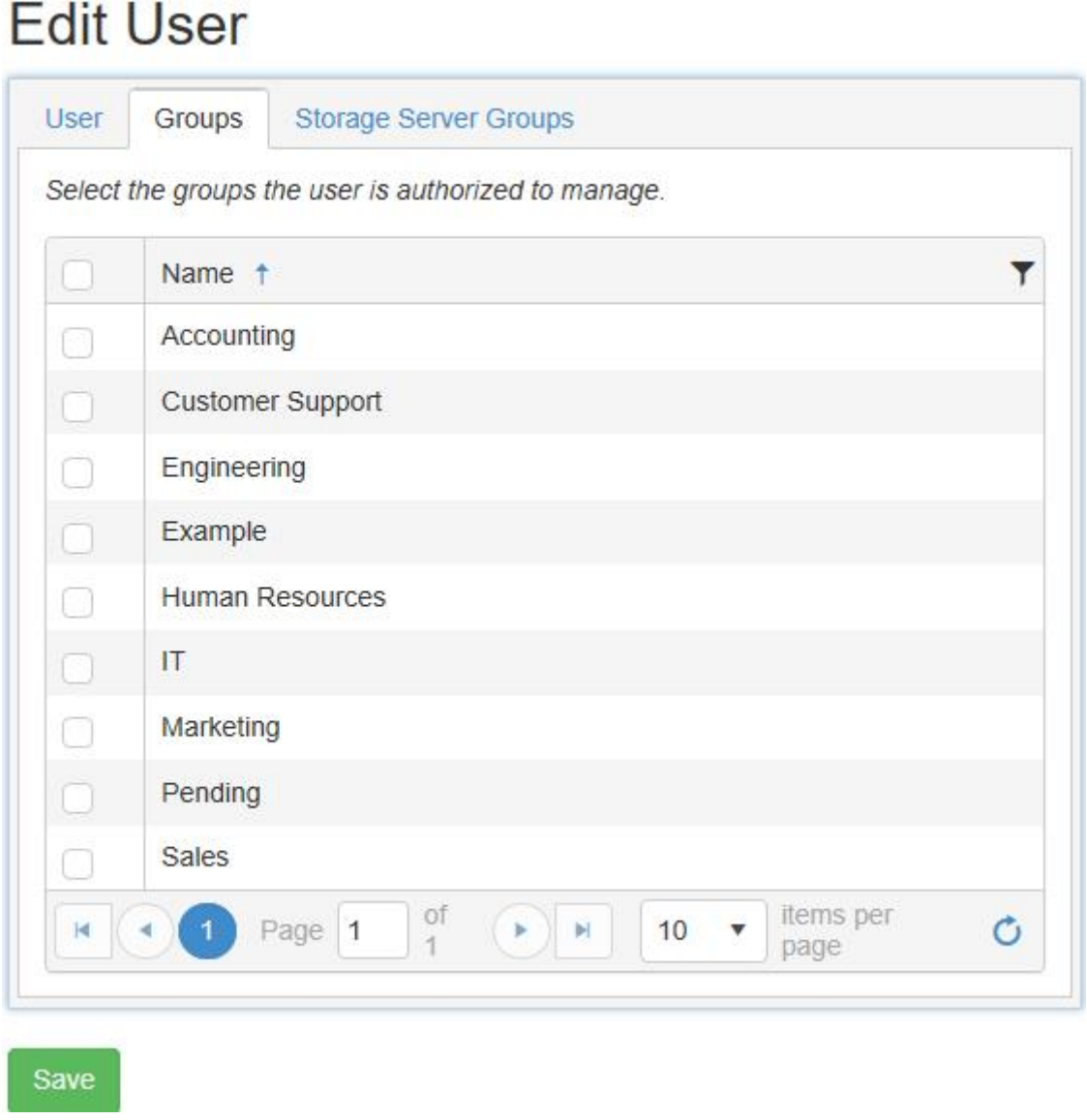
View Users

Edit a user

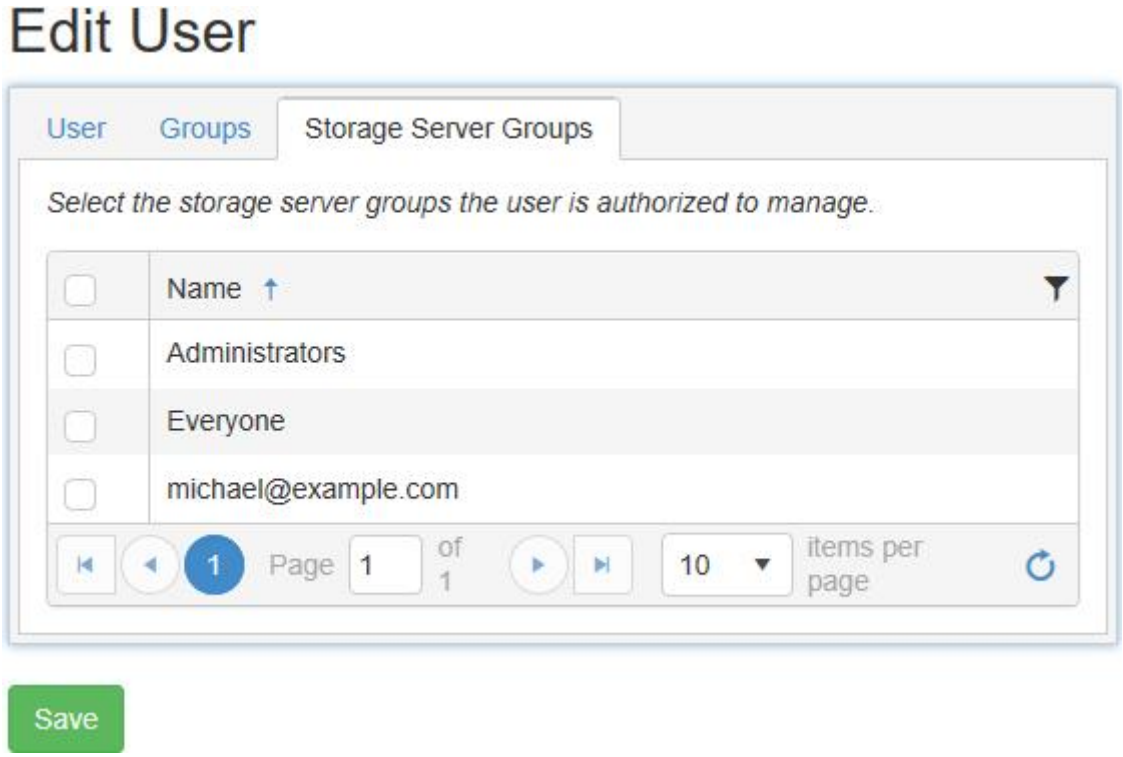
From the "User Details" view, click on the "Edit" button to edit the user.



Click on the Groups tab to modify the groups the user is authorized to manage.



Click on the "Storage Server Groups" tab to modify the storage server groups the user is authorized to manage.



