

Table of Contents

Table of Contents	1
Helpful Links.....	3
Overview	4
Canauri Portal	5
User Preferences.....	7
To Update the Portal Logos	7
Creating Customer Accounts	8
Notification Settings.....	11
Agent Default/Customer Settings.....	12
Fallback email:.....	13
User Auto Protect:	13
Shares Auto Protect:	13
Auto Protect System Root:.....	13
Auto New Subfolders:	13
Driver:.....	13
Native File Monitoring:	13
Extension Change Monitoring:.....	13
Apply to existing endpoints:	13
Folder Exclusion:	13
Process Allow List:.....	13
Installing Canauri.....	14
Manual Installation Instructions	15

Uninstall Canauri.....	16
Method 1: Retire and Uninstall from Portal	16
Method 2: Retire from Portal. Uninstall from the apps & features/ Control panel.	17
Method 3: Canauri installed and not activated scenario.....	17
Automating the Canauri Installation.....	18
RMM Installation.....	18
GPO Deployment	19
PowerShell Script	20
Third-Party Application	21
Configure Canauri Server Settings	22
Remediation/Windows Firewall	23
Honeypot Files	24
Responding to Canauri Alerts	25
Canauri Reports.....	26
Active Paid Licenses Report	26
Configure Agent Offline Report	27
Frequently Asked Questions (FAQ).....	28

Helpful Links

Schedule Install Assistance

<https://www.canauri.com/schedule-a-walk-through/>

Canauri Portal

<https://portal.canauri.com>

Video - Two-Minute Install

<https://www.canauri.com/msp-partners/canauri-installation-video/>

Video - Canauri Portal – Adding a New Customer

<https://www.canauri.com/msp-partners/canauri-portal-adding-a-new-customer/>

Video - Canauri install via Group Policy

<https://www.canauri.com/msp-partners/canauri-gpo-deployment/>

Video - Canauri Install via PowerShell Script

<https://www.canauri.com/msp-partners/canauri-install-via-powershell-script-2/>

Video – Canauri Demo, Stopping 7 Ransomware Variants

<https://www.canauri.com/msp-partners/attack-demo-for-prospective-customers/>

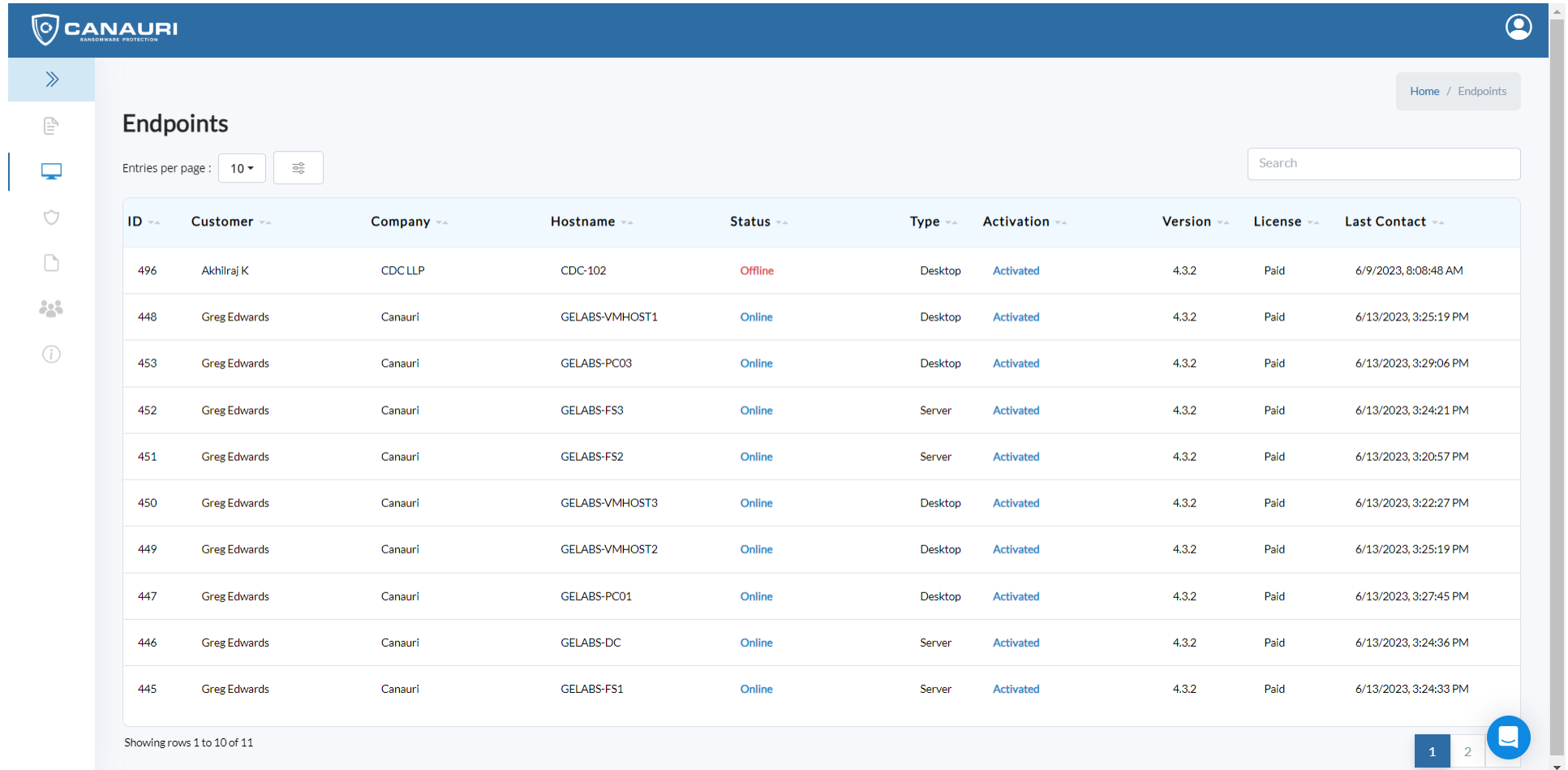
Overview

Canauri was designed to detect and stop actively running ransomware. It is your best line of defense in stopping actively running ransomware that has bypassed other products in the security stack. Canauri protects endpoints by deploying hidden honeypot files to the protected folders. Canauri monitors these hidden honeypot files for ransomware activity and reacts in the event of a ransomware attack. Canauri also has advanced monitoring features like native file monitoring and extension change monitoring that provide additional protection on top of the hidden honeypot files. Lastly, Canauri's advanced driver protection provides faster detection and better intelligence that complements our original honeypot file detection method.

This document outlines how to create and configure new customer accounts in the Canauri web portal and assumes the perspective of the MSP. It also covers configuring Canauri settings, manual installation of the product and mass deployments using Group Policy or an RMM.

Canauri Portal

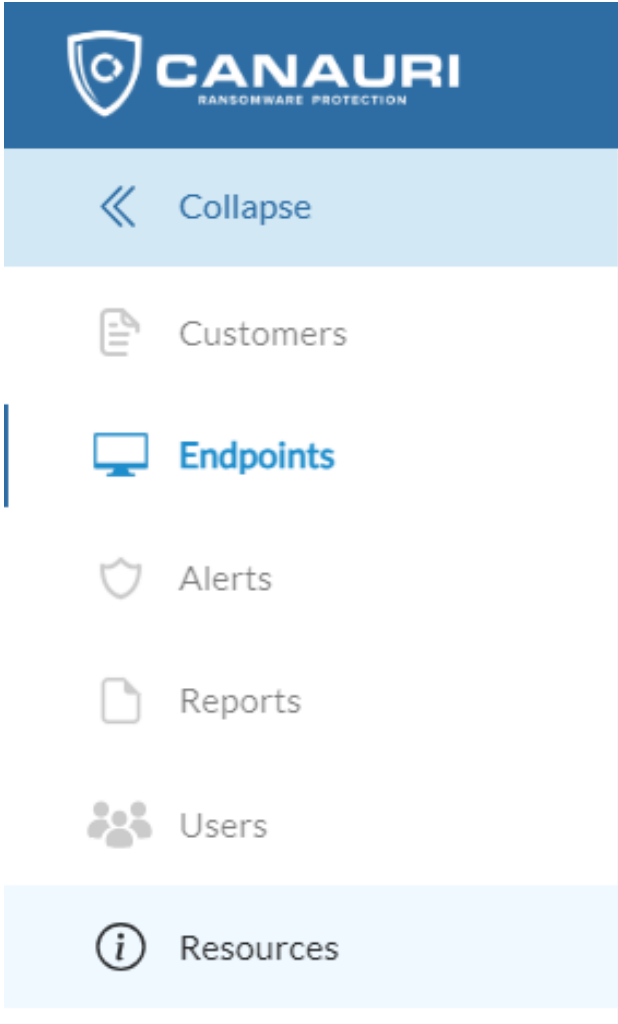
The Canauri Portal URL is <https://portal.canauri.com>. Once you have received your credentials, please login to the portal. All administration of Canauri customer accounts and endpoints is performed from the portal.








