Synology®

C2 Identity Deployment Strategies

Last May 30, 2024

Table of Contents

Introduction

Challenges in identity management

In today's digitally-interconnected world, organizations face a number of cybersecurity challenges, each carrying significant implications for both security and operational efficiency. These challenges go beyond mere inconveniences, posing potential risks to data security, regulatory compliance, and overall business continuity.

One common issue is inconsistencies when it comes to identity authentication methods. Weak or reused passwords, coupled with complicated 2-factor authentication (2FA) setups, can lead to security breaches, monetary losses, and even reputational harm. Manual identity management isn't a foolproof solution either, since employees may unintentionally grant unauthorized access to sensitive data due to outdated controls or misconfigured permissions. This could result in data breaches that affect both regulatory compliance and customer relationships.

Another challenge is managing a remote workforce. Without secure device management or remote access solutions, employees might leave the organization vulnerable to threats like malware or data breaches. Failing to adopt modern authentication practices could leave your organization susceptible to emerging threats, potentially leading to account takeovers or unauthorized access to confidential data.

Amidst these challenges, C2 Identity emerges as a comprehensive solution that addresses the complexities of modern identity management.

C2 Identity as a solution

C2 Identity is an identity and access management (IAM) solution that provides designed to streamline the management of enterprise resources. Whether it's overseeing local services, Mac and Windows devices, or cloud applications, C2 Identity provides centralized control from a single platform. Admins can effortlessly manage user permissions, enable/disable access, and enforce security measures like password policies.

C2 Identity features

Unify your identity management system:

- Sync or import on-premises directory services such as **Active Directory (AD)** or **LDAP** to C2 Identity for centralized user management and authentication.
- Enable **Single Sign-On (SSO)** for various applications using **Security Assertion Markup Language (SAML)**, streamlining user access across the organization.

- Deploy **Edge Servers** as LDAP servers that authenticate locally to ensure continuous synchronization of authentication data between on-premises infrastructure and the C2 Identity cloud server, as well as ensure service availability in case of network failure.
- Utilize the **C2 Identity agent** to manage device authentication and support password configuration and updates for enhanced administrative control and convenience.

Enhance on and offsite security:

- Manage the entire **life cycle of employee accounts** from a single, centralized location, reducing the risk of potential security gaps and delays when revoking access when employees leave.
- Enforce consistent **password rules** across your organization, or implement advanced authentication methods such as **2-Factor Authentication (2FA)** and **passwordless logins** to minimize the risk of unauthorized access.
- Access **centralized logs and monitoring** capabilities to track user activities, detect anomalies, and respond to security incidents effectively.
- Integrate with **C2 Password** to manage passwords for services that don't support direct integration with C2 Identity, ensuring secure access to all of your resources.

Plan Your C2 Identity Deployment

Requirements and supported systems

The C2 Identity portal can be run on any browser, meaning that you can start managing identities and user access to cloud applications, such as Microsoft 365 and Google Workspace, as soon as you sign in.

However, to integrate and manage user accounts via Microsoft Active Directories, LDAP directories, or Edge Servers, you must deploy the C2 Identity agent. With that in mind, it's important to note that each respective agent has specific system requirements depending on its deployment environment. We strongly recommend making yourself familiar with these requirements prior to deployment:

Feature	System requirements	Additional requirements
C2 Identity agent	• **Windows (64-bit only)**: Windows 7, 10, and 11 • **Windows Server**: Windows Server 2008 R2 and above • **macOS**: macOS Catalina (10.15), Big Sur (11), Monterey (12), Ventura (13), and Sonoma (14)	
C2 Identity Edge Server	• **Synology NAS**: DSM 7.0 and above • **Docker**: Any Docker-compatible operating system	• Supported NAS models • Internet access required for data synchronization
C2 Identity AD Sync	• **Windows Server**: Windows Server 2008 R2 SP1 or above	• PowerShell 5.1 and above

C2 Identity LDAP Sync	• **Windows (64-bit only)**: Windows 7, 10, and 11 • **Windows Server**: Windows Server 2008 R2 and above • **Linux**: Ubuntu 16.04 and above	• PowerShell 5.2 and above • Synology LDAP Server (for LDAP directory integration)

Deployment environment

When embarking on your C2 Identity deployment journey, it's important to have a thorough understanding of your organization's existing IT infrastructure. Tailoring your deployment strategy to align with these existing systems helps ensure a seamless integration process.

