

CionSystems Entra ID Auditor, Backup & Restore Subscription Guide



General Information: info@cionsystems.com

Online Support: support@cionsystems.com

© CionSystems Inc. ALL RIGHTS RESERVED.

This guide may not be reproduced or transmitted in part or in whole by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's use under the licensing agreement, without the written permission of CionSystems Inc.

The software application in this guide is provided under a software license (EULA) or non-disclosure agreement. This product may only be used in accordance with the terms of the applicable licensing agreement.

This guide contains proprietary information protected by copyright. For questions regarding the use of this material and product, contact us at:

CionSystems Inc.

6640 185th Ave NE

Redmond, WA-98052, USA

<http://www.CionSystems.com>

Ph: +1.425.605.5325

Trademarks

CionSystems, CionSystems Inc., the CionSystems Inc. logo, CionSystems Active Directory Manager PRO are trademarks of CionSystems. Other trademarks and registered trademarks used in this guide are the property of their respective owners.

How to signup for CionSystems Entra ID Auditor and Recovery

Respond instantly even to advanced threats. Ensure compliance with regulatory standards.

EntraID is the cornerstone for securing access to business-critical applications in Azure or Office365. Yet change reporting and vulnerability monitoring is cumbersome, time-consuming, and often impossible using out of the box tools. In a hybrid environment, it doubles the attack surface and introduces additional opportunities for ransomware and other exploits. This often results in data breaches and insider threats that can go undetected without protections in place. CionSystems Change Auditor provides real-time threat monitoring and security tracking of all key user activity and administrator changes, login activities and other object changes. Furthermore, undo any changes with a click!

- Requirements for signup
 - AZURE Subscription and tenant | Microsoft Office 365 tenant
- To signup for the service
 - Need azure subscription (pay as you go)
 - Required for Microsoft market place
 - Check how to signup for Azure subscription help file



Entra ID Audit And Recovery

A Turnkey Solution For 360 Degree Audit, Alert, Protection And Recovery Of Microsoft Entra ID For Azure And Office365



- ✓ Must have Active Azure or Office 365 Subscription to signup
- ✓ Must be a global admin in your tenant to signup

Respond instantly even to advanced threats. Ensure compliance with regulatory standards.

EntraID is the cornerstone for securing access to business-critical applications in Azure or Office365. Yet change reporting and vulnerability monitoring is cumbersome, time-consuming, and often impossible using out of the box tools. In a hybrid environment, it doubles the attack surface and introduces additional opportunities for ransomware and other exploits. This often results in data breaches and insider threats that can go undetected without protections in place. CionSystems Change Auditor provides real-time threat monitoring and security tracking of all key user activity and administrator changes, login activities and other object changes. Furthermore, undo any changes with a click!

Easy Recovery

Establish a complete Entra ID recovery plan that minimizes downtime with no impact on end users. CionSystems Easy Recovery makes it possible. Easily select exactly what you need or recover many users, groups and group memberships in bulk without PowerShell. You can further select specific attributes and recover. Don't take any chances, mitigate the risk of data loss or service outage from human error and save valuable time and resources.