The screenshot shows the Canauri Portal interface. At the top, there is a navigation bar with the Canauri logo and a user profile icon. Below the navigation bar, the page title "Endpoints" is displayed. To the right of the title, there is a breadcrumb trail "Home / Endpoints" and a search input field. Below the search field, there is a dropdown menu for "Entries per page" set to "10" and a refresh icon. The main content area is a table with 11 rows of endpoint data. The table has columns for ID, Customer, Company, Hostname, Status, Type, Activation, Version, License, and Last Contact. The status column uses color coding: red for "Offline" and blue for "Online". The activation column shows "Activated" in blue. The last contact column shows timestamps. At the bottom left, it says "Showing rows 1 to 10 of 11". At the bottom right, there is a pagination control showing "1" and "2" with a blue circle containing a white icon.

ID	Customer	Company	Hostname	Status	Type	Activation	Version	License	Last Contact
496	Akhilraj K	CDC LLP	CDC-102	Offline	Desktop	Activated	4.3.2	Paid	6/9/2023, 8:08:48 AM
448	Greg Edwards	Canauri	GELABS-VMHOST1	Online	Desktop	Activated	4.3.2	Paid	6/13/2023, 3:25:19 PM
453	Greg Edwards	Canauri	GELABS-PC03	Online	Desktop	Activated	4.3.2	Paid	6/13/2023, 3:29:06 PM
452	Greg Edwards	Canauri	GELABS-FS3	Online	Server	Activated	4.3.2	Paid	6/13/2023, 3:24:21 PM
451	Greg Edwards	Canauri	GELABS-FS2	Online	Server	Activated	4.3.2	Paid	6/13/2023, 3:20:57 PM
450	Greg Edwards	Canauri	GELABS-VMHOST3	Online	Desktop	Activated	4.3.2	Paid	6/13/2023, 3:22:27 PM
449	Greg Edwards	Canauri	GELABS-VMHOST2	Online	Desktop	Activated	4.3.2	Paid	6/13/2023, 3:25:19 PM
447	Greg Edwards	Canauri	GELABS-PC01	Online	Desktop	Activated	4.3.2	Paid	6/13/2023, 3:27:45 PM
446	Greg Edwards	Canauri	GELABS-DC	Online	Server	Activated	4.3.2	Paid	6/13/2023, 3:24:36 PM
445	Greg Edwards	Canauri	GELABS-FS1	Online	Server	Activated	4.3.2	Paid	6/13/2023, 3:24:33 PM

The portal is the central management system for Canauri agents. You can create new customer accounts, update notification and endpoint settings and monitor agent status from the portal. Here is a screenshot of the sandwich menu and a description of each item listed in the menu.



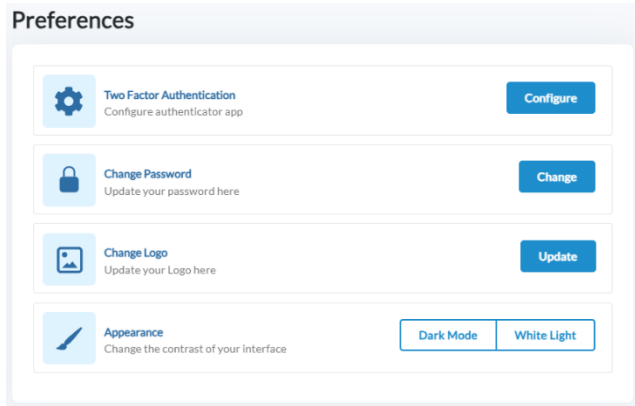
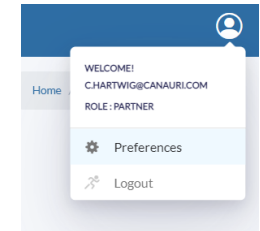
The screenshot shows a vertical sidebar menu for the Canauri portal. At the top is a dark blue header with the Canauri logo and name. Below it is a light blue bar with a double-left arrow icon and the text 'Collapse'. The main menu items are: 'Customers' (document icon), 'Endpoints' (monitor icon, highlighted with a blue vertical bar), 'Alerts' (shield icon), 'Reports' (document icon), 'Users' (group of people icon), and 'Resources' (info icon, highlighted with a light blue bar). To the right of the menu, a list of descriptions is provided for each item.

 Collapse	
 Customers	Customers: View the customer list
 Endpoints	Endpoints: View activated endpoints
 Alerts	Alerts: View Canauri Alerts
 Reports	Reports: Run reports
 Users	Users: Configure user accounts
 Resources	Resources: Access training manuals and videos

User Preferences

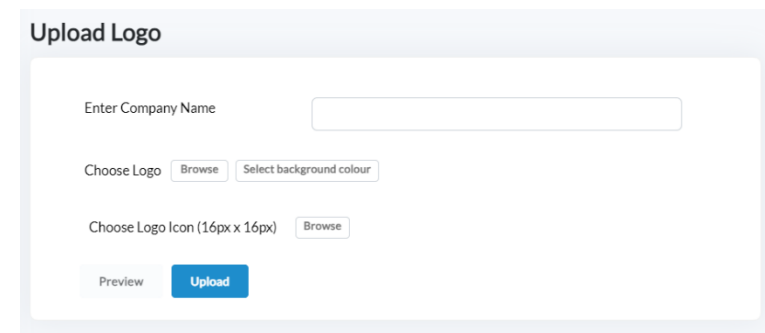
User preferences are found in the portal by clicking the user icon in the upper right corner of the browser.

There are several options available to configure in preferences. The user can update 2FA, change their password, update the logos used and change the appearance in the web browser.



To Update the Portal Logos

1. Login to the Canauri portal at portal.canauri.com
2. Click the User Profile Icon in the upper right of the page
3. Select Preferences
4. Click "Update" button next to Change Logo
5. Enter Company Name
6. Choose a new logo by click "Browse"
7. Change the background color by clicking "Select Background Color"
8. Click "Browse" to Choose Logo Icon
9. Preview and Upload the changes