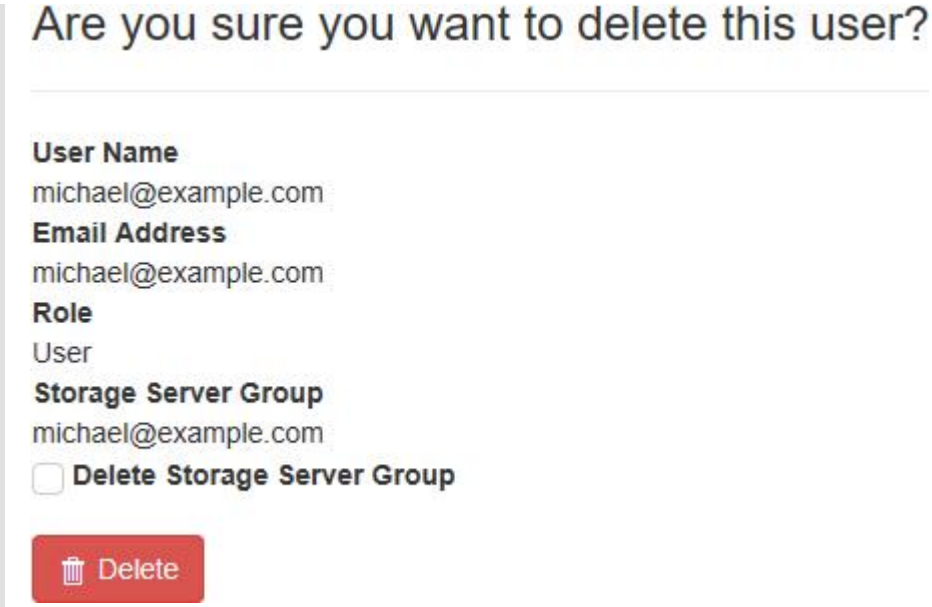
Click on the "Save" button to save the changes made to the user.

 PERMISSIONS REQUIRED

Edit Users

Delete a user

From the "User Details" view, click on the "Delete" button to delete the user.



Check mark the "Delete Storage Server Group" check box to delete the storage server group associated with the user when deleting the user.

Click on the "Delete" button again to confirm deleting the user.

The default storage server group cannot be deleted.

The storage server group cannot be deleted if it's associated with other users.

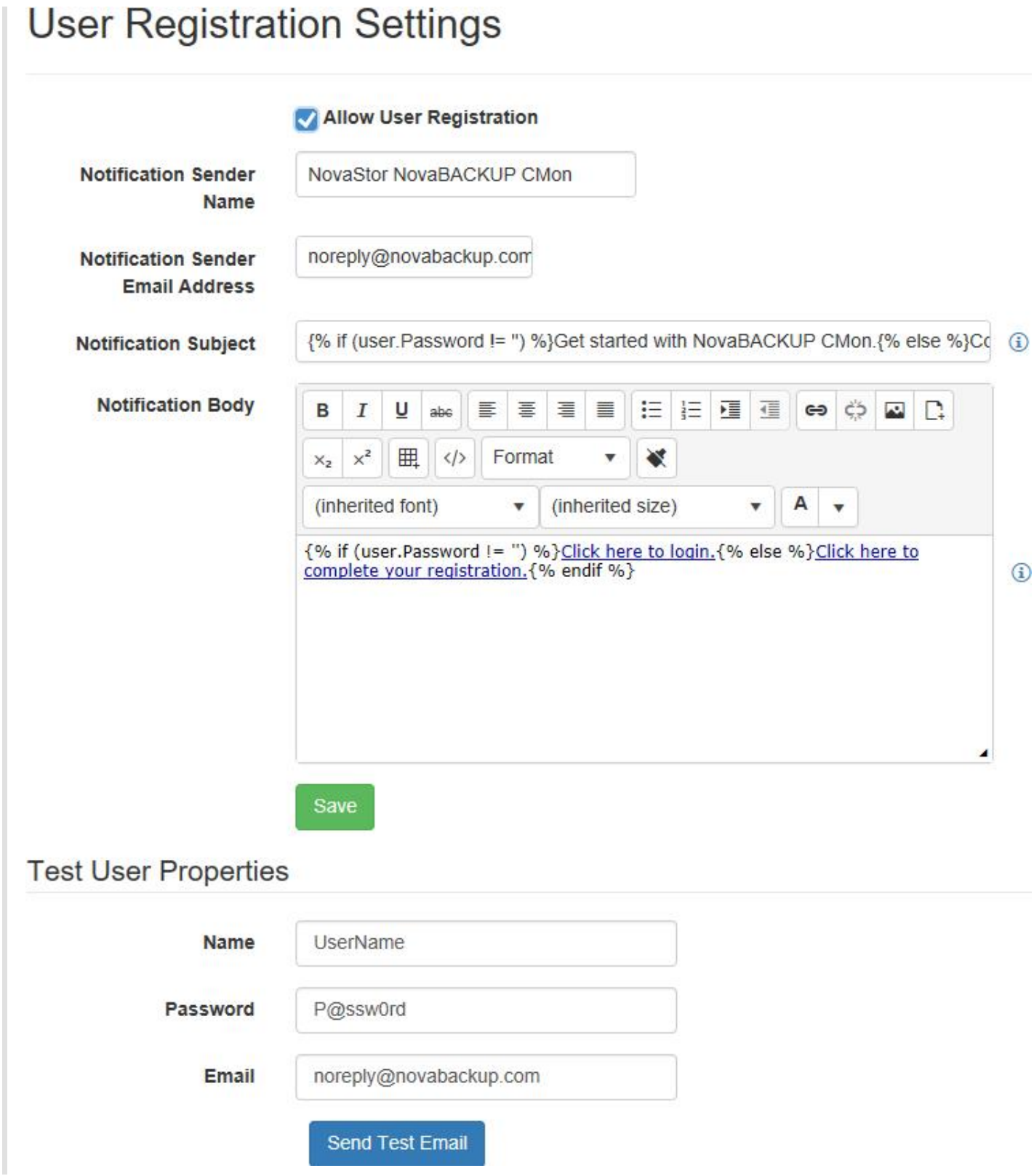
The storage server group cannot be deleted if it's being used with one or more cloud storage accounts.

PERMISSIONS REQUIRED

Edit Users

User Registration Settings

The "User Registration Settings" view allows an administrator to enable or disable user registrations and configure the user registration email template.



The notification email sender name and email address are editable only when using a custom SMTP server.

Notification Email

The user registration notification email subject and body are templates that use markup to output text based on conditions and variables.

Syntax

Introduction

TYPE	DESCRIPTION
Objects	Objects produce content. Object names are denoted by double curly braces: {{ and }}.
Tags	Tags create the logic and control flow for templates. They are denoted by curly braces and percent signs: {% and %}. The markup used in tags does not produce any visible text.

Control flow

SYNTAX	DESCRIPTION
if	Executes a block of code only if a certain condition is true.
elsif / else	Adds more conditions within an if block.
endif	Indicates the end of an if control block.

Operators

SYNTAX	DESCRIPTION
==	equals
!=	does not equal
>	greater than
<	less than
>=	greater than or equal to
<=	less than or equal to
or	logical or
and	logical and

Built-in objects

OBJECT NAME	DESCRIPTION
user.Name	The user's username.
user.Email	The user's email address.
user.Password	The user's password. Putting a password in plain text in an email isn't recommended.
SetPasswordToken	The token used to set the user's password.
SetPasswordUrl	The URL of the page which allows the user to set their password.
LoginUrl	The URL of the login page.