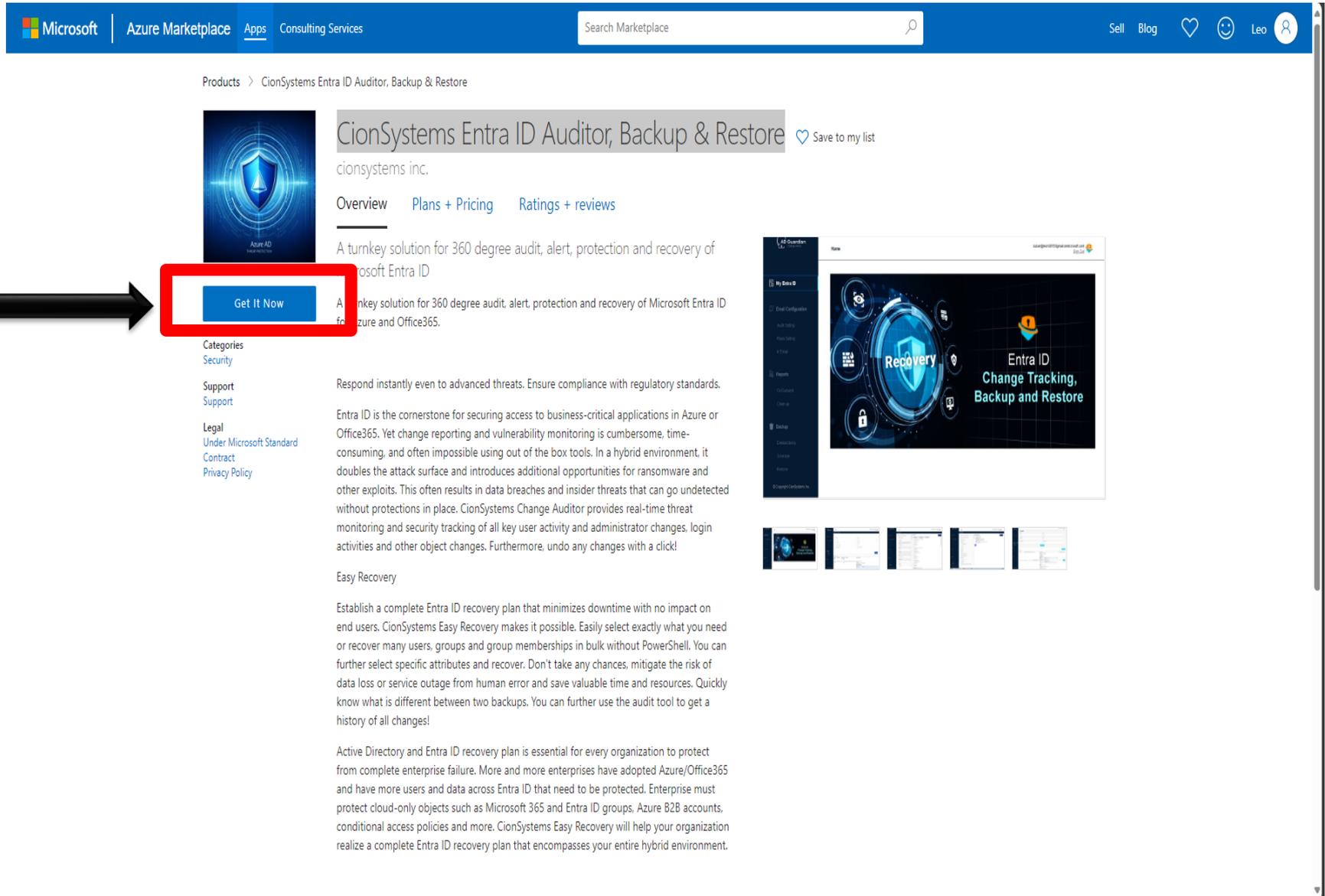
OR

- Go to the Azure market place portal and login using your tenant admin account for the tenant you are signing up for our service:



[Microsoft Azure Marketplace - CionSystems](#)
[Entra ID Auditor, Backup & Restore](#)

Click on “Get It Now” button



Microsoft | Azure Marketplace | Apps | Consulting Services

Search Marketplace

Sell | Blog | Leo

Products > CionSystems Entra ID Auditor, Backup & Restore

CionSystems Entra ID Auditor, Backup & Restore

Save to my list

cionsystems inc.

Overview | Plans + Pricing | Ratings + reviews

A turnkey solution for 360 degree audit, alert, protection and recovery of Microsoft Entra ID

A turnkey solution for 360 degree audit, alert, protection and recovery of Microsoft Entra ID for Azure and Office365.

Get It Now

Categories
Security

Support
Support

Legal
Under Microsoft Standard Contract
Privacy Policy

Respond instantly even to advanced threats. Ensure compliance with regulatory standards.

Entra ID is the cornerstone for securing access to business-critical applications in Azure or Office365. Yet change reporting and vulnerability monitoring is cumbersome, time-consuming, and often impossible using out of the box tools. In a hybrid environment, it doubles the attack surface and introduces additional opportunities for ransomware and other exploits. This often results in data breaches and insider threats that can go undetected without protections in place. CionSystems Change Auditor provides real-time threat monitoring and security tracking of all key user activity and administrator changes, login activities and other object changes. Furthermore, undo any changes with a click!

Easy Recovery

Establish a complete Entra ID recovery plan that minimizes downtime with no impact on end users. CionSystems Easy Recovery makes it possible. Easily select exactly what you need or recover many users, groups and group memberships in bulk without PowerShell. You can further select specific attributes and recover. Don't take any chances, mitigate the risk of data loss or service outage from human error and save valuable time and resources. Quickly know what is different between two backups. You can further use the audit tool to get a history of all changes!

Active Directory and Entra ID recovery plan is essential for every organization to protect from complete enterprise failure. More and more enterprises have adopted Azure/Office365 and have more users and data across Entra ID that need to be protected. Enterprise must protect cloud-only objects such as Microsoft 365 and Entra ID groups, Azure B2B accounts, conditional access policies and more. CionSystems Easy Recovery will help your organization realize a complete Entra ID recovery plan that encompasses your entire hybrid environment.



Complete the form and click on “Continue” button

✕

One more thing ...

 **Dev offer for internal testing**
By cionsystems inc.

This app requires some basic profile information. We have pulled your Microsoft Account data to help you get started. Azure Marketplace will save your information for next time.

Name *	leo	leo
Work email *	leoh08753@gmail.com	
Job title	admin	
Company	Leo Org	
Country / region *	United States ▼	
Phone number *	4256055325	

I give Microsoft permission to use or share my [account information](#) so that the provider or Microsoft can contact me regarding this product and related products. I agree to the provider's [terms of use](#) and [privacy policy](#) and understand that the rights to use this product do not come from Microsoft, unless Microsoft is the provider. Use of Azure Marketplace is governed by separate [terms](#) and [privacy](#).

You're signed in as Leo Leo (leoh@leoh08753gmail.onmicrosoft.com)

Continue

Select a plan and then click on the “Subscribe” button on the Azure portal page



Home >

CionSystems Entra ID Auditor, Backup & Restore (preview) ✨ ...

cionsystems inc.