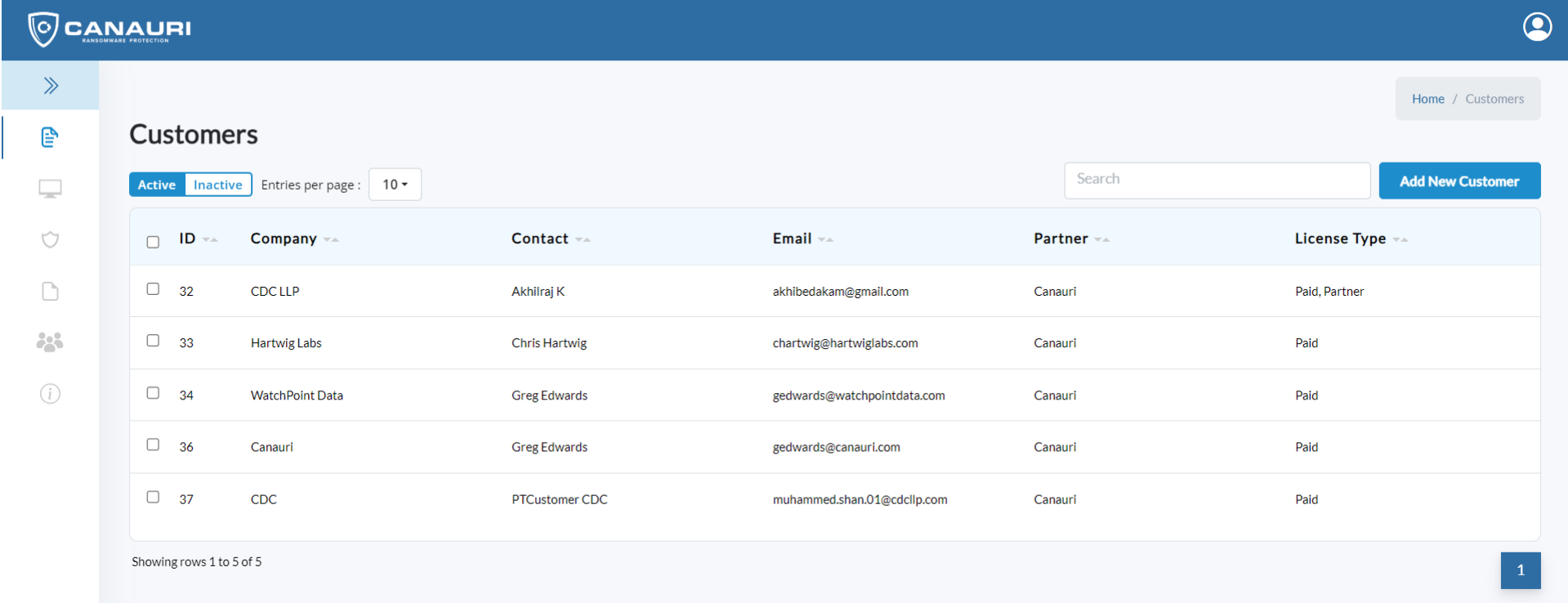


The new logo will replace the Canauri logos in the portal and update the logo on the alert emails.

Creating Customer Accounts

Login to the [Canauri Portal](#) with the credentials provided to you. (If this is the first time you have logged in, you will be required to set up 2FA for secure account logins.)

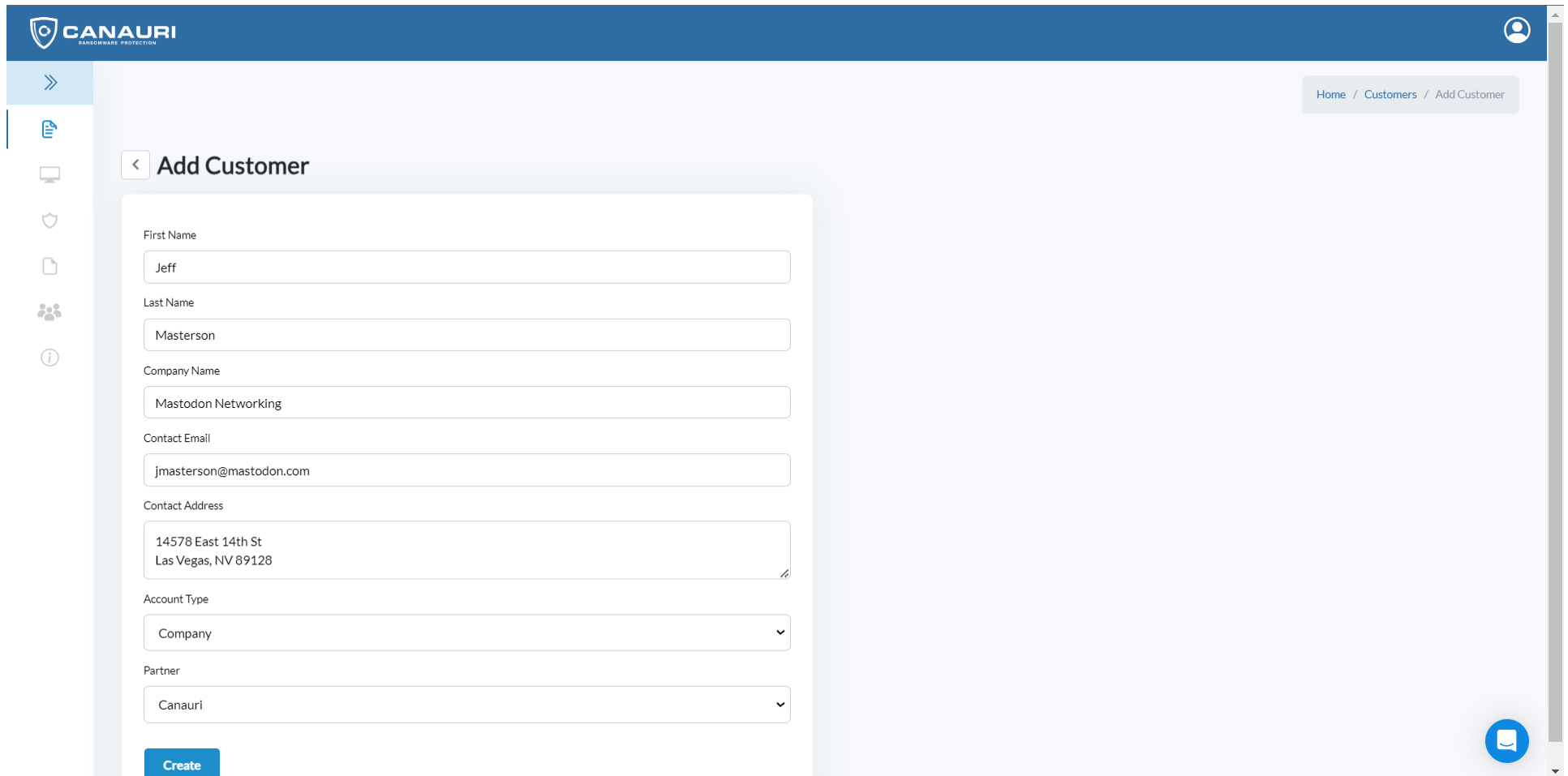
Select “Add New Customer” and fill out the required information. A unique email address is required per customer.



The screenshot shows the Canauri web application interface for managing customers. The header includes the Canauri logo and a user profile icon. The main content area is titled "Customers" and features a navigation sidebar on the left with icons for home, documents, devices, security, files, users, and help. The main area contains a table of customer records with columns for ID, Company, Contact, Email, Partner, and License Type. There are also filters for "Active" and "Inactive" status, a search bar, and an "Add New Customer" button. The table shows 5 rows of data, and a pagination indicator at the bottom right shows "1" out of 5 rows.

ID	Company	Contact	Email	Partner	License Type
32	CDC LLP	Akhilraj K	akhibedakam@gmail.com	Canauri	Paid, Partner
33	Hartwig Labs	Chris Hartwig	chartwig@hartwiglabs.com	Canauri	Paid
34	WatchPoint Data	Greg Edwards	gedwards@watchpointdata.com	Canauri	Paid
36	Canauri	Greg Edwards	gedwards@canauri.com	Canauri	Paid
37	CDC	PTCustomer CDC	muhammed.shan.01@cdclp.com	Canauri	Paid

Click "Create" when you are finished entering the customer information.



CANAURI RANSOMWARE PROTECTION

Home / Customers / Add Customer

< Add Customer

First Name
Jeff

Last Name
Masterson

Company Name
Mastodon Networking

Contact Email
jmasterson@mastodon.com


Contact Address
14578 East 14th St
Las Vegas, NV 89128


Account Type
Company

Partner
Canauri

Create

Click "New License" button to generate a key for the customer and to create the imbedded key installer download link.