PERMISSIONS REQUIRED

View Settings

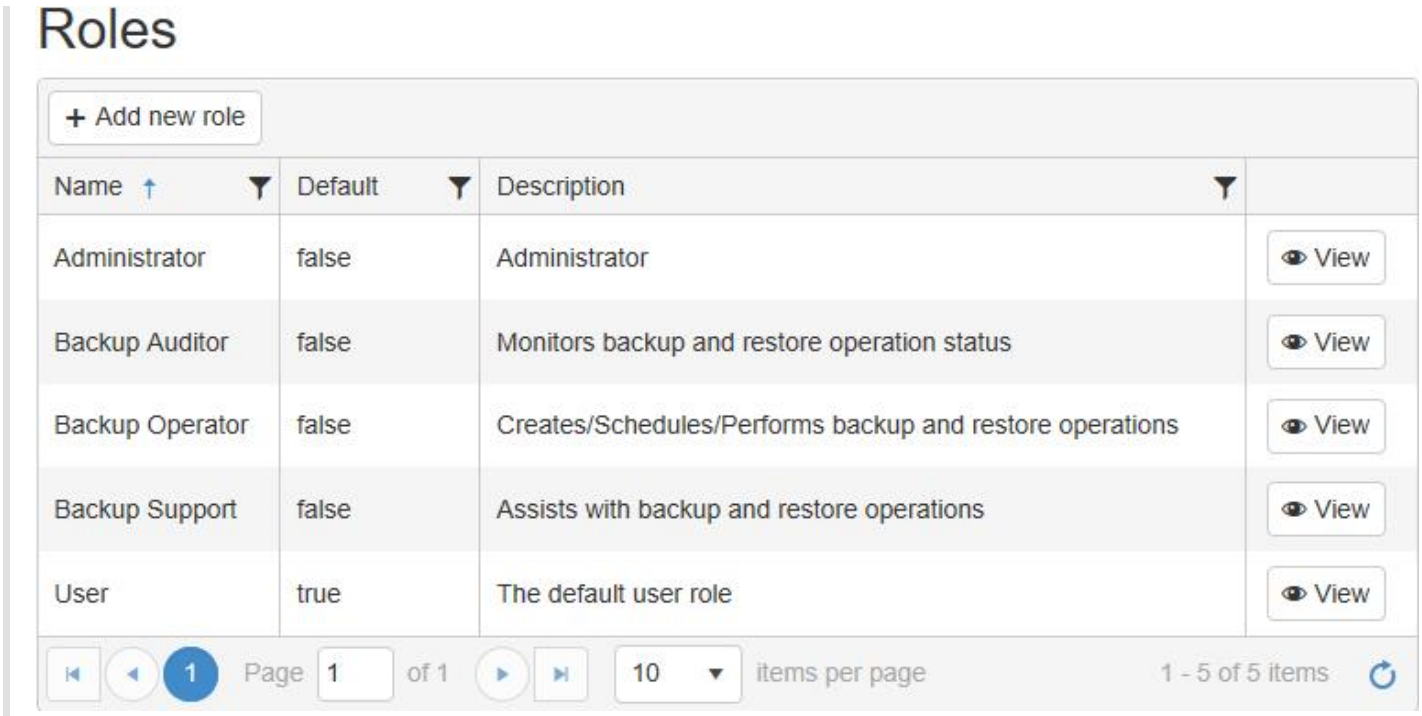
Edit Settings

Related topics:

Notification Settings
User registration

Roles

The "**Roles**" page contains the ability to create, view, and edit Roles. Once on the **Roles** page you can click on "**Add new role**" button to add new roles. From there you will be able to define a custom role.



Click on the **View** button to view the details of a role.

> ![Role Details](../images/Role Details.jpg)

PERMISSIONS REQUIRED

View Roles

Edit Roles

Storage Servers

The "Storage Servers" view allows an administrator to manage NovaBACKUP Storage Servers.

In order for users to create cloud storage accounts, a Storage Server must be added.

PERMISSIONS REQUIRED

View Storage Servers

Add a storage server

From the "Storage Servers" view, click on the "Add new storage server" button to add a new storage server.

Enter the web URL and key for the Storage Server API and click the Next button to continue.

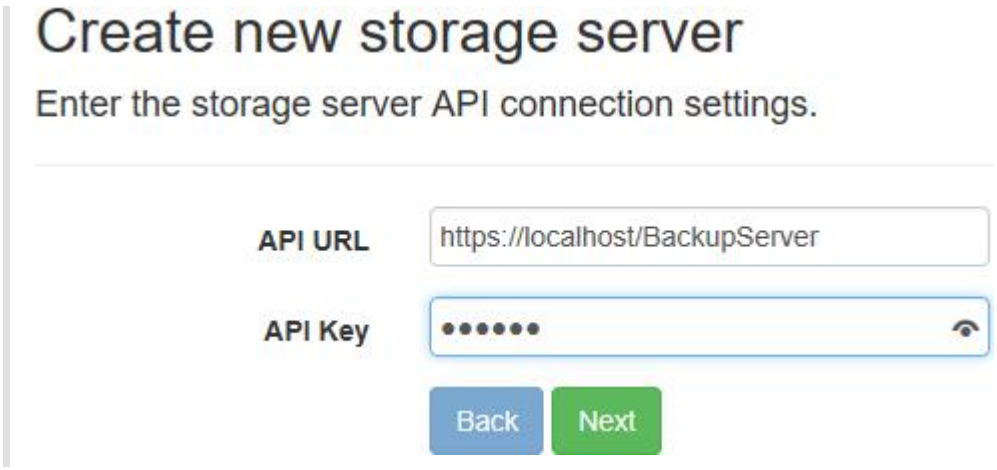
The storage server API is an optional feature installed with the NovaBACKUP Storage Server by default.

It's recommended to use HTTPS for a secure connection.

If a secure connection could not be established because of SSL certificate errors, the errors can be ignored in Security Settings, but this is not recommended.

The API key is configured in the storage server API's "appSettings.config" file and is case sensitive.

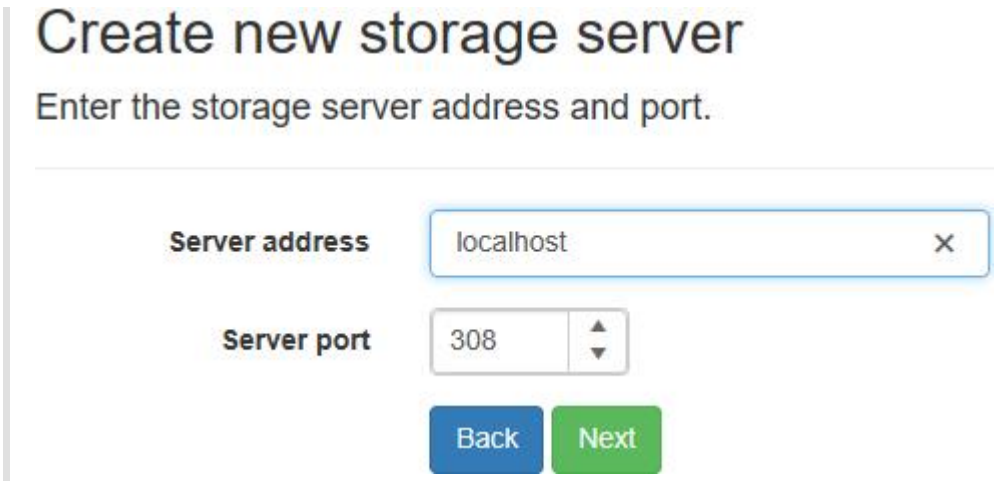
A randomly generated API key is created by default.



Enter the storage server address and port and click the "Next" button to continue.

The storage server address should be publicly resolvable by the backup client.