CionSystems Entra ID Auditor, Backup & Restore (preview) [Add to Favorites](#)

cionsystems inc. | SaaS

Plan

Basic Plan (25 users)

A red rectangular box highlights the "Plan" dropdown menu, which currently shows "Basic Plan (25 users)". Another red rectangular box highlights the blue "Subscribe" button. A large black arrow points from the right towards the "Subscribe" button, and another large black arrow points upwards from the "Plans + Pricing" tab towards the "Plan" dropdown.

[Overview](#) [Plans + Pricing](#) [Usage Information + Support](#) [Ratings + Reviews](#)

Offered under [Microsoft Standard Contract](#).

A turnkey solution for 360 degree audit, alert, protection and recovery of Microsoft Entra ID for Azure and Office365.

Respond instantly even to advanced threats. Ensure compliance with regulatory standards.

Entra ID is the cornerstone for securing access to business-critical applications in Azure or Office365. Yet change reporting and vulnerability monitoring is cumbersome, time-consuming, and often impossible using out of the box tools. In a hybrid environment, it doubles the attack surface and introduces additional opportunities for ransomware and other exploits. This often results in data breaches and insider threats that can go undetected without protections in place. CionSystems Change Auditor provides real-time threat monitoring and security tracking of all key user activity and administrator changes, login activities and other object changes. Furthermore, undo any changes with a click!

Easy Recovery

Establish a complete Entra ID recovery plan that minimizes downtime with no impact on end users. CionSystems Easy Recovery makes it possible. Easily select exactly what you need or recover many users, groups and group memberships in bulk without PowerShell. You can further select specific attributes and recover. Don't take any chances, mitigate the risk of data loss or service outage from human error and save valuable time and resources. Quickly know what is different between two backups. You can further use the audit tool to get a history of all changes!

Active Directory and Entra ID recovery plan is essential for every organization to protect from complete enterprise failure. More and more enterprises have adopted Azure/Office365 and have more users and data across Entra ID that need to be protected. Enterprise must protect cloud-only objects such as Microsoft 365 and Entra ID groups, Azure B2B accounts, conditional access policies and more. CionSystems Easy Recovery will help your organization realize a complete Entra ID recovery plan that encompasses your entire hybrid environment.

Create a new Resource Group and provide a name for the subscription and click on “**Review + subscribe**” button. You can change the Plan if desired.

Microsoft Azure

Home > CionSystems Entra ID Auditor, Backup & Restore (preview) >

Subscribe To CionSystems Entra ID Auditor, Backup & Restore

Subscribe to plan

* Basics Tags Review + subscribe

Fill out the plan details. After you've finished subscribing, configure your SaaS account on the publisher's website to complete the process.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription ①

Resource group * ②

SaaS details

Name * ③

Plan

Basic Plan (10 users) - 1-year subscription

This plan is the most basic one, covering tenants with a minimum of 10 users. Any additional users will be charged at the rate of \$10 USD/enabled Entra ID user/month. If you have any pricing questions, please reach out to sales@cionsystems.com.

[Change plan](#)

1-year subscription

\$100.00/month
Includes:
Entra ID Users: 10

Plus:
Entra ID Users: \$10 per additional enabled entra id user per month

Subtotal | \$1,200.00 for 1 year

④

[Review + subscribe](#) < Previous Next: Tags >

Review and complete the subscription process by clicking on “subscribe” button

Microsoft Azure Search resources, services, and

Home > CionSystems Entra ID Auditor, Backup & Restore (preview) >

Subscribe To CionSystems Entra ID Auditor, Backup & Restore

Subscribe to plan

* Basics [Tags](#) [Review + subscribe](#)

Product + plan details

CionSystems Entra ID Auditor, Backup & Restore - Basic Plan (10 users)
by cionsystems inc.
[Microsoft Standard Contract](#)
[Privacy policy](#)

Terms of use

By clicking "Subscribe" and completing the purchase with the provider, I (a) agree to the legal terms and privacy statements associated with each Marketplace offering above, (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offerings, including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offerings, (c) agree that Microsoft may share my contact information and transaction details (including usage volume associated with the offering) with the sellers of the

Contact details

Name	leo leo
Email address	leoh@leoh08753gmail.onmicrosoft.com
Primary phone number	4256055325

Basics

Subscription	Azure subscription 1
Resource group	cionsaassub
Name	adexploitsub6
Plan	Basic Plan (10 users)
Billing type	1-year subscription
Price/payment frequency	\$100.00/month Includes: Entra ID Users: 10

After subscribing, remember to configure your SaaS account on the publisher's website.

Subscribe < Previous: Tags Next >

Once the subscription is processed, complete the purchase by completing the configuration process on the CionSystems SaaS portal – by clicking on the **“Configure account now”** button.