Here, we will explore a few different deployment scenarios tailored to common IT architectures.

Once you've decided on a deployment approach, you can find the relevant setup instructions you need in this C2 Identity index article.

Integrating existing AD/LDAP services

For organizations looking to transition or integrate their existing directory services to C2 Identity, consider the following deployment approaches:

Scenario	Recommended Method	Instructions
You want to immediately transition to using C2 Identity	Import all at once via a CSV file	• Import users and groups from a CSV file • Import users and groups from Microsoft Active Directory • Import users and groups from an LDAP server
You want to gradually transition to using C2 Identity	Import in phases via AD Sync or LDAP Sync, pausing when needed	• Integrate Active Directory with C2 Identity • Integrate an LDAP directory with C2 Identity
You want to use your AD or LDAP services and C2 Identity at the same time	Integrate your AD or LDAP directory with C2 Identity	

Importing data all at once is suitable for those intending to discontinue the use of the original AD or LDAP service, allowing the direct transfer of user data to C2 Identity.

Alternatively, you can also choose a more gradual transition to maintain operational continuity by implementing a phased import strategy. This involves integrating user data incrementally, manually pausing and resuming the Sync Agent as needed.

Lastly, if you intend to utilize both C2 Identity and existing directory services at the same time, opting for integration is a great choice, since it ensures the seamless and constant synchronization of user data between the two platforms.

Managing local applications for multiple sites

For organizations needing uninterrupted service availability across multiple branch locations or in case of a directory server failure, consider the following deployment approaches:

Scenario	Recommended Method	Instructions
You have multiple NAS deployments at different branches You want to mitigate directory server failure risks	Deploy Edge Servers	• Set up an Edge Server
You're currently using Synology LDAP Server	1. Integrate directory via LDAP Sync 2. Deploy Edge Servers	• Integrate an LDAP directory with C2 Identity • Convert Synology LDAP Server into an edge server
You have applications that support SAML SSO	Implement Single-Sign-On (SSO)	• Integrate an application via custom SAML SSO • Set up your Synology NAS as an SSO client

For organizations with multiple NAS deployments, or for those seeking to enhance resilience against single directory server failures, we suggest deploying Edge Servers. Edge Servers serve as additional points of data synchronization, continuously syncing with the C2 Identity server to ensure on-premises access to applications even without an Internet connection. You can also further enhance authentication service availability in distributed environments by deploying multiple Edge Servers across different branches.

For those currently using Synology LDAP Server on Synology NAS, we suggest leveraging LDAP Sync to integrate it with C2 Identity, allowing you to manage the directory from LDAP Server. This can be additionally complemented with one or more Edge Servers, so that in the event of LDAP Server downtime, the Edge Server can take over to provide authentication services and guarantee uninterrupted access to on-premises applications.

Single Sign-On (SSO) can also be utilized for SAML SSO-supported applications. SAML SSO enhances security by providing a single point of authentication, reducing the risk of password-related breaches, and streamlining the user experience across multiple platforms. By centralizing authentication, SAML SSO simplifies access management while increasing efficiency for both users and admins.

For example, you can set up your Synology NAS as an SSO client for seamless access to services hosted on the NAS. This integration allows users to authenticate once to gain access to multiple applications and services, both cloud-based and local, without needing to sign in separately for each one.

Managing Windows and macOS devices

For organizations with remote employees or those looking to utilize advanced authentication methods, consider the following deployment approaches:

<table>
<tr><th>Scenario</th><th>Recommended Method</th><th>Instructions</th></tr>
<tr><td>You are currently using AD for both macOS and Windows devices</td><td rowspan="2">Use AD Sync to import user accounts to C2 Identity
Deploy the C2 Identity agent to devices</td><td rowspan="2">Integrate Active Directory with C2 Identity
Add a managed device
Install C2 Identity agents via command lines</td></tr>
<tr><td>You are currently using AD and have remote employees</td></tr>
<tr><td>You have remote employees</td><td rowspan="2">Deploy C2 Identity agent to devices</td><td rowspan="2">Add a managed device
Install C2 Identity agents via command lines</td></tr>
<tr><td>You want to implement advanced authentication methods like passwordless logins</td></tr>
</table>

For comprehensive management of Mac and Windows devices, deploying the C2 Identity agent is essential, especially if you have remote employees or need support for advanced authentication methods like passwordless logins.