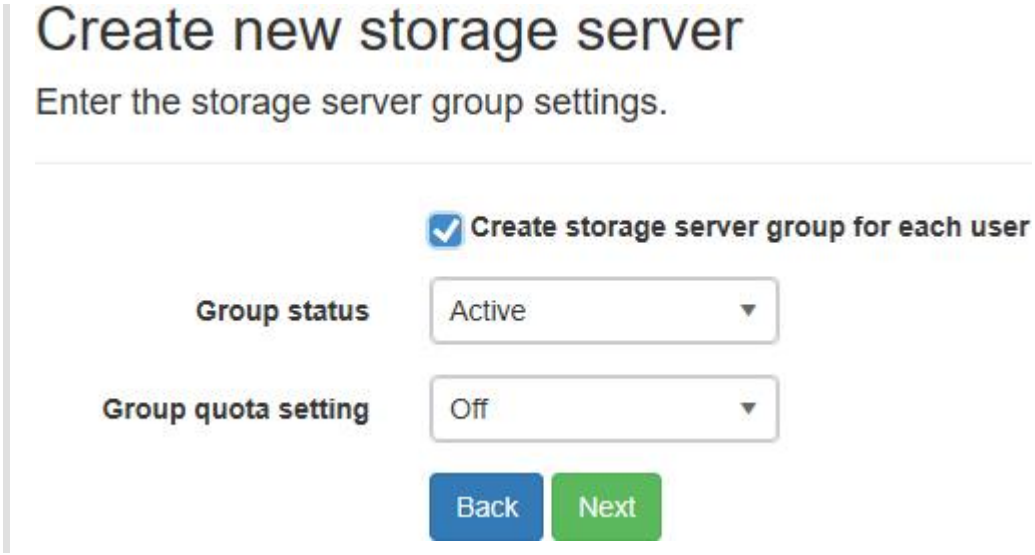
The storage server port is the port the backup server is configured to listening on.



Enter the storage server group settings and click the "Next" button to continue.

If the "Create storage server group for each user" check box is checked:

1. A new storage server group is created for new CMon users.
2. The name of the storage server group will be the same as the username of the CMon user.
3. New cloud storage accounts created for new CMon users will be assigned that storage server group.
4. The group status and quota settings will be used for the new storage server group.



Enter the storage server account settings and click the "Next" button to continue.

When the user is required to enter a backup client license key and the "Account Quota Setting" field is set to "Custom", the user account's quota will be set according to the quota specified for the backup client license key provided when the user signs up for an account.

Otherwise, the "Account Quota (Megabytes)" field must be specified if the user is not required to enter a backup client license key and the "Account Quota Setting" field is set to "Custom".

If a backup client license is used with a data storage quota greater than 2,147,483 GB, then the data storage quota on the cloud storage account will be limited to 2,147,483,647 MB.

When the "Account Quota Setting" field is set to "Group", the user account's quota will be set according to the quota specified for the storage server group specified in the previous step.

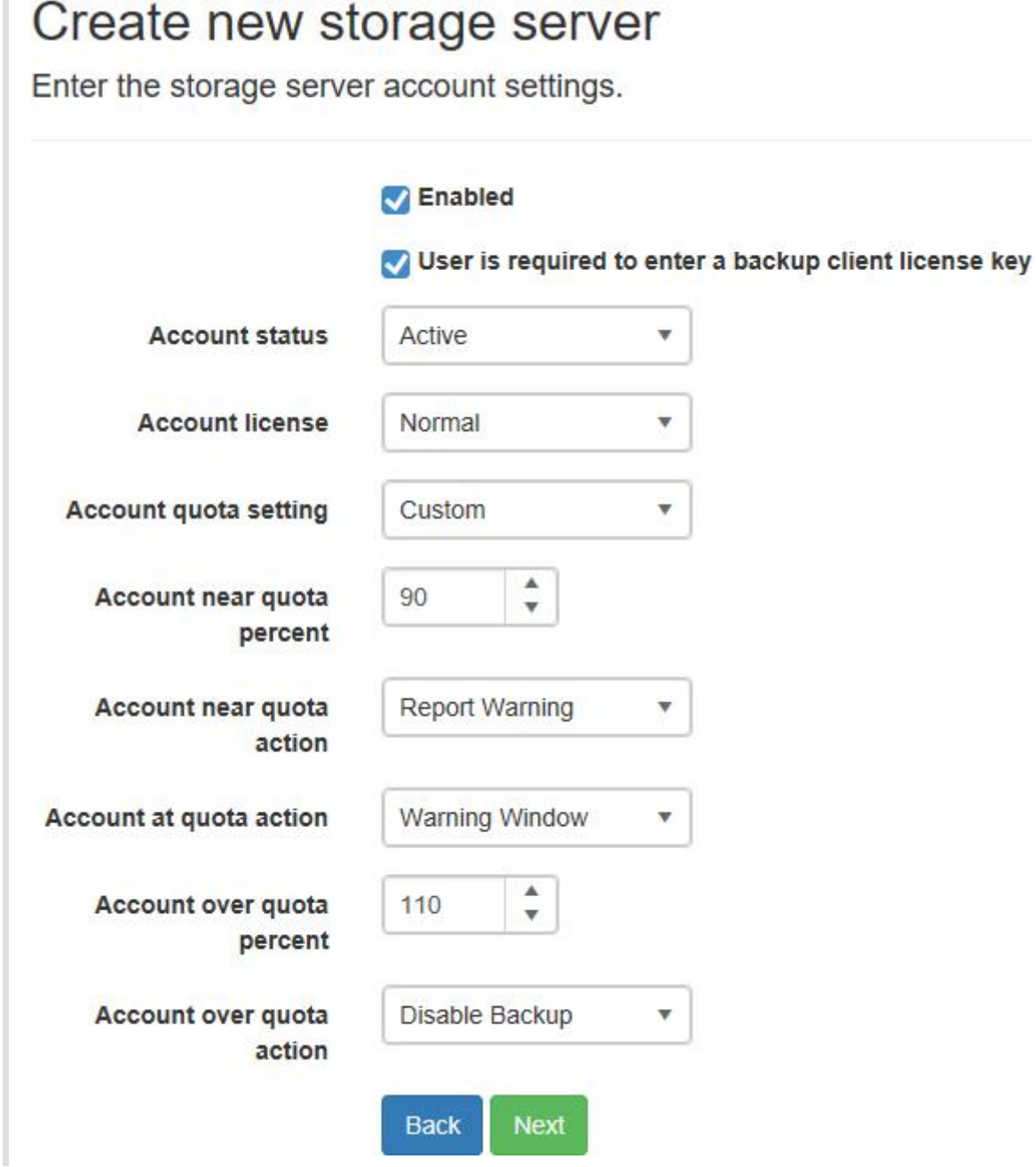
When the "Account Quota Setting" field is set to "No Quota", the user's account will have an unlimited amount of storage space.

The number of computers that can be backed up to the cloud storage account will be based on the maximum number of activations set on the backup client license used to create the account.

If a backup client license is used with a maximum number of activations greater than 5000, then the number of computers on the cloud storage account will be limited to 5000.

If the user is not required to enter a backup client license key, then the "Number of computers" must be specified if the "Multiple computers allowed" checkbox is checked.

The storage server help documentation contains more details about the other settings.



Enter the storage server account data storage and retention policy settings and click the "Next" button to continue.