Microsoft Azure Search resources, services, and

Home > CionSystems Entra ID Auditor, Backup & Restore (preview) > Subscribe To CionSystems Entra ID Auditor, Backup & Restore >

Subscription progress

✔ **Almost done! Next, configure your account on the publisher's website**

SaaS resource name: adexploitsub6

Purchase start time: Tuesday, February 27, 2024 at 10:07:46 PM

Offer & plan details: CionSystems Entra ID Auditor, Backup & Restore - Basic Plan (10 users) - 1-year subscription

^ Next steps

Configure SaaS account

⚠ Your purchase will be complete once you set up your account on the publisher's website. Check your email for instructions on setting up your SaaS account.

Configure account now

Important to know

Billing will start after your account is configured on the publisher's website.

If no action is taken within 30 days, this SaaS subscription will be automatically deleted.

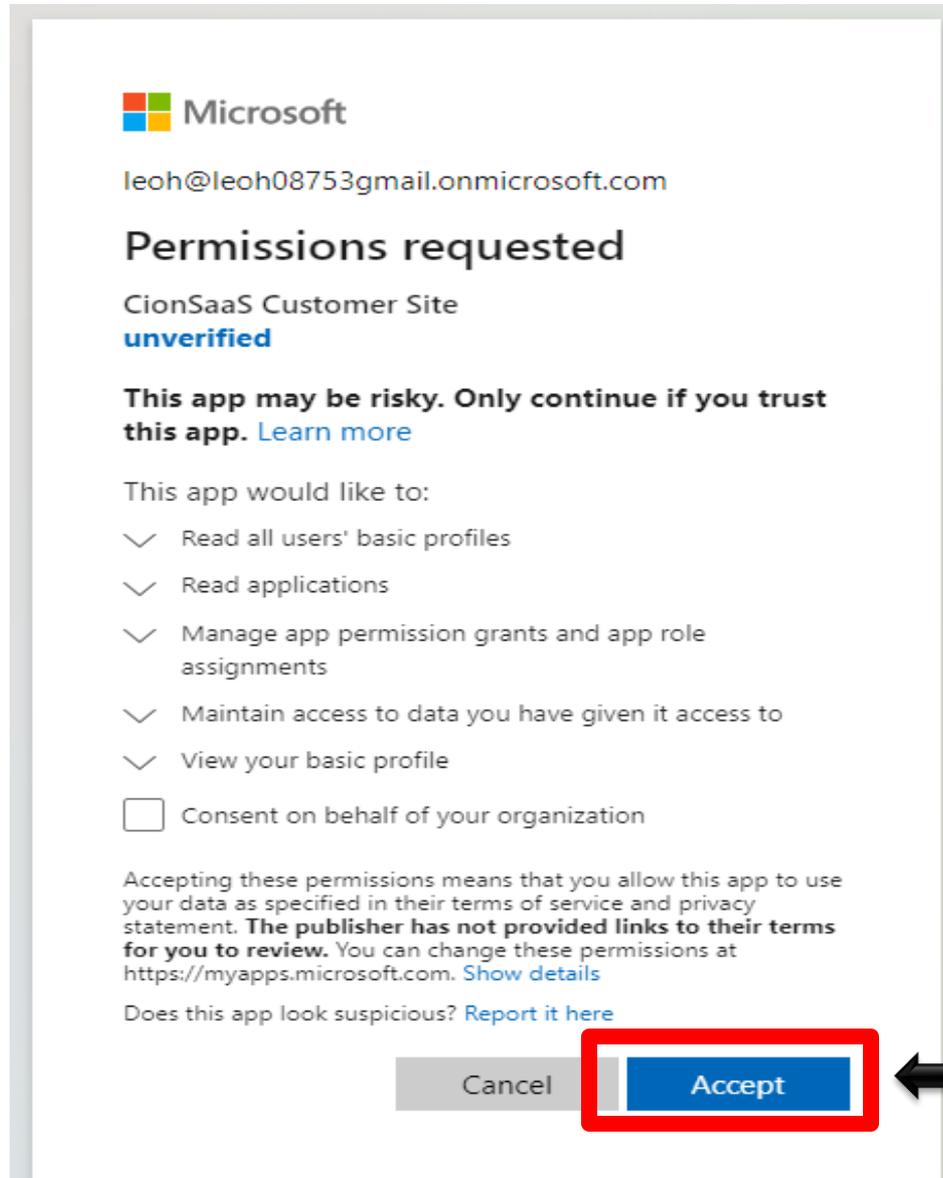
Your SaaS subscription will appear on the [SaaS](#) page in the Azure portal. To access it easily, save it to your favorite services or pin it to the dashboard.

If missed completing the configuration process and need to get back to the subscription page, go back to the Resource Group and the Resource you created in step 5 – click on the **“Configure account now”** button.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various utility icons. The breadcrumb trail indicates the user is in the 'Resource groups' section for 'adexploitsub6'. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Automation, Tasks (preview), and Help. The main content area is titled 'Product and plan details' and contains a message: 'Configure your SaaS account on the publisher's website to complete the purchase. Billing will start after your account is configured. If no action is taken within 30 days from the initial subscription, this SaaS subscription will be automatically deleted.' Below this message is a blue button labeled 'Configure account now', which is highlighted with a red rectangular box and a black arrow pointing towards it from the right. Below the button, there is a table with subscription details:

Basic Plan (10 users) - 1-year subscription	Billing term	Recurring billing	Billing term & price	Billing info
<p>Pending account configuration</p> <p>This plan is the most basic one, covering tenants with a minimum of 10 users. Any additional users will be charged at the rate of \$10 USD/enabled Entra ID user/month. If you have any pricing questions, please reach out to sales@cionsystems.com.</p> <p>Change plan</p>	<p>1-year subscription</p> <p>View billing</p>	<p>Edit recurring billing</p>	<p>\$100.00/month</p> <p>Includes:</p> <p>Entra ID Users: 10</p> <p>Plus:</p> <p>Entra ID Users: \$10 per additional enabled entra id user per month</p>	<p>Created on: 2/27/2024</p> <p>Purchased by: leoh@leoh08753gmail.onmicrosoft.com</p> <p>Azure subscription: Azure subscription 1</p> <p>Change Azure subscription</p> <p>Resource group: cionsaassub</p> <p>Change resource group</p>

You may see a Graph permission consent popup when you navigate to our SaaS portal for the first time. Click on **“Accept”** button



The image shows a Microsoft Graph permission consent popup. At the top left is the Microsoft logo. Below it is the email address 'leoh@leoh08753gmail.onmicrosoft.com'. The main heading is 'Permissions requested'. Underneath, it says 'CionSaaS Customer Site' and 'unverified' in blue. A warning message states: 'This app may be risky. Only continue if you trust this app. Learn more'. A list of permissions follows, each with a checkmark icon: 'Read all users' basic profiles', 'Read applications', 'Manage app permission grants and app role assignments', 'Maintain access to data you have given it access to', and 'View your basic profile'. There is an unchecked checkbox for 'Consent on behalf of your organization'. A paragraph of text explains that accepting means allowing data use as per terms of service and privacy statement, and notes that the publisher has not provided links to their terms for review. It provides a URL 'https://myapps.microsoft.com' and a 'Show details' link. At the bottom, there is a 'Report it here' link. At the very bottom are two buttons: a grey 'Cancel' button and a blue 'Accept' button. The 'Accept' button is highlighted with a red rectangular border, and a black arrow points to it from the right side of the image.

Microsoft

leoh@leoh08753gmail.onmicrosoft.com

Permissions requested

CionSaaS Customer Site
unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Read all users' basic profiles
- ✓ Read applications
- ✓ Manage app permission grants and app role assignments
- ✓ Maintain access to data you have given it access to
- ✓ View your basic profile

Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel Accept

After consenting, proceed to the next page; On the SaaS portal, verify subscription information and click on the “**Subscribe**” button

The application uses cookies to give you a better experience. By proceeding to access the application, you agree to our use of cookies. OK

ADMIN CONSENT & APP ROLE ASSIGNMENT

To complete your subscription, you must first consent to our service offering. You can go to [Cion Systems Entra ID Management Application](#) to consent to our SPN and come back here to complete the role assignment. Once you have completed the role assignment, you can use the application. Use the **Role Assignments** menu tab to complete this task.

SUBSCRIPTION DETAILS

Customer Email	leoh@leoh08753gmail.onmicrosoft.com
Customer Name	leo leo
ID	b620e3c1-5a1a-40d5-d208-e2869fb67726
Name	adexploitsub6
Status	PendingFulfillmentStart
Offer Name	cionsys-prod-offer-preview
Plan	cioncustplan1yr
Purchaser Email	leoh@leoh08753gmail.onmicrosoft.com
Azure Tenant ID	df5aa9d5-ae88-498f-8c27-35310759ce7a

Subscribe

Enroll your tenant into the service by following the instructions on the SaaS portal page. For consent, click on the “CionSystems Entra ID Management Application” button on the home page and go through the enrollment & consenting process:

AD Guardian
Change Alerts

Home

Sign In

My Entra ID

Recovery

Entra ID
Change Tracking,
Backup and Restore

Enroll your company into CionSystems AAD capabilities!

© Copyright CionSystems Inc.

Review the permissions requested and click on the “Accept” button to complete the consent process.

The screenshot shows a Microsoft consent screen. On the left, the Microsoft logo is at the top, followed by the email address 'preston@preston0768gmail.onmicrosoft.com'. Below that, the heading 'Permissions requested' is displayed with the subtext 'Review for your organization'. The application name 'CionSystems.TenantUI' is shown with a status of 'unverified'. A warning message states: 'This application is not published by Microsoft or your organization.' Below this, it says 'This app would like to:' followed by a list of permissions, each with a dropdown arrow. The permissions include: Read and write directory RBAC settings, Read and write administrative units, Maintain access to data you have given it access to, Sign in and read user profile, Read and write all users' full profiles, Read and write all groups, Read and write directory data, Access directory as the signed in user, Read and write all applications, Read all access reviews, Manage all access reviews, Read and write all administrative units, Read all terms of use agreements, Read and write all terms of use agreements, Read API connectors for authentication flows, Read and write API connectors for authentication flows, Read and write all applications, Manage app permission grants and app role assignments, Read all audit log data, Read all devices, Read and write devices, and Read directory data.