>>

<
>

Home / Customers / Customer Details

<
>
<
>
<
>
<
>
<
>

Jeff Masterson

🗑️

Edit Details

Customer Details

Name	Jeff Masterson
Partner Name	Canauri
Email	jmasterson@mastodon.com
Partner Contact	chartwig@canauri.com
Company	Mastodon Networking
Servers Activated	0
Desktop Activated	0

Devices

Notification Settings

Agent Default Settings

Deactivate

Customer Licenses

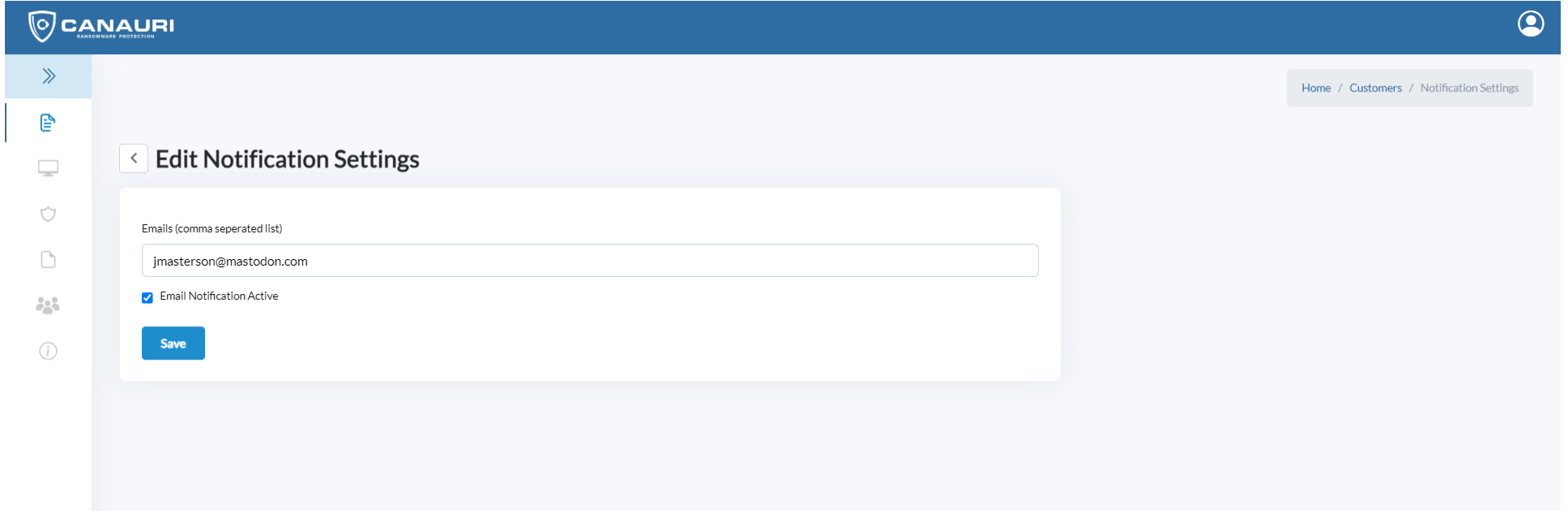
New License

Key	Active Servers	Active Desktops	Expiration Date	Type	Actions
AG33-0AYB-69HK-SWQO	0	0	12/30/2099	Paid	<div style="display: flex; gap: 10px;"> <div style="border: 1px solid #ccc; padding: 2px 5px; font-size: 12px;">🗑️ Devices</div> <div style="border: 1px solid #ccc; padding: 2px 5px; font-size: 12px; color: #007bff;">📄 Download</div> </div>

💬

Notification Settings

When an alert is generated by Canauri, the agent checks in with the portal to verify the proper email address for notification. If the portal cannot be reached, the Canauri agent will use its internal SMTP server to send an email to the address listed under “Agent Default Settings.” The “Notification Settings” email field will accept a comma separated list of emails.



CANAURI RANSOMWARE PROTECTION

Home / Customers / Notification Settings

< Edit Notification Settings

Emails (comma seperated list)

Email Notification Active

Save

Agent Default/Customer Settings

These settings will be pushed to the agent after installation. These settings can also be updated and pushed down to existing agents. **We recommend configuring agent settings and folder exclusions first via the portal, then install Canauri to your endpoints.**

CANAU RI RANSOMWARE PROTECTION
User Profile Icon

Home / Customers / Customer Settings

Customer Settings

Fallback email ⓘ

Configuration

- User Auto Protect ⓘ
- Driver Detection
- Shares Auto Protect ⓘ
- Native File Protection ⓘ
- Auto Protect System Root ⓘ
- Auto New Sub Folders ⓘ
- Extension Change Monitor ⓘ

Default Upgrade Channel

Apply to existing endpoints
 Save

Folder Exclusion ⓘ Add

10 ▾
🗑️

<input type="checkbox"/>	Path	Search
No Data		

Process Allow List ⓘ Add

10 ▾
🗑️

<input type="checkbox"/>	Path	Search
No Data		

Fallback email:

The email is pushed to the agent and will be used if the agent cannot communicate with the portal to send the email.

User Auto Protect:

When checked, Canauri will protect all user profiles automatically.

Shares Auto Protect:

When checked, Canauri will protect the shared folders automatically.

Auto Protect System Root:

When checked, Canauri will protect the default volume automatically.

Auto New Subfolders:

Automatically protect new subfolders created in a protected directory.

Driver:

The driver feature improves upon the first generation of Canauri that relied on Windows event logging only. Because the driver has visibility to the kernel it can gather more information about an event, and it can do it much faster. This next generation feature for Canauri can detect and stop an attack in a second or less.

Native File Monitoring:

For every folder protected by Canauri, native file monitoring can also be enabled. Native file monitoring is a process of recruiting data files to monitor. This feature prevents ransomware from evading detection by skipping hidden files. By monitoring native files, you increase the speed of detection as well because now we are seeing the ransomware hit data files and honeypot files at the same time.

Extension Change Monitoring:

Almost every variant of ransomware changes the file extension on files after they have been encrypted so monitoring for X number of file extension changes in X number of seconds is a very good way to detect ransomware activity.

Apply to existing endpoints:

Apply setting to some or all the existing endpoints.

Folder Exclusion:

Exclude a folder from protection if an application is generating false positives.

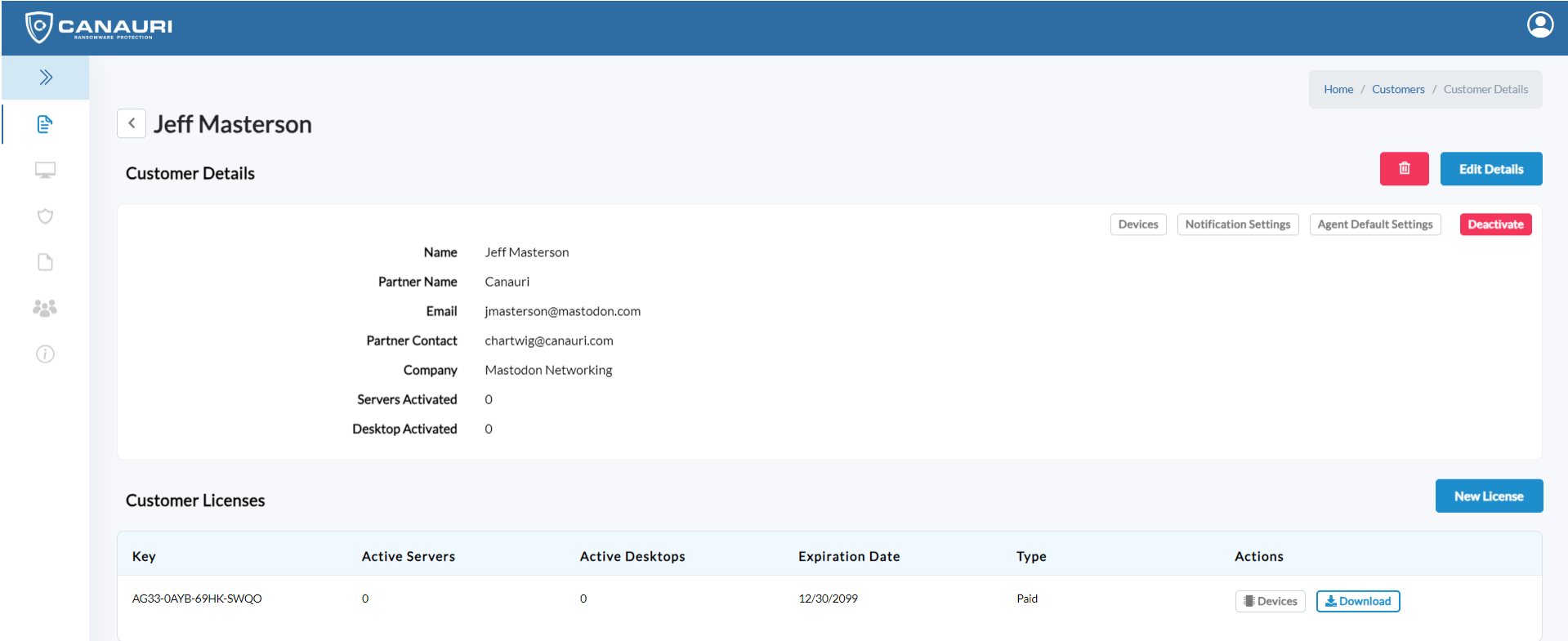
Process Allow List:

Whitelist a process by name or file path.