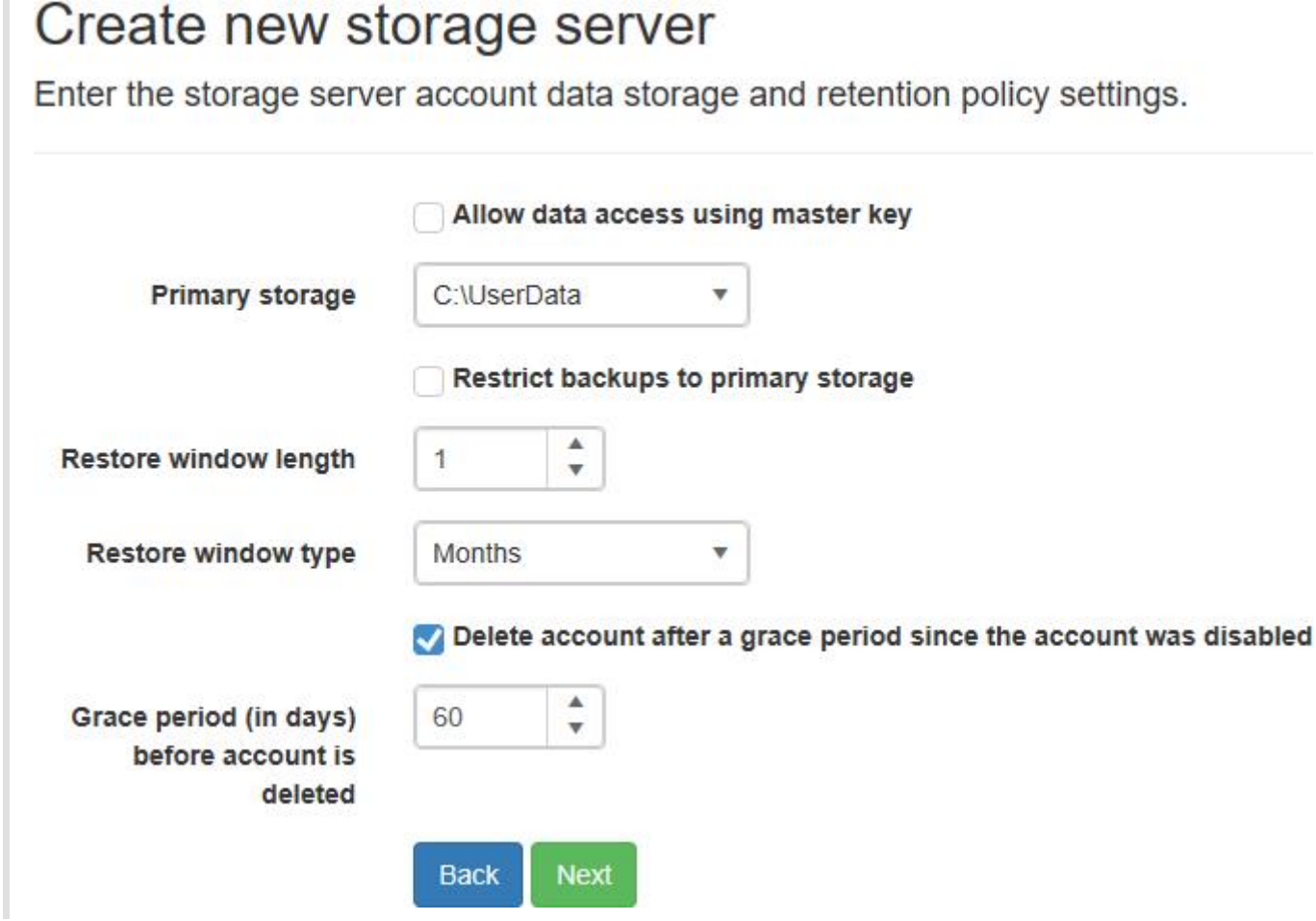
If the cloud storage account was created with a backup client license key, the account will automatically be disabled if the backup client license is disabled, expired, no longer supports cloud storage, or if the upgrade subscription is expired.

The cloud storage account will automatically be re-enabled if the license and upgrade subscription, if any, become valid again.

An account can also be disabled from the storage server directly.

After an account is disabled, the user will not be able to connect to the storage server.

If the "Delete account after a grace period since the account was disabled" check box is checked, the account will be deleted after the specified grace period since the account was disabled.

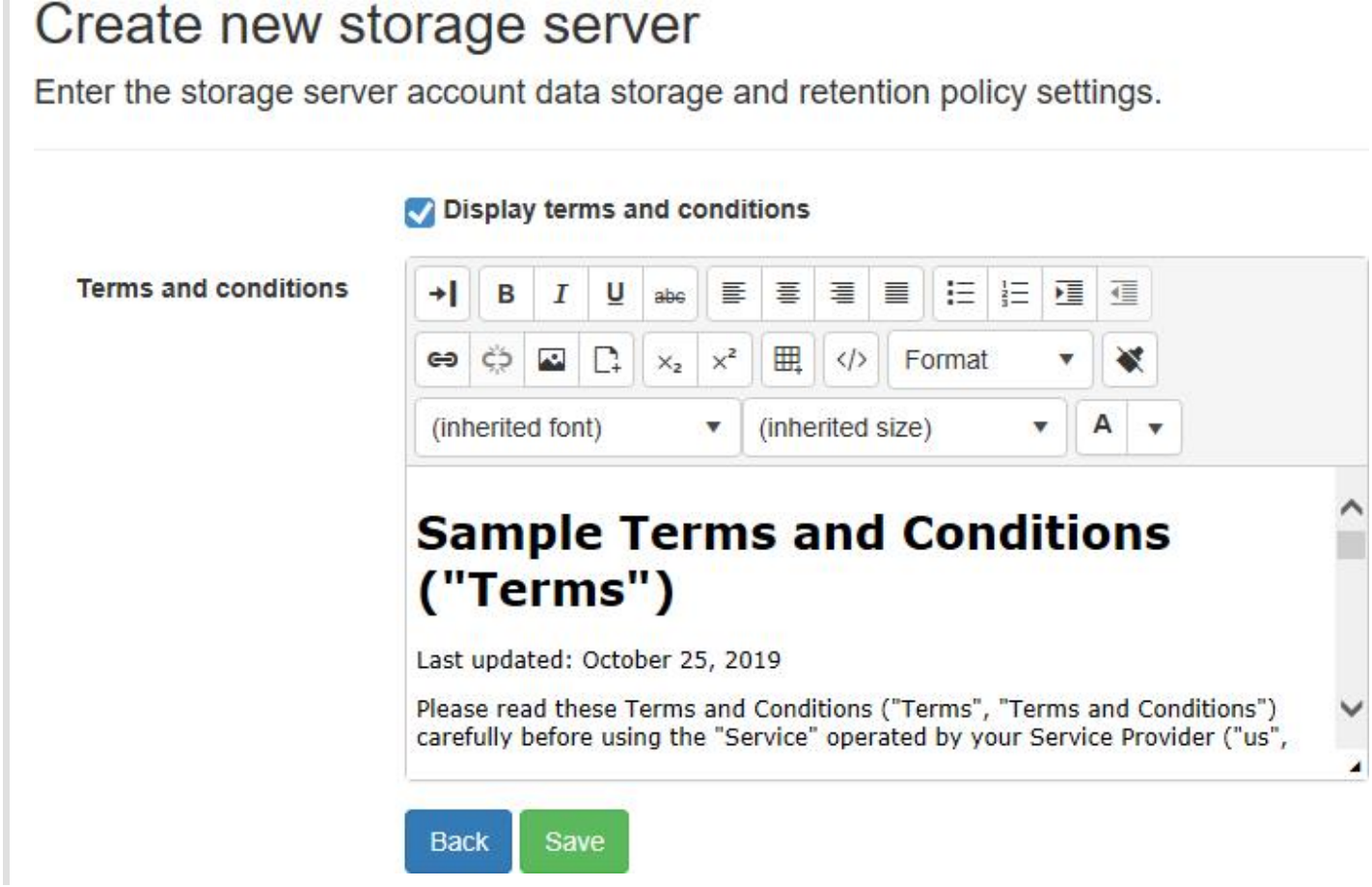


Optionally enable displaying the terms and conditions and click the "Save" button to continue.