On the right side of the screen, there is a list of permissions, each with a dropdown arrow. These include: Read identity providers, Read and write identity providers, Read all identity user flows, Read and write all identity user flows, Read organization information, Read your organization's policies, Read your organization's conditional access policies, Read consent and permission grant policies, Read and write your organization's directory access review default policy, Read and write your organization's authorization policy, Read privileged access to Azure AD roles, Read privileged access to Azure AD groups, Read privileged access to Azure resources, Read and write privileged access to Azure AD roles, Read and write privileged access to Azure AD groups, Read and write privileged access to Azure resources, Read and write all directory RBAC settings, Read all users' full profiles, Read and write all users' full profiles, Read all users' authentication methods, and Read and write all users' authentication methods.

Below the permissions list, there is a warning: 'If you accept, this app will get access to the specified resources for all users in your organization. No one else will be permitted to review these permissions.' Another warning states: 'If you accept, these apps will also have access to your user profile information: CionSystems.TenantSvc.WebAPI, AAD B2C App Restore Graph App.' A third warning says: 'Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. The publisher has not provided links to their terms for you to review. You can change these permissions at https://myapps.microsoft.com. Show details'.

At the bottom of the screen, there are two buttons: 'Cancel' and 'Accept'. The 'Accept' button is highlighted with a red border. A large black arrow points down towards the 'Accept' button.

Validate the confirmation page

Sign up Success - Cion Systems

cionsystemstenantux.azurewebsites.net/Account/SignUpSuccess

Home

AD Guardian
Change Alerts

Sign up Success

You have successfully signed up. Please follow the [documentation to assign application roles](#).

My Entra ID

Return to the SaaS portal window and complete setup by clicking on the “Subscribe” button

The application uses cookies to give you a better experience. By proceeding to access the application, you agree to our use of cookies. OK

ADMIN CONSENT & APP ROLE ASSIGNMENT

You can go to [Cion Systems Entra ID Management Application](#) to consent to our SPN and come back here to complete this task.

SUBSCRIPTION DETAILS

Customer Email	leoh@leoh08753gmail.onmicrosoft.com
Customer Name	leo leo
ID	b620e3c1-5a1a-40d5-d208-e2869fb67726
Name	adexploitsub6
Status	PendingFulfillmentStart
Offer Name	cionsys-prod-offer-preview
Plan	cioncustplan1yr
Purchaser Email	leoh@leoh08753gmail.onmicrosoft.com
Azure Tenant ID	dfsaa9d5-ae88-498f-8c27-35310759ce7a

Subscribe

You'll see this page that indicates that the provisioning process is in progress

The screenshot shows a web interface for CionSystems. At the top left is the CionSystems logo with the tagline "Next Generation Enterprise Identity Management (EM)". At the top right is the email address "leoh@leoh08753". Below the header is a navigation menu with "Home", "Profile", and "Role Assignments". A dark grey banner at the top contains a cookie consent message: "The application uses cookies to give you a better experience. By proceeding to access the application, you agree to our use of cookies." with an "OK" button. The main content area has a heading "ADMIN CONSENT & APP ROLE ASSIGNMENT" followed by instructions: "To complete the subscripion process, you need to admin consent to our application in your tenant by enrolling it into our service offering. You can go to [Cion Systems Entra ID Management Application](#) to consent to our SPN and come back here to complete the subscription process. Once you have completed the consent process, you need to provision users from your tenant with appropriate roles to use the application. Use the **Role Assignments** menu tab to complete this task." Below this is a heading "SUBSCRIPTION DETAILS" and a table of subscription information. A white box with a loading spinner and the text "* Just a moment..." is overlaid on the "Customer Email" field. At the bottom right is a "Subscribe" button.

Home Profile Role Assignments

The application uses cookies to give you a better experience. By proceeding to access the application, you agree to our use of cookies. OK

ADMIN CONSENT & APP ROLE ASSIGNMENT

To complete the subscripion process, you need to admin consent to our application in your tenant by enrolling it into our service offering. You can go to [Cion Systems Entra ID Management Application](#) to consent to our SPN and come back here to complete the subscription process. Once you have completed the consent process, you need to provision users from your tenant with appropriate roles to use the application. Use the **Role Assignments** menu tab to complete this task.