Managing cloud applications

For organizations looking for comprehensive management of all of their cloud applications, consider the following deployment approaches:

Scenario	Recommended Method	Instructions
You have cloud applications that support SAML	Use SAML SSO to integrate your cloud applications	• Integrate applications with C2 Identity • How do I integrate Slack via custom SAML SSO?
You have cloud applications that don't support SAML	Use C2 Password to manage your cloud app credentials	• Manage credentials with C2 Password • C2 Password - Tutorials & FAQs Overview • C2 Password Business Quick Start Guide

If the applications you need to use support SAML integration, you should utilize this feature for consistent access control and user management. For applications that do not support SAML, integrate them via C2 Password to ensure secure management and enhance your users' experience.

Configure C2 Identity for your organization

After you've assessed your organizational needs and decided on a deployment method based on the scenarios provided in Deployment environment, refer to C2 Identity - Tutorials & FAQs Overview to find the tutorials you need for setup and configuration.

Practical Scenarios for Implementation

This chapter offers insights into real-world identity management challenges commonly faced by enterprises and provides tailored best practices to address these issues effectively.

Simplifying identity management for growing organizations

In today's digital era, organizations, particularly those with large work forces and relatively smaller IT teams, often grapple with the complex task of managing authentication systems and implementing security policies. This struggle originates from the need to balance user accessibility and system security, a task that becomes increasingly complicated as a company expands.

To understand the complexities involved, let's look at the following case of an organization in need of an identity management solution to address several pressing challenges:

- **Many different accounts**: An LDAP server is used to internal services and various cloud applications, with each user on a separate account. However, having separate accounts for each service can lead to confusion for both users and managers, and can violate current security compliance policies and regulations.
- **Difficulty with macOS integration**: Device authentication is done via Microsoft Active Directory (AD), which works well for Windows devices, but integration for Macs can be technically challenging.
- **Employee mobility**: Remote work and the mobility of sales personnel complicates authentication, especially in terms of managing macOS devices.
- **No passwordless options**: Their traditional directory services lack passwordless sign-in options, posing potential security concerns.

It's clear that this organization had numerous factors to take into account when choosing a new identity solution. The diverse features and flexible configurations of C2 Identity made it possible for them to deploy it easily and seamlessly as their identity solution.

We'll explore these features and provide best practices for seamless integration and setup for similar situations.

Integrating C2 Identity with existing directory

For organizations authenticating internal services using AD and LDAP servers who are also looking to gradually transition to C2 Identity, we recommend using the **synchronization** method for C2 Identity deployment.

This ensures that user data on your AD and LDAP servers are consistently aligned with C2 Identity, not only allowing for user access management and creation via the C2 Identity portal, but also providing a transition period for your organization to start utilizing C2 Identity's features while still relying on the original domain server for authentication. Since all account data are stored in the cloud, you can cease using your domain server at any time to fully transition to C2 Identity.

Deploying Windows and macOS devices

Admins can easily deploy the C2 Identity agent to both local or remote Windows and macOS devices by downloading and installing it using a **connect key** from the admin portal. However, when you have a large number of users, manual agent installation isn't ideal. Instead, we recommend using mass deployment to deploy the agent to all of the devices in your organization for a smoother on-boarding process.

We recommend using either of the following options to mass deploy the C2 Identity agent:

- **Command-line deployment**: Mass deployment for both macOS and Windows devices can be easily achieved by executing command-line instructions. Devices managed by Active Directory Domain Services, Microsoft Intune, or Jamf can utilize this method for efficient deployment.
- **GPO deployment from Microsoft AD / Synology Directory Server**: If you use Microsoft AD or Synology Directory Server for Windows device authentication, you can deploy a large number of Windows PCs within the domain using **Group Policy Objects (GPO)**. For seamless agent installation, GPO settings can be configured for synchronization across all devices.