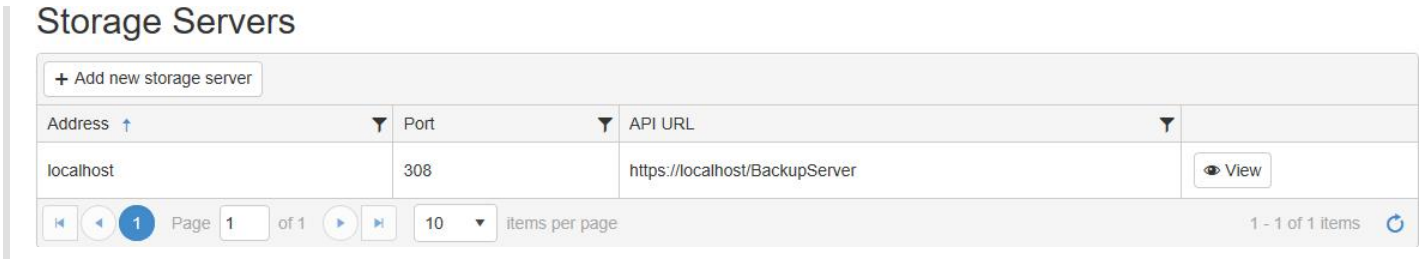
If enabled, the user must accept the terms and conditions before a cloud storage account is created.

The Import button can be used to insert a Microsoft Office Open XML Format word processing document (DOCX), Rich Text Format (RTF), Adobe Portable Document Format (PDF), HyperText Markup Language (HTML), and plain text (txt) file into the terms and conditions editor.

For more details on how the terms and conditions is displayed, see Terms and Conditions.



After creating the storage server, it will be displayed in the data grid.



Only one storage server is supported.

The CMon will periodically query the license for any changes and update the cloud account accordingly.

PERMISSIONS REQUIRED

Edit Storage Servers

Related topics:

Create a cloud storage account

Web Hook Settings

The `Web Hook Settings` page allows a user to view and modify the current web hook settings.

The web hook receiver is used to receive notifications from the License Server when a license has been updated. When a notification has been received, the cloud storage account associated with that license will be updated.

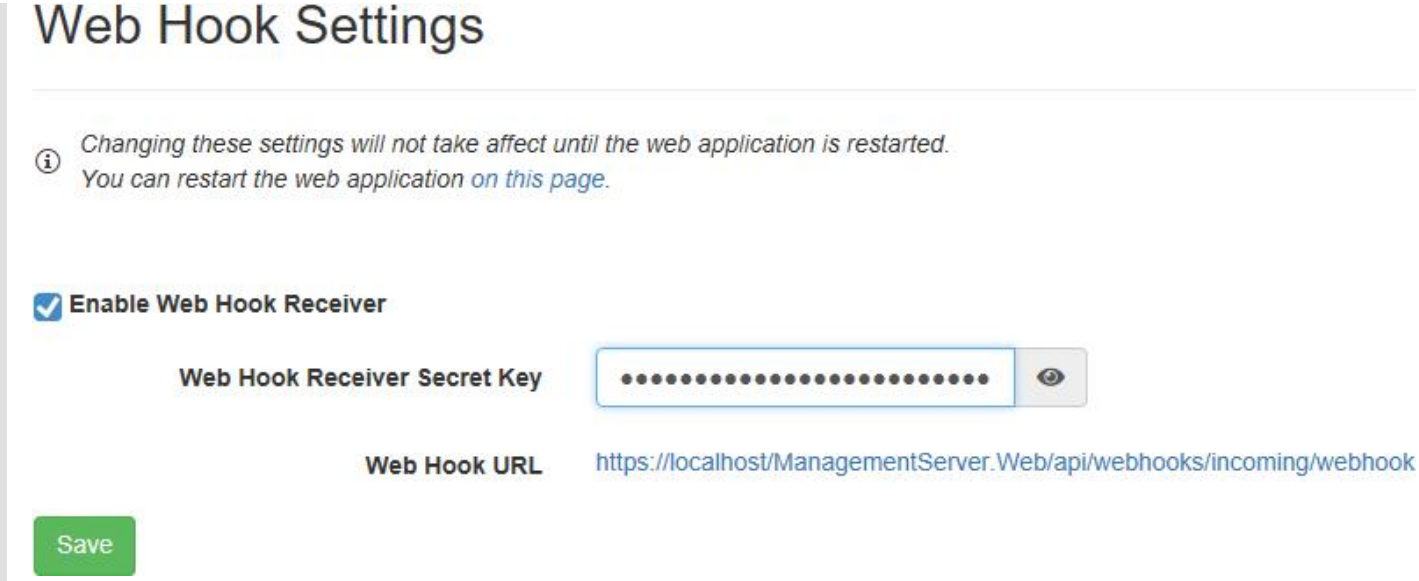
The web hook receiver secret key is required and must have a minimum of 32 and a maximum of 256 characters.

The web hook receiver secret key must not contain commas, equals signs, and leading or trailing spaces.

The secret key is used to verify that the caller is authorized to send requests.

The web hook receiver must be accessible using HTTPS for it to accept requests.

The web hook URL displayed is built based on the URL of the current page and may not be accurate depending on the hosting environment.



The web hook receiver also restricts access depending on the IP address of the caller.

See IP Filter Configuration for more information.

PERMISSIONS REQUIRED

View Settings

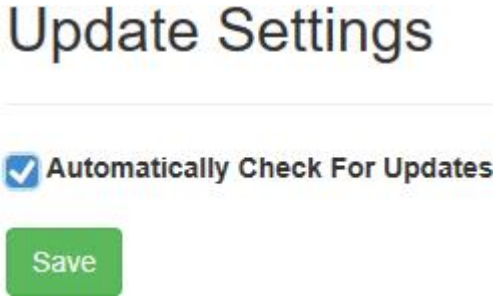
Edit Settings

Update Settings

The "Update Settings" view allows an administrator to enable or disable automatically checking for updates.

It's recommend to enable automatically checking for updates to automatically receive notifications when a new update is available.

If enabled, the "Management Server" windows service automatically checks for updates every 7 days.



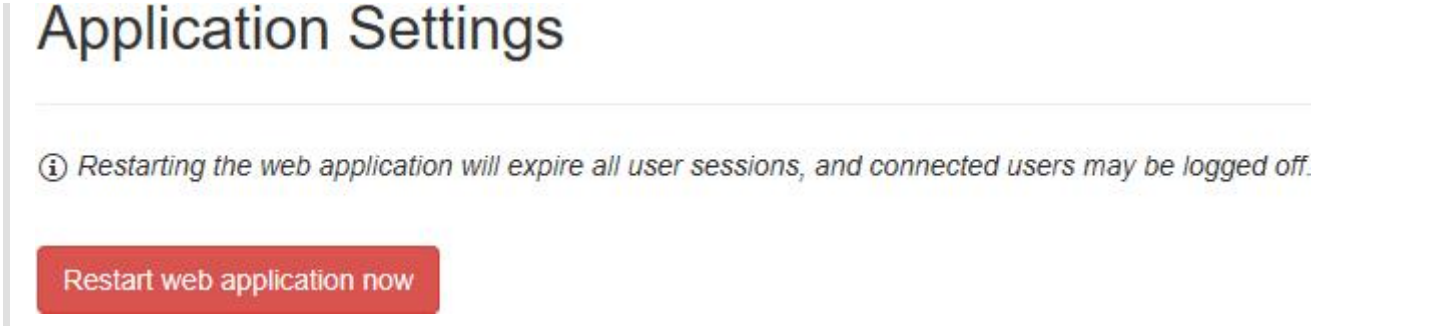
PERMISSIONS REQUIRED

View Settings

Edit Settings

Application Settings

The `Application Settings` page allows a user to restart the web application.