Installing Canauri

Before installing Canauri, make sure you have read all previous sections detailing creating a new customer, and configuring Notification Settings, and Agent Default Settings.

After the customer license key has been generated you will notice a “Download” button to the right of the key. By clicking the download button your browser will download the key embedded installer. Next you can install Canauri manually on each endpoint, or you have several options to automate the installation. Automated methods include deployment via Group Policy, PowerShell scripting, RMM tools and third-party installers.



The screenshot shows the Canauri web interface. At the top, there is a navigation bar with the Canauri logo and a user profile icon. Below the navigation bar, there is a breadcrumb trail: Home / Customers / Customer Details. The main content area is titled "Jeff Masterson" and "Customer Details". On the right side of the details section, there are buttons for "Edit Details" (blue), "Deactivate" (red), "Devices" (grey), "Notification Settings" (grey), and "Agent Default Settings" (grey). The details section contains the following information:

- Name: Jeff Masterson
- Partner Name: Canauri
- Email: jmasterson@mastodon.com
- Partner Contact: chartwig@canauri.com
- Company: Mastodon Networking
- Servers Activated: 0
- Desktop Activated: 0

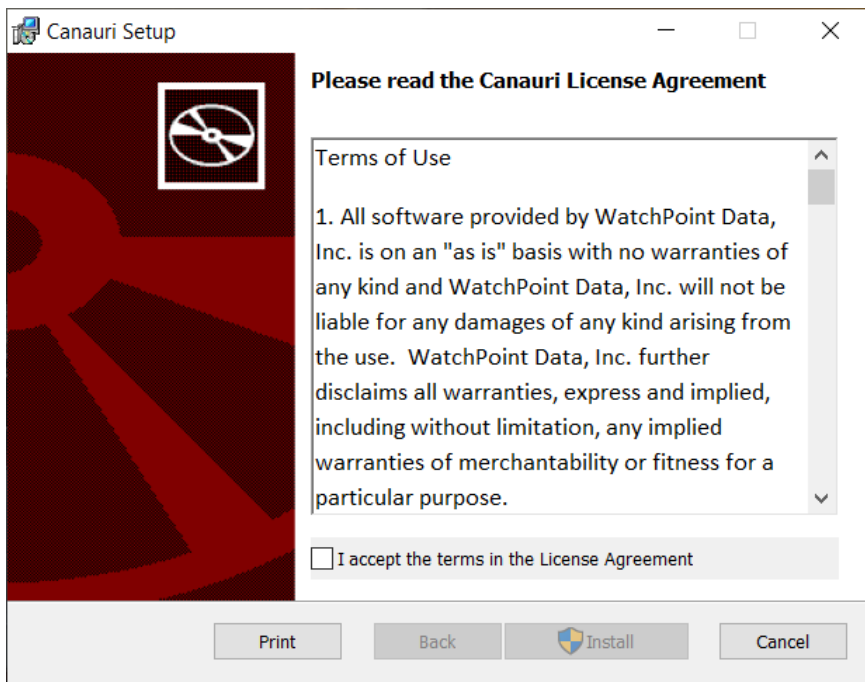
Below the details section, there is a "Customer Licenses" section with a "New License" button (blue). The licenses are displayed in a table:

Key	Active Servers	Active Desktops	Expiration Date	Type	Actions
AG33-0AYB-69HK-SWQO	0	0	12/30/2099	Paid	Devices Download

Manual Installation Instructions

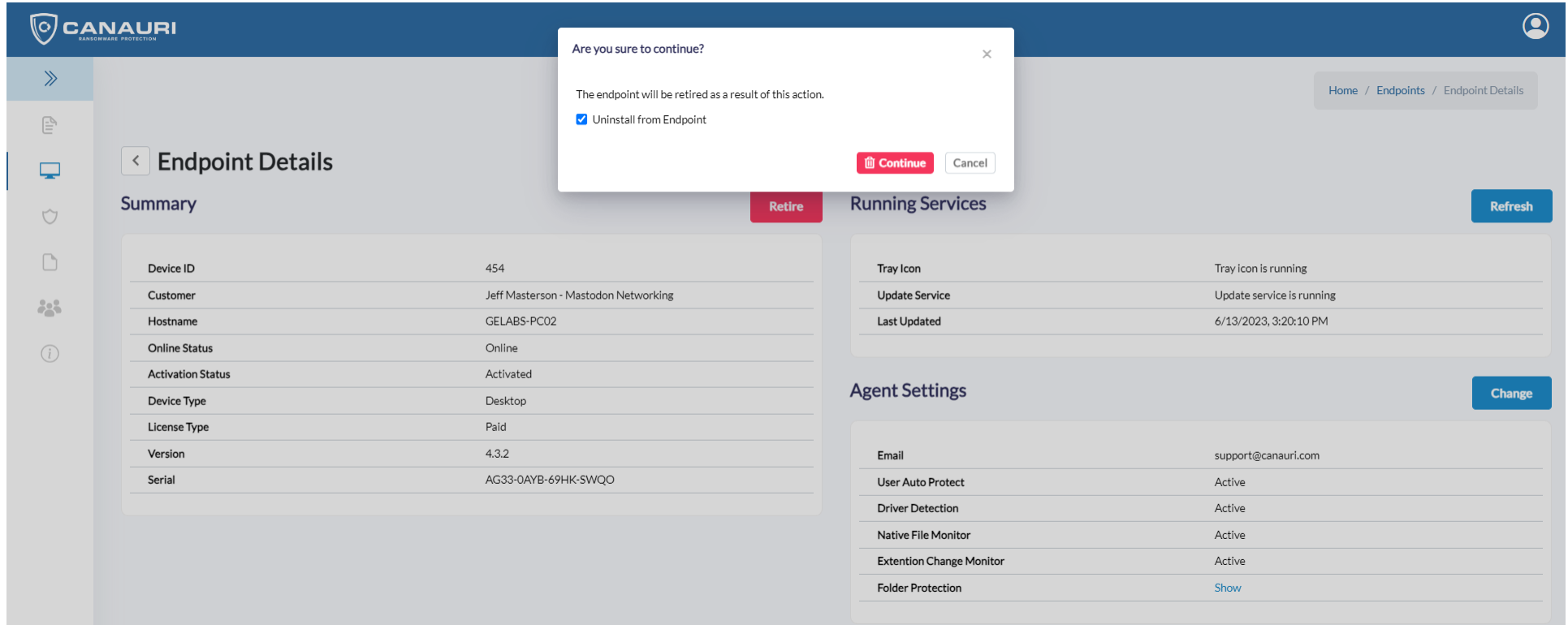
- 1) Download the key embedded installer from the Customer Details page in the Canauri Portal.
- 2) Double-click Canauri-installer.msi to start the software installation.
- 3) Review the Canauri License Agreement then check the box “I accept the terms in the License Agreement.”
- 4) Next, click the “Install” button.
- 5) Click “Finish” once the installation is complete.
- 6) The Canauri Installation is complete.

After the installation, Canauri will sync settings with the portal and run its first integrity check. During the integrity check, Canauri syncs the agent settings and begins the automated deployment and protection process.



Uninstall Canauri

There are several methods available to uninstall Canauri. The product should be retired and uninstalled from the Canauri Portal whenever possible.