Configuring user roles and security policies

Organizations with diverse device operating systems and remote employees can take advantage of C2 Identity's security features and user role configurations to prevent potential security issues.

Assign roles automatically via default groups

In C2 Identity, groups are a tool for organizing users and managing their access to devices, applications, and other resources more efficiently. Groups can also be nested within one another to simplify the task of assigning privileges to a multitude of users.

There are two default groups in C2 Identity:

- **Default device users**: Users in this group automatically get access to all new devices. Adding users to the **Default device users** group lets you assign device roles without having to

configure each user individually.

- **Everyone**: This group includes all user accounts and is nested within the **Default device users group** by default, so users in the **Everyone** group will have access privileges inherited from this group. If you don't want all users to have admin privileges, you can either adjust permissions for the **Everyone** group directly, or move the **Everyone** group out of the **Default device users** group.

We suggest taking advantage of these default groups to streamline the identity and device management process for both your IT team and the rest of your users. You can do this by first separating the **Everyone** group from **Default device users**. Then, give **Default device users** "**Administrator**" privileges and add your IT team members to it. If needed, you can also adjust the **Everyone** group permissions.

Configuring permissions for these default groups in this way not only ensures that newly added IT team members automatically have admin privileges to manage employee devices, but also that regular employees don't have unnecessary permissions to other devices for security purposes.

Enforce passwordless sign-in

Since traditional passwords are not always secure for regular log-ins, we strongly recommend implementing passwordless sign-ins to increase security and simplify the authentication process. Passwordless policies can be enforced for certain user groups, ensuring both flexibility and compliance with security standards.

Configure security policies via commands

After installing the C2 Identity agent on devices, admins can manage security policies centrally via **Commands** in the **C2 Identity admin portal**. Settings for these policies can be configured in bulk, including enforcing policies like automatic updates, locking the control panel, and more. This lightens the IT load for smoother and more efficient authentication management.

Authenticating internal and cloud applications

When you have a diverse range of both internal and cloud services that you need to provide authentication services for, it's essential to adopt solutions that streamline and secure access across your organization.

Convert LDAP Servers to Edge Servers

For organizations using Synology LDAP Server or Synology Directory Server, Edge Servers are especially useful for authenticating local services. Converting a Synology LDAP Server to a C2 Identity Edge Server is straightforward and enables LDAP clients to authenticate users without needing to rebind to the directory service.

To address concerns regarding downtime during the LDAP to Edge Server conversion process, we suggest duplicating the current directory server before conversion. It's important to make sure that all client-side applications are already configured to switch to the new Edge Server's IP address for uninterrupted service availability. While this approach requires additional configuration efforts on the client side, it offers a viable alternative for organizations prioritizing continuous service availability during the conversion period.

Utilize user groups and provisioning

For organizations with a large number of users, along with many different applications, we suggest utilizing **user groups** and **user provisioning** to streamline access.

User groups can be assigned to specific applications that support Security Assertion Markup Language (SAML). This allows these users to access applications using either individual or communal work group accounts. Using communal accounts for applications while maintaining individual C2 user accounts and passwords is more cost-effective and makes account management easier.

Along with that, automated user provisioning or de-provisioning processes can help ensure that each user has separate accounts for signing in to various SaaS applications based on organizational requirements. This automation streamlines IT processes related to user life-cycle management, including on-boarding, transfers, promotions, and off-boarding.

Conclusion

Modern identity management can pose many complexities and uncertainties for organizations, particularly concerning cybersecurity. A weak identity management framework leaves the door open for security breaches, which can result in significant monetary loss, damage to reputation, non-compliance issues, and strained client relationships.

C2 Identity provides a comprehensive solution to these challenges. Offering robust security, seamless integration, and flexible deployment options, it caters to a variety of organizational needs. By carefully aligning your deployment strategy with existing systems, integration becomes a breeze. But that's not all - C2 Identity's features empower you to manage remote work forces, authenticate devices, and handle cloud applications with ease. Once you fully grasp its capabilities, you'll be able to leverage C2 Identity to safeguard your organization's digital assets and boost operational efficiency.