PERMISSIONS REQUIRED

Edit Settings

Server Administration Desktop Application

The CMon Server Administration utility is a desktop application installed on the local server where CMon is installed.

A shortcut is created in the Start menu called "NovaBACKUP CMon Server Administration".

It allows you to change the CMon server address and port number and unlock user accounts.

Scheduled Task

A scheduled task named "NovaBACKUPManagementServer" is created in the Windows Task Scheduler that's responsible for sending notifications and deleting old job logs as configured in the settings.

The task does not delete job logs which have unsent notifications.

The configuration file contains a setting for the database command timeout.

The file is located in the Web installation directory. For example,

```
C:\Program Files (x86)\NovaStor\NovaBACKUP Central Management
Console\ScheduledTask\ManagementServer.Service.ScheduledTask.Console.exe.config
```

Database Command Timeout

The default value is 0 which prevents the command from timing out. An empty value will instruct the application to use the default database provider's timeout value.

```
<appSettings>
  <add key="DatabaseCommandTimeout" value="0"/>
</appSettings>
```

Web Configuration File

The web configuration file (web.config) contains some of the application settings such as the database connection string, log file path, log verbosity, and persistent login behavior.

The file is located in the Web installation directory. For example,
`C:\Program Files (x86)\NovaStor\NovaBACKUP Central Management Console\WebRoot\Web\web.config`

Persistent login settings

When a user chooses to login and persist their login information, the default behavior is to keep them logged in for 7 days since they last visited the web application.

```
<authentication mode="Forms">
  <!-- forms session times out in 7 days -->
  <forms loginUrl="~/Account/Login" slidingExpiration="true" path="/" name="ManagementServer"
timeout="10080" protection="All"/>
</authentication>
```

For more technical information about these configuration settings, see forms Element for authentication (ASP.NET Settings Schema).

IP Filter Configuration File

The web hook receiver restricts access depending on the IP address of the caller.

These restrictions are specified in the `IPFilter.config` file in the web application installation directory.

Default File Path

32-bit Operating System

`C:\Program Files\NovaStor\NovaBACKUP Central Management Console\WebRoot\Web\IPFilter.config`.

64-bit Operating System

```
C:\Program Files (x86)\NovaStor\NovaBACKUP Central Management
Console\WebRoot\Web\IPFilter.config
```

.

Syntax

No more than two hosts can be specified in an `<allow />` element because the hosts attribute signifies either one IP address or a range of IP addresses.

Examples

One IP Address

```
<allow hosts="198.51.100.0" />
```

A Range of IP Addresses

```
<allow hosts="198.51.100.0,198.51.100.255" />
```

Help

Documentation

About

Known Issues

Troubleshooting Tips

Windows Service Logging

Standalone Web Server Logging

Web Site Logging

Scheduled Task Logging

Help Documentation

The Help Documentation link opens a new window to display the Central Monitoring Console (CMon) User Manual in a web browser.

A download link is provided on the bottom of each page to download a PDF version.

You can also send us feedback by clicking the email link on the bottom.

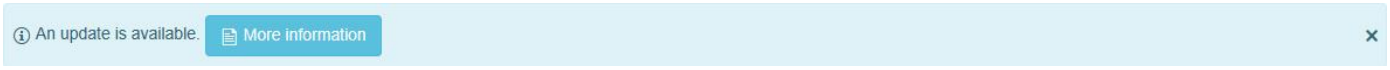
About

The About page displays product version information about CMon for logged in users.

Logged in users in a role with "View Settings" permission can also manually check for product updates on this page.

CMon can be configured to automatically check for product updates in the Update Settings page.

If an update is available, a notification is displayed on all pages, except the About page, for logged in users in a role with "View Settings" permission.

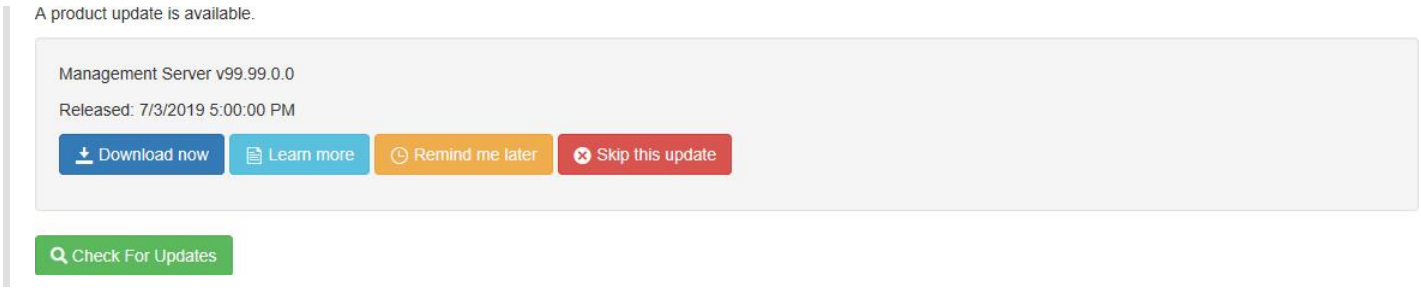


The product update notification contains a "More Information" button, which redirects them to the About page.

If a product update is available, the About page will display information about the new version:

- The new version number.
- The released date of the new version.
- Links to "Download now" and "Learn more" if available.
- The last time a check for updates was performed.
- A "Remind me later" button which will snooze the product update notification for 24 hours.
- The next time the product update notification will appear if the "Remind me later" button was clicked.
- A "Skip this update" button which will dismiss/skip the product update notification, specifically for the new version.

If the "Skip this update" button was clicked and a version is available that's newer than the version that was previous skipped, then the product update notification will re-appear.



If no updates are available, the About page displays the message, "The latest version is already installed".

If there's more than one update available, the About page will only display the latest version.

If the "Skip this update" button was clicked, and then the "Remind me later" button is clicked, the product update notification will re-appear after 24 hours.

PERMISSIONS REQUIRED

View Settings

Known Issues

- Retention and Import jobs are not monitored/reported
- When using CMon over HTTP, usernames and passwords are sent in plain text
- It is recommended to use SSL/HTTPS for security reasons.
- Some inputs are not validated for maximum lengths.

Troubleshooting Tips

The Management Service may not be started.

The Management Service must be started to be accessible. Run the Services control panel and start the "Management Service" windows service. If it fails to start, see Windows Service Logging for troubleshooting.

The Web Server may not be started.

The Web Server must be started to be accessible. Depending on which web server hosts the console application, run the Services control panel and start the appropriate windows service:

- If using the standalone web server, start the "Management Web Server" windows service. If it fails to start, see Standalone Web Server Logging for troubleshooting.
- If using Internet Information Services (IIS), start the "World Wide Web Publishing Service" windows service.

A firewall may be blocking one or more required ports.

If the Management Service is behind a firewall, make sure its configured port is open. The port number was specified during installation and saved in the "Management Server" windows service "system.serviceModel.services.config" configuration file. You can launch the Server Administration utility to quickly view and optionally edit the port number. The Management Service uses the TCP protocol.