The screenshot shows the Canauri portal interface. A modal dialog box is open in the center, asking for confirmation to retire an endpoint. The dialog text reads: "Are you sure to continue?", "The endpoint will be retired as a result of this action.", and "Uninstall from Endpoint" (checked). There are "Continue" and "Cancel" buttons. In the background, the "Endpoint Details" page is visible, featuring a "Summary" table, a "Retire" button, "Running Services" section, and "Agent Settings" section.

Summary	
Device ID	454
Customer	Jeff Masterson - Mastodon Networking
Hostname	GELABS-PC02
Online Status	Online
Activation Status	Activated
Device Type	Desktop
License Type	Paid
Version	4.3.2
Serial	AG33-0AYB-69HK-SWQO

Running Services	
Tray Icon	Tray icon is running
Update Service	Update service is running
Last Updated	6/13/2023, 3:20:10 PM

Agent Settings	
Email	support@canauri.com
User Auto Protect	Active
Driver Detection	Active
Native File Monitor	Active
Extention Change Monitor	Active
Folder Protection	Show

Method 1: Retire and Uninstall from Portal

1. Click on an endpoint from the Endpoint List to open Endpoint Details.
2. Click "Retire" button.
3. Ensure "Uninstall from Endpoint" is selected and press "Continue".
4. The client will check in with the portal every 15 minutes and schedule the uninstall if it has been requested.
5. The client will schedule an uninstall task in the task scheduler after 2 minutes.
6. Canauri will uninstall silently.

Method 2: Retire from Portal. Uninstall from the apps & features/ Control panel.

1. Retire from the portal with uninstall checkbox checked.
2. Perform manual uninstall from the apps & features/ Control panel.
3. The Canauri agent will check in with the portal and then uninstall.

Method 3: Canauri installed and not activated scenario.

1. Normal apps & features/ Control panel uninstall will work since the agent has not been activated and has not checked in with the portal.

Automating the Canauri Installation

The Canauri installation can be automated in several ways. We recommend utilizing an RMM for automated installations; however, if an RMM isn't available you can still automate the installation using Windows GPO on a domain controller, a powershell script, or third-party installers.

RMM Installation

Canauri supports installation via several different RMM products. Please consult your RMM documentation, check the resources tab for further info about RMM installations or reach out to <mailto:support@canauri.com> and set up a meeting to discuss your RMM deployment.



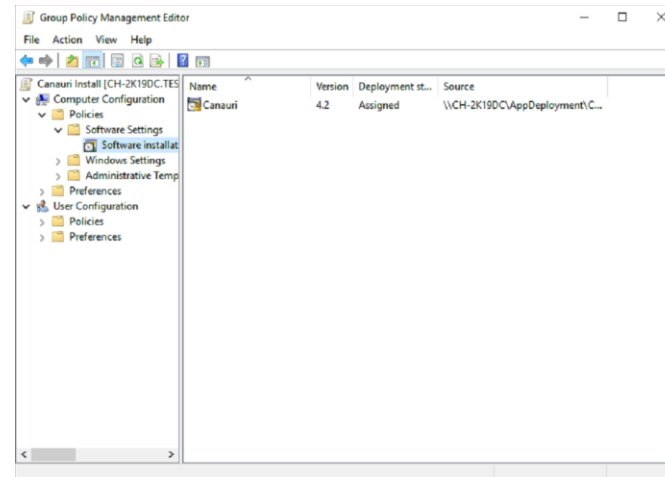
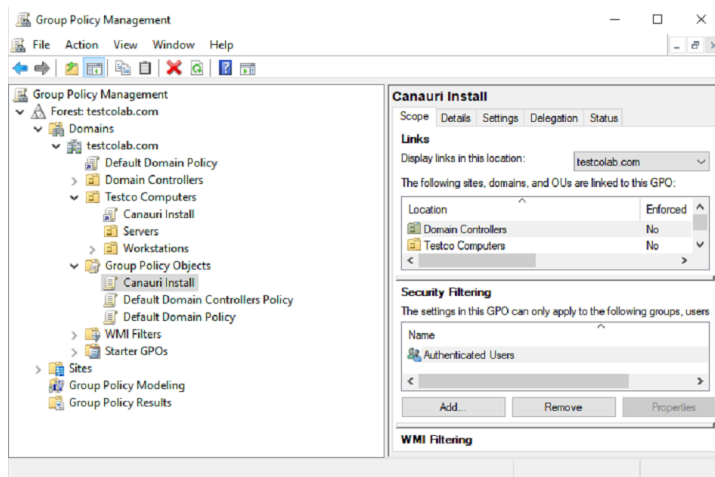
GPO Deployment

Canauri can be pushed out using Windows Group Policy.

How to use Group Policy to remotely install software in Windows Server 2003 and Windows Server 2008.

These instructions apply to all versions of Windows Server.

<https://support.microsoft.com/en-us/help/816102/how-to-use-group-policy-to-remotely-install-software-in-windows-server>



PowerShell Script

The PowerShell script can be run independently or inside an RMM. This makes using the script very versatile in any network situation. The PowerShell script sets three variables: the web path for download, the local path to copy files to and the path to the shared network folder that contains the json config file.

Create a powershell script with the following information and then you can run this script from your RMM or on the customer network.

```
#variables
$cs_web_path = '<insert URL to customer imbedded key installer here>'
$cs_local_path = 'C:\Temp\Canauri_Install'

#Check if temp directory exists
if(Get-Item -Path $cs_local_path -ErrorAction Ignore)
{
Write-Host "Folder Exists"
}
else
{
#PowerShell Create directory if not exists
New-Item $cs_local_path -ItemType Directory
}
#Download latest version of Canauri and save to temp
Invoke-WebRequest -uri $cs_web_path -OutFile $cs_local_path\Canauri-installer.msi

#Install Canauri
msiexec /qn /i $cs_local_path\Canauri-installer.msi /!*v
```

Third-Party Application

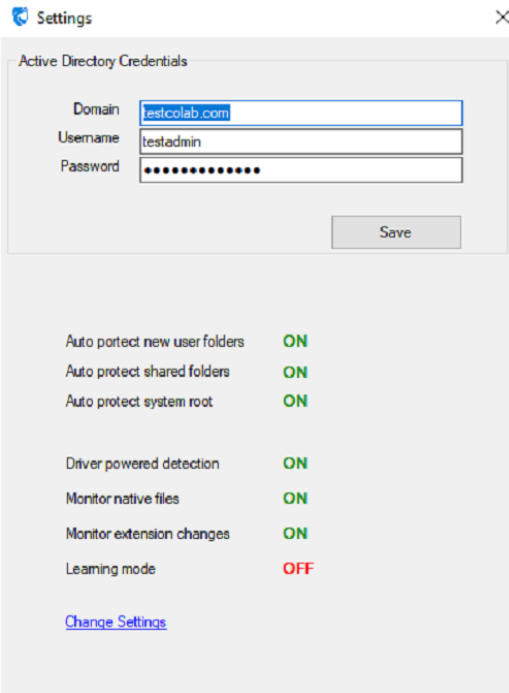
It is possible to install Canauri via a third-party installer. We do not provide support for third-party installers, but they follow the same principle as the other methods of installation. You simply create an install job then push to a target list of endpoints.



Configure Canauri Server Settings

Active Directory Credentials: When installing on a server, you should also configure the domain settings. Configuring the domain settings will allow Canauri Server to send a shutdown command to the workstation after it has been isolated from the network share. If the domain settings are not configured, Canauri will still stop the attack against the network share by isolating the infected host from the share, but the workstation will not get shut down.

Server Settings



The screenshot shows the Canauri Settings window. The 'Active Directory Credentials' section contains three input fields: 'Domain' with the value 'testcolab.com', 'Username' with the value 'testadmin', and 'Password' with a masked password. A 'Save' button is located below these fields. Below the credentials section, there are several toggle switches for various protection features:

Auto protect new user folders	ON
Auto protect shared folders	ON
Auto protect system root	ON
Driver powered detection	ON
Monitor native files	ON
Monitor extension changes	ON
Learning mode	OFF

A 'Change Settings' link is located at the bottom left of the window.

Log in to the server and open Canauri from the desktop or tray icon. Enter the Active Directory Credentials. Make sure and click "Save" after entering the settings and close the Settings window. Canauri will verify and alert you if your credentials are invalid.