SUBSCRIPTION DETAILS

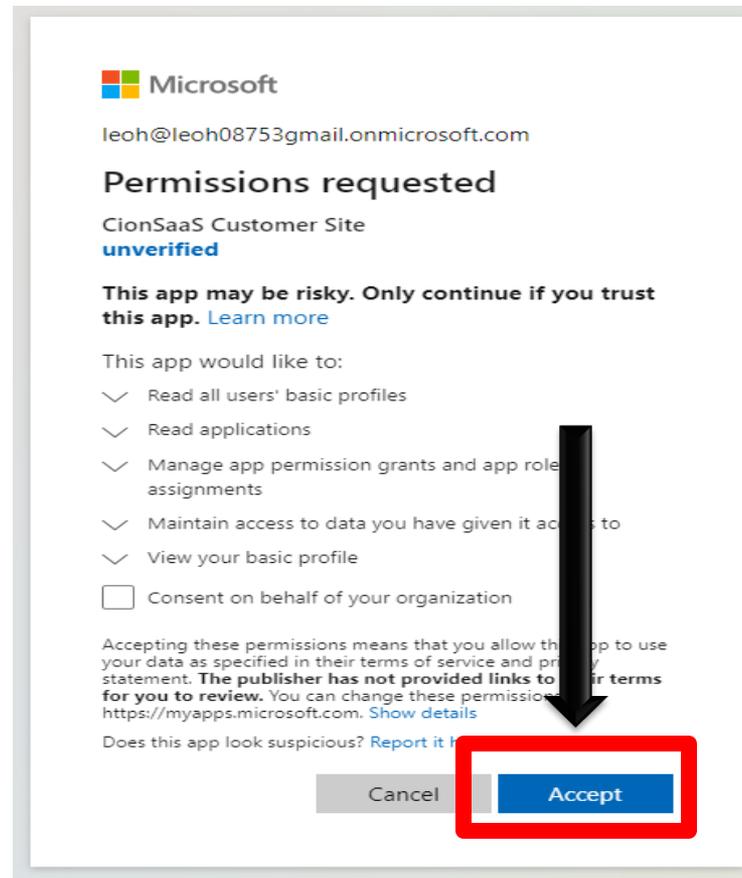
Customer Email	leo
Customer Name	leo leo
ID	b620e3c1-5a1a-40d5-d208-e2869fb67726
Name	adexploitsub6
Status	PendingFulfillmentStart
Offer Name	cionsys-prod-offer-preview
Plan	cioncustplan1yr
Purchaser Email	leoh@leoh08753gmail.onmicrosoft.com
Azure Tenant ID	df5aa9d5-ae88-498f-8c27-35310759ce7a

Subscribe

Once the provisioning process is complete, you'll see this page

The screenshot displays a web application interface. At the top left is the CionSystems logo. A navigation bar contains links for Home, Profile, and Role Assignments. A light blue cookie consent banner is visible, with an 'OK' button on the right. Below this, a grey message box states: 'Processing your request. Updated status of the activity is available in the subscription list.' A large black arrow points from the 'OK' button down to a blue button labeled 'Go to Subscription List', which is highlighted with a red rectangular border.

You should also identify a set of users who you want to grant the necessary roles within the CionSystems Entra ID Management portal to allow them access to your tenant data. These users are from your directory and they should be granted the **“TenantAdmin”** role within our system: You may get a one-time prompt to consent for Graph Permissions for the application in your tenant when you navigate to the **“Role Assignments”**