If the web server is behind a firewall, make sure its configured port is open. The port number may have been specified during installation and saved in the main "Management Web Server" windows service configuration file if the standalone web server was selected.

The Management Service address may be incorrect.

The Management Service address must be configured correctly to be accessible. The server address was specified during installation and saved in the "Management Server" windows service "system.serviceModel.services.config" configuration file. You can launch the Server Administration utility to quickly view and optionally edit the server address.

Log Files

The best way to determine the underlying cause of issues is to analyze the logs.

The application configuration files contain settings that may need to be modified in order to enable logging.

These application configuration files can be edited in a simple text editor (ex. notepad).

After you are done troubleshooting, remember to revert your changes.

Windows Service Logging

Standalone Web Server Logging

Web Site Logging

Scheduled Task Logging

Windows Service Logging

Windows Service Configuration File

The "Management Server" windows service configuration file with a default installation is located here: "C:\Program Files\NovaStor\NovaBACKUP Central Management Console\Service\ManagementServer.Service.WindowsServiceHost.exe.config"

When this file is modified, the internal services will automatically restart and use the latest changes.

If the configuration file contains errors, the windows service will not start.

If the windows service is already started, it will automatically stop.

Log File Location

With a default installation, the log files are located here: "C:\Program Files\NovaStor\NovaBACKUP Central Management Console\Service\Logs"

How to enable logging for the "Management Server" windows service

Open the main "Management Server" windows service configuration file, unless otherwise specified, perform the steps outlined below, and then save the file. This generates a fairly large amount of trace data in the Logs directory.

Enable Log Listeners

Enable logging to the Application Event Log and a Flat File.

Change this: **XML**

```
<configuration>
  ...
  <loggingConfiguration ...>
    ...
    <categorySources>
      <add switchValue="All" name="General" />
    </categorySources>
  ...
```

to: **XML**

```
<configuration>
  ...
  <loggingConfiguration ...>
```

```
    ...
    <categorySources>
      <add switchValue="All" name="General" >
        <listeners>
          <add name="Event Log Listener" />
          <add name="Flat File Trace Listener" />
        </listeners>
      </add>
    </categorySources>
  ...
```

Errors will now be logged in the trace.log file in the Logs directory by default.

Enable WCF Verbose Activity Tracing

For communication issues bet, Set the switchValue attributes to Verbose, ActivityTracing.

Change this: **XML**

```
<configuration>
  ...
  <system.diagnostics>
      <sources>
        <source name="System.ServiceModel" switchValue="Warning" propagateActivity="true">
        ...
        <source name="System.ServiceModel.MessageLogging" switchValue="Warning">
    ...
```

to: **XML**

```
<configuration>
  ...
  <system.diagnostics>
      <sources>
        <source name="System.ServiceModel" switchValue="Verbose, ActivityTracing"
propagateActivity="true">
        ...
        <source name="System.ServiceModel.MessageLogging" switchValue="Verbose,
ActivityTracing">
    ...
```

Errors will now be logged in app_tracelog.svclog and app_messages.svclog files in the Logs directory by default.

Enable Message Logging

Open "system.serviceModel.diagnostics.config" and enable logMessagesAtServiceLevel, logMalformedMessages, and logMessagesAtTransportLevel.

Change this: **XML**

```
<configuration>
  ...
```

```
  <system.serviceModel>
    ...
      <diagnostics>
      <messageLogging logMessagesAtServiceLevel="false" logMalformedMessages="false"
logMessagesAtTransportLevel="false"  />
    ...
```

to: **XML**

```
<configuration>
  ...
  <system.serviceModel>
    ...
      <diagnostics>
      <messageLogging logMessagesAtServiceLevel="true" logMalformedMessages="true"
logMessagesAtTransportLevel="true" />
    ...
```

Enable Message Logging with Personally Identifiable Information

For example, this logs the remote IP address of clients connecting to the service.

Open "C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config" and set enableLoggingKnownPii.

Change this: **XML**

```
<configuration>
  ...
  <system.serviceModel>
    ...
      <machineSettings enableLoggingKnownPii="false" />
    ...
```

to: **XML**

```
<configuration>
  ...
  <system.serviceModel>
    ...
      <machineSettings enableLoggingKnownPii="true" />
    ...
```

Open "system.serviceModel.diagnostics.config" and enable logMessagesAtServiceLevel, logMalformedMessages, logMessagesAtTransportLevel, logEntireMessage, and logKnwonPii.

Change this: **XML**

```
<configuration>
  ...
  <system.serviceModel>
    ...
      <diagnostics>
```

```
      <messageLogging logMessagesAtServiceLevel="false" logMalformedMessages="false"
logMessagesAtTransportLevel="false"  />
    ...
```

to: **XML**

```
<configuration>
  ...
  <system.serviceModel>
    ...
      <diagnostics>
      <messageLogging logMessagesAtServiceLevel="true" logMalformedMessages="true"
logMessagesAtTransportLevel="true" logEntireMessage="true" logKnwonPii="true" />
    ...
```

Standalone Web Server Logging

Standalone Web Server Configuration File

The "Management Web Server" windows service configuration file with a default installation is located here: "C:\Program Files\NovaStor\NovaBACKUP Central Management Console\WebRoot\Web\bin\ManagementServer.WebServer.WindowsServiceHost.exe.config"

Log File Location

With a default installation, the log files are located here: "C:\Program Files\NovaStor\NovaBACKUP Central Management Console\WebRoot"

How to enable logging for the "Management Web Server" windows service

Open the "Management Web Server" windows service configuration file, perform the step outlined below, and then save the file. This generates a web.log file in "C:\Program Files\NovaStor\NovaBACKUP Central Management Console\WebRoot" for example.

Enable Log Listeners

Enable logging to a Flat File.

Change this: **XML**

```
<configuration>
  ...
  <loggingConfiguration ...>
    ...
    <categorySources>
      ...
      <add name="Info" switchValue="All" />
    </categorySources>
  ...
```

to: **XML**

```
<configuration>
  ...
  <loggingConfiguration ...>
    ...
    <categorySources>
      ...
      <add name="Info" switchValue="All" >
        <listeners>
```

```
          <add name="Flat File Destination" />
        </listeners>
      </add>
    </categorySources>
  ...
```

Web Site Logging

Web Site Configuration File

The "Management Server" Web Site configuration file with a default installation is located here: "C:\Program Files\NovaStor\NovaBACKUP Central Management Console\WebRoot\Web\web.config"

Log File Location

With a default installation, the log files are located here: "C:\Program Files\NovaStor\NovaBACKUP Central Management Console\WebRoot"

How to enable logging for the "Management Server" Web Site

The "Management Server" Web Site configuration file is configured with logging enabled by default. This generates a web.log file in "C:\Program Files\NovaStor\NovaBACKUP Central Management Console\WebRoot" for example.

Scheduled Task Logging

Scheduled Task Configuration File

The "NovaBACKUPManagementServer" Scheduled Task configuration file with a default installation is located here: "C:\Program Files\NovaStor\NovaBACKUP Central Management Console\ScheduledTask\ManagementServer.Service.ScheduledTask.Console.exe.config"

Log File Location

With a default installation, the log files are located here: "C:\Program Files\NovaStor\NovaBACKUP Central Management Console\ScheduledTask\Logs"

How to enable logging for the "Management Server" Web Site

The "Management Server" Web Site configuration file is configured with logging enabled by default. This generates a trace.log file in the Logs folder.