Remediation/Windows Firewall

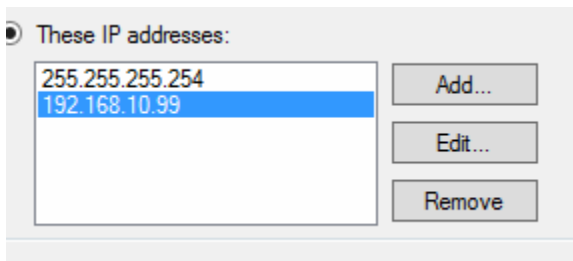
You should know what to do once an infected computer is identified and disconnected from the server. Canauri creates a Windows firewall rule that blocks an infected computer and prevents it from connecting to the server.

The firewall rule will not be visible until ransomware activity is identified for the first time. After the first attack or attack test, you will see this listed as an inbound firewall rule.



Once an infected computer is identified, you'll right-click, select the scope tab to remove the infected computer's IP address. Please note that 255.255.255.254 is there by default.

Select the infected computer's IP address and click "Remove" then "OK."



Honeypot Files

Canauri creates ‘Honeypot files’ within the directories selected for protection. The honeypot files are used as bait by Canauri as it continuously monitors the files for signs of ransomware activity. The screenshot to the right is an example of the honeypot files created by Canauri.

The honeypot files have random file names, random file extensions and random file sizes. This allows the honeypot files to comingle between company data files and detect the ransomware attack wherever it may start in the protected folder.

The hidden attribute hides the honeypot files from end users but not from ransomware. It’s important to make sure that workstations on your network do not have “View hidden files” turned on, so users avoid generating a false positive alert by deleting the hidden honeypot files. If a user deletes any of the files, Canauri will redeploy those files automatically as long as the directory hasn’t been deleted as well.

Name	Date modified	Type	Size
Add Pop.wma	5/20/2022 6:18 PM	WMA File	28 KB
Checkpoint Test.doc	5/20/2022 6:18 PM	Microsoft Word 9...	40 KB
Enable Publish.mov	5/20/2022 6:18 PM	MOV File	69 KB
Group Expand.ram	5/20/2022 6:18 PM	RAM File	28 KB
Join Stop.mpeg	5/20/2022 6:18 PM	MPEG File	24 KB
Receive Disable.wmv	5/20/2022 6:18 PM	WMV File	64 KB
Remove Set.mpeg	5/20/2022 6:18 PM	MPEG File	35 KB
Save Protect.ogg	5/20/2022 6:18 PM	OGG File	26 KB
Step Resolve.ppt	5/20/2022 6:18 PM	Microsoft PowerP...	34 KB
Submit Exit.midi	5/20/2022 6:18 PM	MIDI Sequence	27 KB
Assert Revoke.mpeg	5/20/2022 6:18 PM	MPEG File	49 KB
Debug Format.pdf	5/20/2022 6:18 PM	Adobe Acrobat D...	39 KB
Disconnect Unpublish.doc	5/20/2022 6:18 PM	Microsoft Word 9...	20 KB
Exit Redo.mpg	5/20/2022 6:18 PM	MPG File	32 KB
Expand Compare.doc	5/20/2022 6:18 PM	Microsoft Word 9...	51 KB
Grant Approve.docx	5/20/2022 6:18 PM	Microsoft Word D...	68 KB
Merge Convert.rm	5/20/2022 6:18 PM	RM File	42 KB
Open Register.mpeg3	5/20/2022 6:18 PM	MPEG3 File	21 KB
Pop Suspend.midi	5/20/2022 6:18 PM	MIDI Sequence	37 KB
Register Initialize.mp4	5/20/2022 6:18 PM	MP4 File	27 KB
Select Skip.avi	5/20/2022 6:18 PM	Video Clip	25 KB
Submit Merge.pptx	5/20/2022 6:18 PM	Microsoft PowerP...	55 KB
Switch Step.doc	5/20/2022 6:18 PM	Microsoft Word 9...	20 KB
Test Get.doc	5/20/2022 6:18 PM	Microsoft Word 9...	31 KB
Update Receive.ram	5/20/2022 6:18 PM	RAM File	41 KB

Responding to Canauri Alerts

Canauri displays a desktop alert when a ransomware attack is detected, and Canauri also sends an email alert to the email address configured in settings. It is important that administrators examine these alerts immediately. This document outlines what to do when a ransomware alert message is received.

Sample Alert Message

Ransomware attack detected on Computer:SCOTT-PC User:Scott at Time:2022-06-13 15:30:49 GMT+00:00. A potentially malicious process of C:\temp\ransomware.EXE has been stopped. C:\Users\Jonathan\Desktop\Projects\CWT\Watch Confirm.mov was the last file overwritten by the potentially malicious process. Please check the host immediately.

Determine if Alert is a False Positive or a Real Ransomware Attack

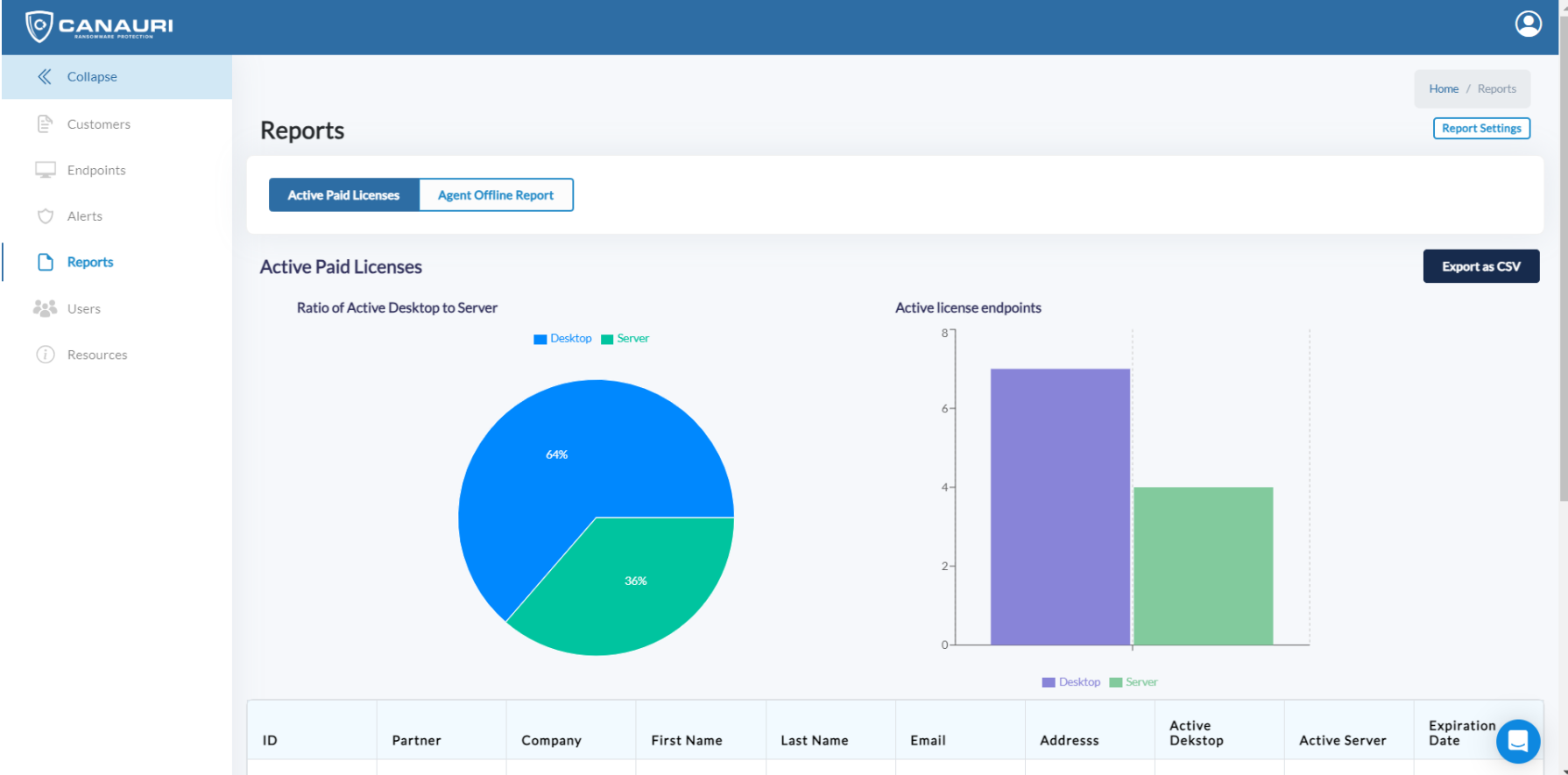
If a user does not have hidden files turned off and that user tries to rename, move or delete a watcher file, the Canauri alert mechanism will be activated. Ensure viewing hidden files is turned off for the user and consider configuring GPO to turn off viewing of hidden files for all users.