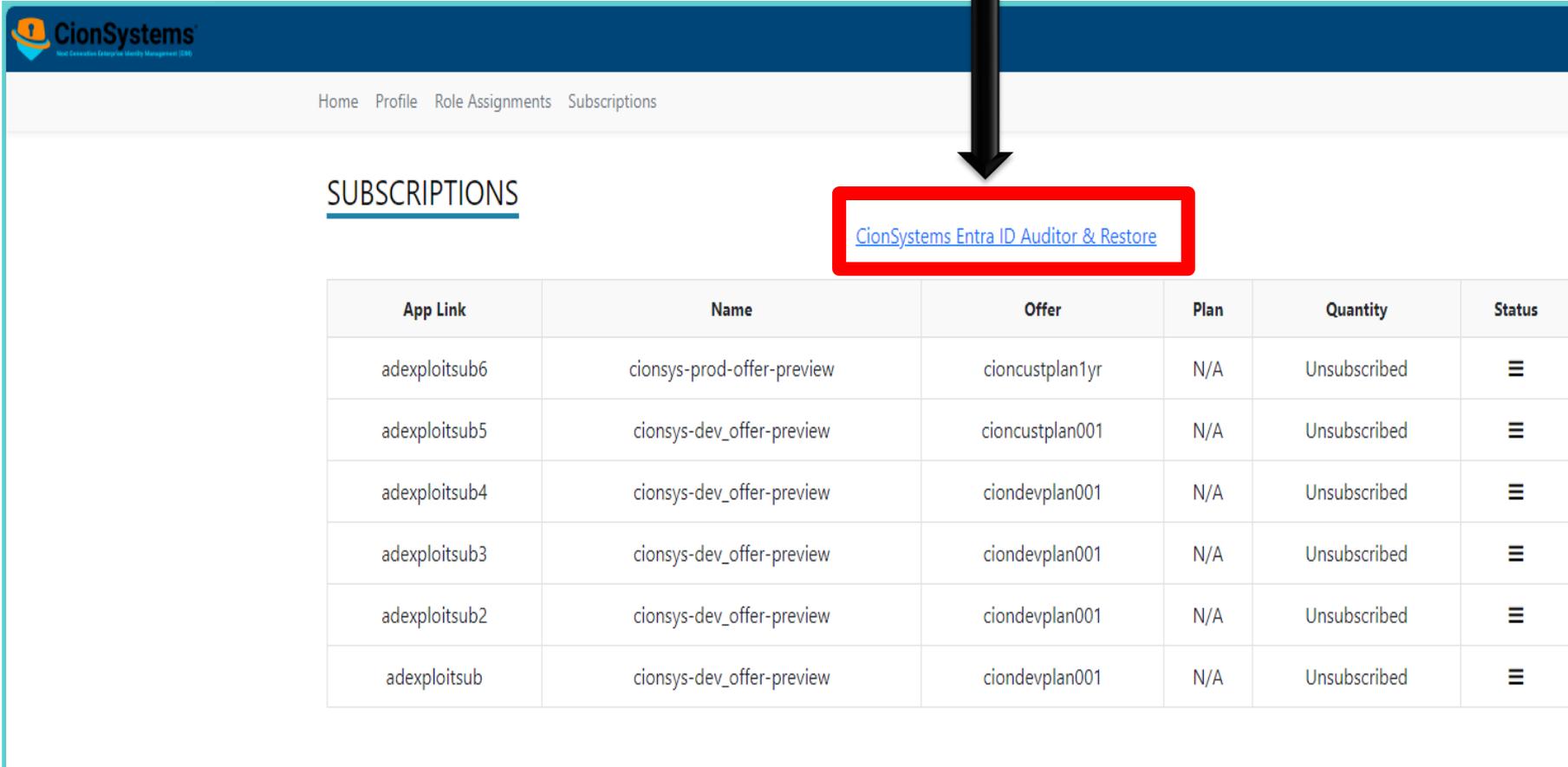


In the below grid, fill in the UPN of the user and select a role – only use TenantAdmins role, and assign the role to the users. Users will need this role to use the CionSystems Entra ID Auditor and Restore application

APP ROLE ASSIGNMENTS

Name	Resource Name	Role Name	Role Description	Principal Type	Action
leo leo	CionSystems.TenantSvc.WebAPI	TenantAdmins	Admins of the tenant that is onboarding to the service	User	Remove Assignment
mukhtar	CionSystems.TenantSvc.WebAPI	TenantAdmins	Admins of the tenant that is onboarding to the service	User	Remove Assignment
zonuptechnologies	CionSystems.TenantSvc.WebAPI	TenantAdmins	Admins of the tenant that is onboarding to the service	User	Remove Assignment
Login Test Account	CionSystems.TenantSvc.WebAPI	Billing Admin	App role for the billing admins who can manage payment information for the tenants	User	Remove Assignment
Login Test Account	CionSystems.TenantSvc.WebAPI	TenantAdmins	Admins of the tenant that is onboarding to the service	User	Remove Assignment
<input type="text" value="Enter user UPN"/>	<input type="text" value="Select Role"/>	<input type="text" value="▼"/>	<input type="button" value="Add User to Role"/>		

To Access the CionSystems Entra ID Auditor & Recovery application, you can go to the “Subscriptions” top navigation menu option and click



The screenshot shows the CionSystems application interface. At the top left is the CionSystems logo with the tagline "Your Connected Enterprise Health Management". Below the logo is a navigation bar with the following options: Home, Profile, Role Assignments, and Subscriptions. The "Subscriptions" option is highlighted. Below the navigation bar is a section titled "SUBSCRIPTIONS". To the right of this section is a link labeled "CionSystems Entra ID Auditor & Restore", which is highlighted with a red rectangular box. A large black arrow points from the text above to this link. Below the link is a table with the following columns: App Link, Name, Offer, Plan, Quantity, and Status. The table contains six rows of subscription data.

App Link	Name	Offer	Plan	Quantity	Status
adexploitsub6	cionsys-prod-offer-preview	cioncustplan1yr	N/A	Unsubscribed	≡
adexploitsub5	cionsys-dev_offer-preview	cioncustplan001	N/A	Unsubscribed	≡
adexploitsub4	cionsys-dev_offer-preview	ciondevplan001	N/A	Unsubscribed	≡
adexploitsub3	cionsys-dev_offer-preview	ciondevplan001	N/A	Unsubscribed	≡
adexploitsub2	cionsys-dev_offer-preview	ciondevplan001	N/A	Unsubscribed	≡
adexploitsub	cionsys-dev_offer-preview	ciondevplan001	N/A	Unsubscribed	≡

Now CionSystems Inc will finalize activation of your subscription and allow you to access the full suite of services

Contact Notes:

For technical support or feature requests, please contact us at Support@CionSystems.com or 425.605.5325

For sales or other business inquiries, we can be reached at Sales@CionSystems.com or 425.605.5325

If you'd like to view a complete list of our Active Directory Management solutions, please visit us online at www.CionSystems.com

Disclaimer

The information in this document is provided in connection with CionSystems products. No license, express or implied, to any intellectual property right, is granted by this document or in connection with the sale of CionSystems products. EXCEPT AS SET FORTH IN CIONSYSTEMS' LICENSE AGREEMENT FOR THIS PRODUCT, CIONSYSTEMS INC. ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED, OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL CIONSYSTEMS INC. BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF CIONSYSTEMS INC. HAS BEEN ADVISED IN WRITING OF THE POSSIBILITY OF SUCH DAMAGES. CionSystems may update this document or the software application without notice.



CionSystems Inc.

6640 185th Ave NE,

Redmond, WA-98052, USA

www.CionSystems.com

Ph: +1.425.605.5325

This guide is provided for informational purposes only, and the contents may not be reproduced or transmitted in any form or by any means without our written permission