Ransomware Attack

If an alert is generated and you find a few files that have been encrypted in the folder mentioned in the ransomware alert, you will know a real ransomware attack was detected and stopped. In this case, you will want to pull the infected machine off the network and remove the infection or reimage the machine before deploying it back on the network.

Canauri Reports

Login to the Canauri portal and configure your Agent Offline Report. This report will query your customer endpoints and report any servers or workstations that are offline for the time period. Canauri suggests setting the Agent Offline Report to email you if a server has been offline for 24 hours and if a workstation has been offline for 30 days or more.



Active Paid Licenses

Ratio of Active Desktop to Server

Category	Percentage
Desktop	64%
Server	36%

Active license endpoints

Category	Count
Desktop	7
Server	4

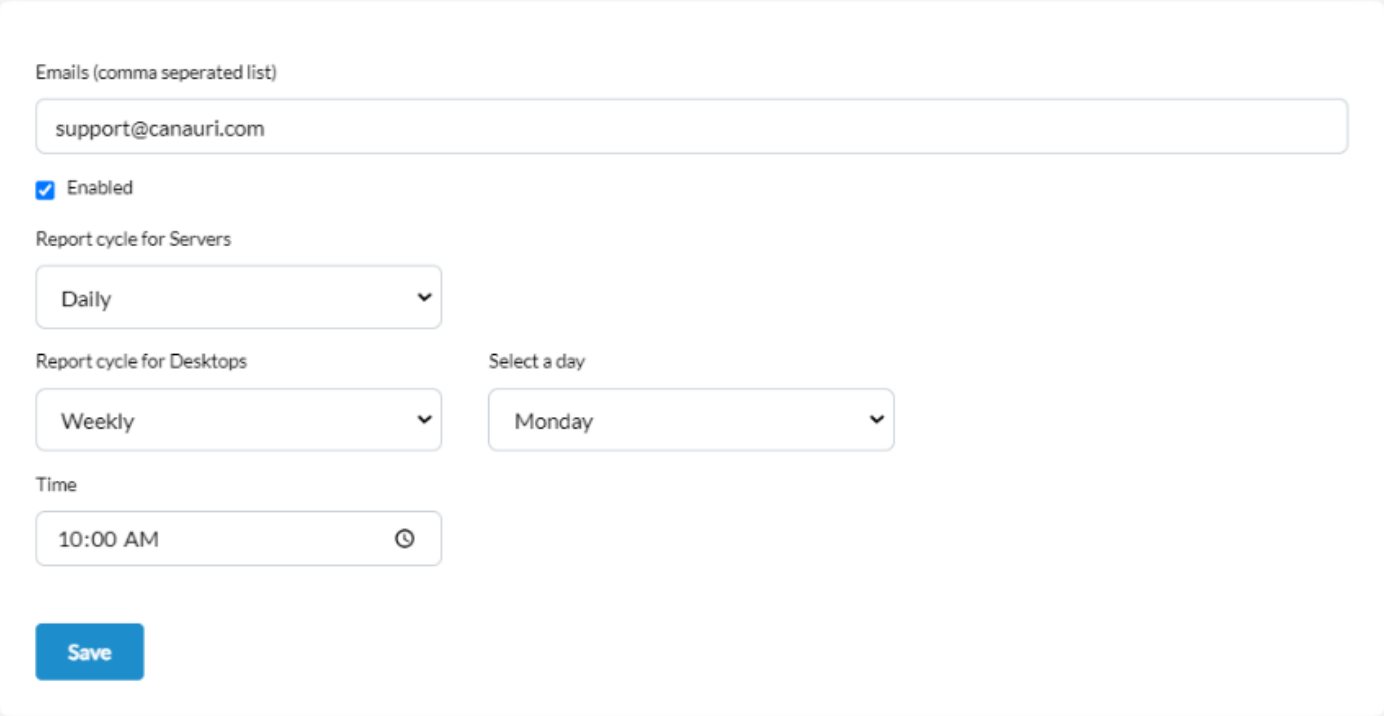
ID	Partner	Company	First Name	Last Name	Email	Address	Active Dekstop	Active Server	Expiration Date
----	---------	---------	------------	-----------	-------	---------	----------------	---------------	-----------------

Active Paid Licenses Report

This report shows the number of active server and active desktop licenses activated per customer. There are no settings to configure in this report.

Configure Agent Offline Report

1. Expand the sandwich menu and choose Reports.
2. Click the “Report Settings” button in the upper right corner of the page.
3. Configure the report settings.



The screenshot shows a configuration form for Agent Offline Reports. It includes a text input for email addresses, a checked 'Enabled' checkbox, and dropdown menus for report cycles for Servers (Daily), Desktops (Weekly), and a 'Select a day' dropdown (Monday). A time picker is set to 10:00 AM, and a blue 'Save' button is at the bottom.

Emails (comma seperated list)

support@canauri.com

Enabled

Report cycle for Servers

Daily

Report cycle for Desktops

Weekly

Select a day

Monday

Time

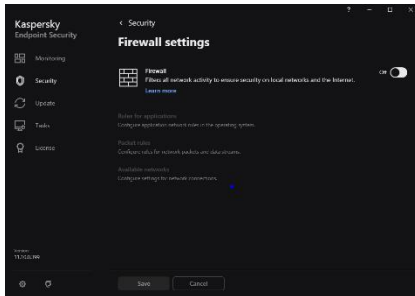
10:00 AM

Save

Frequently Asked Questions (FAQ)

Does Canauri conflict with other security products?

Kaspersky Endpoint Security – You must turn off the Firewall feature of KES on **servers only**. Canauri Server isolates infected hosts by IP address in the Windows Firewall. If KES Firewall feature is enabled, host isolation will not work.



What port does Canauri use to send alert messages?

Canauri uses SMTP to connect to a mandrill server to send email. Smtplib.mandrillapp.com:587. Please ensure this port is open.

Will Canauri automatically protect new folders?

Canauri runs an integrity check each hour and adds new folders automatically.

What is Canauri resource utilization?

Canauri uses a minimal amount of CPU and RAM. Typically, less than 1% of CPU and 200MB of RAM.

Will Canauri isolate the offending workstation automatically?

Yes. Canauri uses an algorithm to monitor specially crafted honeypot files, native files and file extension changes. When ransomware attacks your server, Canauri correlates the offending user and immediately isolates that user. It simultaneously notifies the specified email.

Do you have a PC version of Canauri?

Yes. Canauri Server and Canauri Desktop are both available for download. The single msi installer can be used for both server and desktop installations.

Does Canauri automatically update?

Yes. Canauri will automatically update to the latest version as it becomes available.

How long does it take to install Canauri?

A typical server installation will take 15 minutes or less. The workstation version installs in as little as 5 minutes.

Will my backup trigger Canauri?

No. Your backup only updates the archive bit and doesn't modify the file.

How quickly will Canauri work to stop a ransomware attack?

Canauri detects and stops a ransomware attack in as little as 1-2 seconds.

Does Canauri detect and stop all ransomware?

Canauri will detect and stop all variants of ransomware whether new or zero-day.

What if the infection happens directly on the server?

Canauri Server will stop a local attack running on the server. If you are the victim of a ransomware attack that happens directly on the server, you are the victim of a hack and attack. You should consider your entire network compromised and act accordingly.